Reference

Mark Craig

Table of Contents

***Reference for OpenDJ directory server and bundled tools. The OpenDJ** project offers open source LDAP directory services in Java.*

Preface

This reference covers OpenDJ directory server configuration, tools bundled with OpenDJ directory server, and a number of other topics such as supported languages and standards.

Who Should Use this Reference

This reference is written for OpenDJ integrators and administrators.

For API specifications suitable for OpenDJ developers, see the appropriate Javadoc.

Formatting Conventions

Most examples in the documentation are created in GNU/Linux or Mac OS X operating environments. If distinctions are necessary between operating environments, examples are labeled with the operating environment name in parentheses. To avoid repetition file system directory names are often given only in UNIX format as in `/path/to/server` , even if the text applies to `C:\path\to\server` as well. Absolute path names usually begin with the placeholder `/path/to/` . This path might translate to `/opt/` , `C:\Program Files\` , or somewhere else on your system. Command-line, terminal sessions are formatted as follows:

```
$ echo $JAVA_HOME
/path/to/jdk
```

Command output is sometimes formatted for narrower, more readable output even though formatting parameters are not shown in the command. Program listings are formatted as follows:

```
class Test {
    public static void main(String [] args)  {
        System.out.println("This is a program listing.");
    }
}
```

Accessing Documentation Online

Open Identity Platform Community publishes comprehensive documentation online:

- The Open Identity Platform Community Documentation offers a large and increasing number of up-to-date, practical articles that help you deploy and manage Open Identity Platform software.
- Open Identity Platform product documentation, such as this document, aims to be technically accurate and complete with respect to the software documented. It is visible to everyone and covers all product features and examples of how to use them.

Joining the Open Identity Platform Community

Visit the community resource center where you can find information about each project, download nightly builds, browse the resource catalog, ask and answer questions on the forums, find community events near you, and of course get the source code as well.

Getting Support and the Contacting Open Identity Platform Community

Open Identity Platform Community Approved Vendors provide support services, professional services, trainings, and partner services to assist you in setting up and maintaining your deployments.

Tools Reference

You can find bundle tools under the folder where you installed OpenDJ directory server as listed in "Command-Line Tools" in the *Administration Guide*.

backendstat(1)

Name

backendstat - gather OpenDJ backend debugging information

Synopsis

`backendstat {subcommand} {options}`

Description

This utility can be used to debug a backend.

Options

The `backendstat` command takes the following options:

`-V | --version`
: Display Directory Server version information.

  Default: false

`-H | --help`
: Display this usage information.

  Default: false

Subcommands

The `backendstat` command supports the following subcommands:

backendstat dump-index

Dump records from an index, decoding keys and values. Depending on index size, this subcommand can generate lots of output.

Options

`-n | --backendID {backendName}`
: The backend ID of the backend.

`-b | --baseDN {baseDN}`
: The base DN within the backend.

`-i | --indexName {indexName}`

The name of the index.

`-q | --statsOnly`

Do not display backend data, just statistics.

Default: false

`-K | --maxKeyValue {maxKeyValue}`

Only show records with keys that should be ordered before the provided value using the comparator for the database container.

`-k | --minKeyValue {minKeyValue}`

Only show records with keys that should be ordered after the provided value using the comparator for the database container.

`-X | --maxHexKeyValue {maxKeyValue}`

Only show records with keys that should be ordered before the provided value using the comparator for the database container.

`-x | --minHexKeyValue {minKeyValue}`

Only show records with keys that should be ordered after the provided value using the comparator for the database container.

`-S | --maxDataSize {maxDataSize}`

Only show records whose data is no larger than the provided value.

Default: -1

`-s | --minDataSize {minDataSize}`

Only show records whose data is no smaller than the provided value.

Default: -1

`-p | --skipDecode`

Do not try to decode backend data to their appropriate types.

Default: false

backendstat dump-raw-db

Dump the raw records in hexadecimal format for a low-level database within the pluggable backend's storage engine. Depending on index size, this subcommand can generate lots of output.

Options

`-n | --backendID {backendName}`

The backend ID of the backend.

`-d | --dbName {databaseName}`

The raw database name.

`-q | --statsOnly`

Do not display backend data, just statistics.

Default: false

`-K | --maxKeyValue {maxKeyValue}`

Only show records with keys that should be ordered before the provided value using the comparator for the database container.

`-k | --minKeyValue {minKeyValue}`

Only show records with keys that should be ordered after the provided value using the comparator for the database container.

`-X | --maxHexKeyValue {maxKeyValue}`

Only show records with keys that should be ordered before the provided value using the comparator for the database container.

`-x | --minHexKeyValue {minKeyValue}`

Only show records with keys that should be ordered after the provided value using the comparator for the database container.

`-S | --maxDataSize {maxDataSize}`

Only show records whose data is no larger than the provided value.

Default: -1

`-s | --minDataSize {minDataSize}`

Only show records whose data is no smaller than the provided value.

Default: -1

`-l | --singleLine`

Write hexadecimal data on a single line instead of pretty format.

Default: false

backendstat list-backends

List the pluggable backends.

backendstat list-base-dns

List the base DNs in a backend.

Options

`-n | --backendID {backendName}`

The backend ID of the backend.

backendstat list-indexes

List the indexes associated with a pluggable backend. This subcommand may take a long time to complete depending on the size of the backend.

Options

`-n | --backendID {backendName}`

The backend ID of the backend.

`-b | --baseDN {baseDN}`

The base DN within the backend.

backendstat list-raw-dbs

List the low-level databases within a pluggable backend's storage engine. This subcommand may take a long time to complete depending on the size of the backend.

Options

`-n | --backendID {backendName}`

The backend ID of the backend.

`-u | --useSIUnits`

Uses SI Units for printing sizes.

Default: false

backendstat show-index-status

Shows the status of indexes for a backend base DN. This subcommand can take a long time to complete, as it reads all indexes for all backends.

<xinclude:include href="variablelist-backendstat-index-status.xml" />

Options

`-n | --backendID {backendName}`

The backend ID of the backend.

`-b | --baseDN {baseDN}`

The base DN within the backend.

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following example displays index information.

```
$ bin/backendstat dump-index  -n userRoot -b dc=example,dc=com -i id2childrencount

    Key (len 2): 1#52
    Value (len 8): 1
    Key (len 2): 2#52
    Value (len 8): 500000
    Key (len 9): Total Children Count
    Value (len 8): 500001

    Total Records: 3
    Total / Average Key Size: 13 bytes / 4 bytes
    Total / Average Data Size: 24 bytes / 8 bytes
```

backup(1)

Name

backup - back up OpenDJ directory data

Synopsis

`backup`

Description

This utility can be used to back up one or more Directory Server backends.

Options

The `backup` command takes the following options:

Command options:

`-a | --backUpAll`

Back up all backends in the server.

Default: false

`-A | --hash`

Generate a hash of the backup contents.

Default: false

`-B | --incrementalBaseID {backupID}`

Backup ID of the source archive for an incremental backup.

`-c | --compress`

Compress the backup contents.

Default: false

`-d | --backupDirectory {backupDir}`

Path to the target directory for the backup file(s).

`-i | --incremental`

Perform an incremental backup rather than a full backup.

Default: false

`-I | --backupID {backupID}`

Use the provided identifier for the backup.

`-n | --backendID {backendName}`

Backend ID for the backend to archive.

`--offline`

Indicates that the command must be run in offline mode.

Default: false

`-s | --signHash`

Sign the hash of the backup contents.

Default: false

`-y | --encrypt`

Encrypt the backup contents.

Default: false

Task Backend Connection Options

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Task Scheduling Options

`--completionNotify {emailAddress}`

Email address of a recipient to be notified when the task completes. This option may be specified more than once.

`--dependency {taskID}`

ID of a task upon which this task depends. A task will not start execution until all its dependencies have completed execution.

`--errorNotify {emailAddress}`

Email address of a recipient to be notified if an error occurs when this task executes. This option may be specified more than once.

`--failedDependencyAction {action}`

Action this task will take should one if its dependent tasks fail. The value must be one of PROCESS,CANCEL,DISABLE. If not specified defaults to CANCEL.

`--recurringTask {schedulePattern}`

Indicates the task is recurring and will be scheduled according to the value argument expressed in crontab(5) compatible time/date pattern.

`-t | --start {startTime}`

Indicates the date/time at which this operation will start when scheduled as a server task expressed in YYYYMMDDhhmmssZ format for UTC time or YYYYMMDDhhmmss for local time. A value of '0' will cause the task to be scheduled for immediate execution. When this option is specified the operation will be scheduled to start at the specified time after which this utility will exit immediately.

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

1

An error occurred.

Examples

The following example backs up all user data while the server is online.

```
$ backup -p 4444 -D "cn=Directory Manager" -w password \
 -a -d /path/to/opendj/bak -t 0
Backup task 20110613143801866 scheduled to start ...
```

The following example schedules back up of all user data every night at 2 AM when the server is online, and notifies diradmin@example.com when finished, or on error.

```
$ backup -p 4444 -D "cn=Directory Manager" -w password -a \
 -d /path/to/opendj/bak --recurringTask "00 02 * * *" \
 --completionNotify diradmin@example.com --errorNotify diradmin@example.com
Recurring Backup task BackupTask-988d6adf-4d65-44bf-8546-6ea74a2480b0
scheduled successfully
```

The following example backs up all user data while the server is offline.

```
$ stop-ds
Stopping Server...
...

$ backup --backupAll --backupDirectory /path/to/opendj/bak
... msg=The backup process completed successfully

$ start-ds
... The Directory Server has started successfully
```

base64(1)

Name

base64 - encode and decode base64 strings

Synopsis

`base64 {subcommand} {options}`

Description

This utility can be used to encode and decode information using base64.

Options

The `base64` command takes the following options:

`-V | --version`
: Display Directory Server version information.

  Default: false

`-H | --help`
: Display this usage information.

  Default: false

Subcommands

The `base64` command supports the following subcommands:

base64 decode

Decode base64-encoded information into raw data. When no options are specified, this subcommand reads from standard input and writes to standard output.

Options

`-d | --encodedData {data}`
: The base64-encoded data to be decoded.

`-f | --encodedDataFile {path}`
: The path to a file containing the base64-encoded data to be decoded.

`-o | --toRawFile {path}`

The path to a file to which the raw base64-decoded data should be written.

base64 encode

Encode raw data using base64. When no options are specified, this subcommand reads from standard input and writes to standard output.

Options

`-d | --rawData {data}`

The raw data to be base64 encoded.

`-f | --rawDataFile {path}`

The path to a file containing the raw data to be base64 encoded.

`-o | --toEncodedFile {path}`

The path to a file to which the base64-encoded data should be written.

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following command shows the changes from the external change log in human-readable format.

```
$ base64 decode -d YWRkOiBkZXNjcmlwdGlvbgpkZXNjcmlwdGlvbjogQSB0aGlyZCBjaGFuZ2UK\
LQpyZXBsYWNlOiBtb2RpZmllcnNOYW1lCm1vZGlmaWVyc05hbWU6IGNuPURpcmVjdG9yeSBNYW5hZ2V\
yLGNuPVJvb3QgRE5zLGNuPWNvbmZpZwotCnJlcGxhY2U6IG1vZGlmeVRpbWVzdGFtcAptb2RpZnlUaW\
1lc3RhbXA6IDIwMTEwNjEzMDcxMjEwWgotCg==
add: description
description: A third change
-
replace: modifiersName
modifiersName: cn=Directory Manager,cn=Root DNs,cn=config
-
replace: modifyTimestamp
modifyTimestamp: 20110613071210Z
-
```

control-panel(1)

Name

control-panel - start the OpenDJ graphical admin interface

Synopsis

`control-panel`

Description

This utility can be used to display the Control Panel window which displays basic server information and allows to do some basic administration tasks on the server.

If no host name or port is provided, the tool will try to connect to the local server.

Options

The `control-panel` command takes the following options:

Command options:

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-r | --remote`

Connect to a remote server.

Default: false

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following example starts the Control Panel on a remote host.

```
$ control-panel -r -h opendj.example.com -p 4444 &
```

create-rc-script(1)

Name

create-rc-script - script to manage OpenDJ as a service on UNIX

Synopsis

`create-rc-script`

Description

Create an RC script that may be used to start, stop, and restart the Directory Server on UNIX-based systems.

Options

The `create-rc-script` command takes the following options:

Command options:

`-f | --outputFile {path}`

The path to the output file to create.

`-j | --javaHome {path}`

The path to the Java installation that should be used to run the server.

`-J | --javaArgs {args}`

A set of arguments that should be passed to the JVM when running the server.

`-u | --userName {userName}`

The name of the user account under which the server should run.

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following example adds a script to start OpenDJ at boot time on a Debian-based system, and then updates the runlevel system to use the script.

```
$ sudo create-rc-script -f /etc/init.d/opendj -u opendj-user
$ sudo update-rc.d opendj
```

dsconfig(1)

Name

dsconfig - manage OpenDJ directory server configuration

Synopsis

`dsconfig {subcommand} {options}`

Description

This utility can be used to define a base configuration for the Directory Server.

The `dsconfig` command is the primary command-line tool for viewing and editing OpenDJ configuration. When started without arguments, `dsconfig` prompts you for administration connection information, including the host name, administration port number, administrator bind DN and administrator password. The `dsconfig` command then connects securely to the directory server over the administration port. Once connected it presents you with a menu-driven interface to the server configuration.

When you pass connection information, subcommands, and additional options to `dsconfig`, the command runs in script mode and so is not interactive, though it can prompt you to ask whether to apply changes and whether to trust certificates (unless you use the `--no-prompt` and `--trustAll` options, respectively).

You can prepare `dsconfig` batch scripts by running the tool with the `--commandFilePath` option in interactive mode, then reading from the batch file with the `--batchFilePath` option in script mode. Batch files can be useful when you have many `dsconfig` commands to run and want to avoid starting the JVM for each command. Alternatively, you can read commands from standard input by using the `--batch` option.

The `dsconfig` command categorizes directory server configuration into *components*, also called *managed objects*. Actual components often inherit from a parent component type. For example, one component is a Connection Handler. An LDAP Connection Handler is a type of Connection Handler. You configure the LDAP Connection Handler component to specify how OpenDJ directory server handles LDAP connections coming from client applications.

Configuration components have *properties*. For example, the LDAP Connection Handler component has properties such as `listen-port` and `allow-start-tls`. You can set the component's `listen-port` property to `389` to use the default LDAP port number. You can set the component's `allow-start-tls` property to `true` to permit LDAP client applications to use StartTLS. Much of the configuration you do with `dsconfig` involves setting component properties.

Options

The `dsconfig` command takes the following options:

Command options:

`--batch`

Reads from standard input a set of commands to be executed.

Default: false

`--commandFilePath {path}`

The full path to the file where the equivalent non-interactive commands will be written when this command is run in interactive mode.

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`--displayCommand`

Display the equivalent non-interactive argument in the standard output when this command is run in interactive mode.

Default: false

`--help-all`

Display all subcommands.

Default: false

`--help-core-server`

Display subcommands relating to core server.

Default: false

`--help-database`

Display subcommands relating to caching and back-ends.

Default: false

`--help-logging`

Display subcommands relating to logging.

Default: false

`--help-replication`

Display subcommands relating to replication.

Default: false

`--help-security`

Display subcommands relating to authentication and authorization.

Default: false

`--help-service-discovery`

Display subcommands relating to service discovery mechanism.

Default: false

`--help-user-management`

Display subcommands relating to user management.

Default: false

Configuration Options

`--advanced`

Allows the configuration of advanced components and properties.

Default: false

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-E | --reportAuthzID`

Use the authorization identity control.

Default: false

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`--usePasswordPolicyControl`

Use the password policy request control.

Default: false

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Utility input/output options:

`-F | --batchFilePath {batchFilePath}`

Path to a batch file containing a set of commands to be executed.

`-n | --no-prompt`

Use non-interactive mode. If data in the command is missing, the user is not prompted and the tool will fail.

Default: false

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-Q | --quiet`

Use quiet mode.

Default: false

`-s | --script-friendly`

Use script-friendly mode.

Default: false

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Subcommands

The `dsconfig` command provides many subcommands.

Subcommands let you create, list, and delete entire configuration components, and also let you get and set component properties. Subcommands therefore have names that reflect these five actions.

- create-*component*
- list-*component*s
- delete-*component*
- get-*component*-prop
- set-*component*-prop

Here, *component* names are names of managed object types. Subcommand *component* names are lower-case, hyphenated versions of the friendly names. When you act on an actual configuration component, you provide the name of the component as an option argument. For example, the Log Publisher component has these corresponding subcommands.

- `create-log-publisher`
- `list-log-publishers`
- `delete-log-publisher`
- `get-log-publisher-prop`
- `set-log-publisher-prop`

When you create or delete Log Publisher components and when you get and set their configuration properties, you provide the name of the actual log publisher, which you can find by using the `list-log-publishers` subcommand.

```
$ dsconfig \
 list-log-publishers \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --trustAll

Log Publisher                 : Type                    : enabled
------------------------------:-------------------------:--------
File-Based Access Logger      : file-based-access       : true
File-Based Audit Logger       : file-based-audit        : false
File-Based Debug Logger       : file-based-debug        : false
File-Based Error Logger       : file-based-error        : true
File-Based HTTP Access Logger : file-based-http-access : false
Replication Repair Logger     : file-based-error        : true

$ dsconfig \
 get-log-publisher-prop \
 --publisher-name "File-Based Access Logger" \
 --property rotation-policy \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --trustAll
Property        : Value(s)
----------------:---------------------------------------------------------------
rotation-policy : 24 Hours Time Limit Rotation Policy, Size Limit Rotation
                : Policy
```

Many subcommands let you set property values. Notice in the reference for the subcommands below that specific options are available for handling multi-valued properties. Whereas you can assign a single property value by using the `--set` option, you assign multiple values to a multi-valued property by using the `--add` option. You can reset the values of the multi-valued property by using the `--reset` option. Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some

durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Use the following options to view help for subcommands.

`dsconfig --help-all`
: Display all subcommands

`dsconfig --help-core-server`
: Display subcommands relating to core server

`dsconfig --help-database`
: Display subcommands relating to caching and back-ends

`dsconfig --help-logging`
: Display subcommands relating to logging

`dsconfig --help-replication`
: Display subcommands relating to replication

`dsconfig --help-security`
: Display subcommands relating to authentication and authorization

`dsconfig --help-user-management`
: Display subcommands relating to user management

For help with individual subcommands, either use `dsconfig subcommand --help`, or start `dsconfig` in interactive mode, without specifying a subcommand.

To view all component properties, use the `dsconfig list-properties` command.

The `dsconfig` command supports the following subcommands:

- dsconfig create-access-log-filtering-criteria: Creates Access Log Filtering Criteria
- dsconfig create-account-status-notification-handler: Creates Account Status Notification Handlers
- dsconfig create-alert-handler: Creates Alert Handlers
- dsconfig create-backend: Creates Backends

- dsconfig create-backend-index: Creates Backend Indexes
- dsconfig create-backend-vlv-index: Creates Backend VLV Indexes
- dsconfig create-certificate-mapper: Creates Certificate Mappers
- dsconfig create-connection-handler: Creates Connection Handlers
- dsconfig create-debug-target: Creates Debug Targets
- dsconfig create-entry-cache: Creates Entry Caches
- dsconfig create-extended-operation-handler: Creates Extended Operation Handlers
- dsconfig create-group-implementation: Creates Group Implementations
- dsconfig create-http-authorization-mechanism: Creates HTTP Authorization Mechanisms
- dsconfig create-http-endpoint: Creates HTTP Endpoints
- dsconfig create-identity-mapper: Creates Identity Mappers
- dsconfig create-key-manager-provider: Creates Key Manager Providers
- dsconfig create-log-publisher: Creates Log Publishers
- dsconfig create-log-retention-policy: Creates Log Retention Policies
- dsconfig create-log-rotation-policy: Creates Log Rotation Policies
- dsconfig create-monitor-provider: Creates Monitor Providers
- dsconfig create-password-generator: Creates Password Generators
- dsconfig create-password-policy: Creates Authentication Policies
- dsconfig create-password-storage-scheme: Creates Password Storage Schemes
- dsconfig create-password-validator: Creates Password Validators
- dsconfig create-plugin: Creates Plugins
- dsconfig create-replication-domain: Creates Replication Domains
- dsconfig create-replication-server: Creates Replication Servers
- dsconfig create-sasl-mechanism-handler: Creates SASL Mechanism Handlers
- dsconfig create-schema-provider: Creates Schema Providers
- dsconfig create-service-discovery-mechanism: Creates Service Discovery Mechanisms
- dsconfig create-synchronization-provider: Creates Synchronization Providers
- dsconfig create-trust-manager-provider: Creates Trust Manager Providers
- dsconfig create-virtual-attribute: Creates Virtual Attributes
- dsconfig delete-access-log-filtering-criteria: Deletes Access Log Filtering Criteria
- dsconfig delete-account-status-notification-handler: Deletes Account Status Notification Handlers
- dsconfig delete-alert-handler: Deletes Alert Handlers
- dsconfig delete-backend: Deletes Backends
- dsconfig delete-backend-index: Deletes Backend Indexes

- dsconfig delete-backend-vlv-index: Deletes Backend VLV Indexes
- dsconfig delete-certificate-mapper: Deletes Certificate Mappers
- dsconfig delete-connection-handler: Deletes Connection Handlers
- dsconfig delete-debug-target: Deletes Debug Targets
- dsconfig delete-entry-cache: Deletes Entry Caches
- dsconfig delete-extended-operation-handler: Deletes Extended Operation Handlers
- dsconfig delete-group-implementation: Deletes Group Implementations
- dsconfig delete-http-authorization-mechanism: Deletes HTTP Authorization Mechanisms
- dsconfig delete-http-endpoint: Deletes HTTP Endpoints
- dsconfig delete-identity-mapper: Deletes Identity Mappers
- dsconfig delete-key-manager-provider: Deletes Key Manager Providers
- dsconfig delete-log-publisher: Deletes Log Publishers
- dsconfig delete-log-retention-policy: Deletes Log Retention Policies
- dsconfig delete-log-rotation-policy: Deletes Log Rotation Policies
- dsconfig delete-monitor-provider: Deletes Monitor Providers
- dsconfig delete-password-generator: Deletes Password Generators
- dsconfig delete-password-policy: Deletes Authentication Policies
- dsconfig delete-password-storage-scheme: Deletes Password Storage Schemes
- dsconfig delete-password-validator: Deletes Password Validators
- dsconfig delete-plugin: Deletes Plugins
- dsconfig delete-replication-domain: Deletes Replication Domains
- dsconfig delete-replication-server: Deletes Replication Servers
- dsconfig delete-sasl-mechanism-handler: Deletes SASL Mechanism Handlers
- dsconfig delete-schema-provider: Deletes Schema Providers
- dsconfig delete-service-discovery-mechanism: Deletes Service Discovery Mechanisms
- dsconfig delete-synchronization-provider: Deletes Synchronization Providers
- dsconfig delete-trust-manager-provider: Deletes Trust Manager Providers
- dsconfig delete-virtual-attribute: Deletes Virtual Attributes
- dsconfig get-access-control-handler-prop: Shows Access Control Handler properties
- dsconfig get-access-log-filtering-criteria-prop: Shows Access Log Filtering Criteria properties
- dsconfig get-account-status-notification-handler-prop: Shows Account Status Notification Handler properties
- dsconfig get-administration-connector-prop: Shows Administration Connector properties
- dsconfig get-alert-handler-prop: Shows Alert Handler properties
- dsconfig get-backend-index-prop: Shows Backend Index properties

- dsconfig get-backend-prop: Shows Backend properties
- dsconfig get-backend-vlv-index-prop: Shows Backend VLV Index properties
- dsconfig get-certificate-mapper-prop: Shows Certificate Mapper properties
- dsconfig get-connection-handler-prop: Shows Connection Handler properties
- dsconfig get-crypto-manager-prop: Shows Crypto Manager properties
- dsconfig get-debug-target-prop: Shows Debug Target properties
- dsconfig get-entry-cache-prop: Shows Entry Cache properties
- dsconfig get-extended-operation-handler-prop: Shows Extended Operation Handler properties
- dsconfig get-external-changelog-domain-prop: Shows External Changelog Domain properties
- dsconfig get-global-configuration-prop: Shows Global Configuration properties
- dsconfig get-group-implementation-prop: Shows Group Implementation properties
- dsconfig get-http-authorization-mechanism-prop: Shows HTTP Authorization Mechanism properties
- dsconfig get-http-endpoint-prop: Shows HTTP Endpoint properties
- dsconfig get-identity-mapper-prop: Shows Identity Mapper properties
- dsconfig get-key-manager-provider-prop: Shows Key Manager Provider properties
- dsconfig get-log-publisher-prop: Shows Log Publisher properties
- dsconfig get-log-retention-policy-prop: Shows Log Retention Policy properties
- dsconfig get-log-rotation-policy-prop: Shows Log Rotation Policy properties
- dsconfig get-monitor-provider-prop: Shows Monitor Provider properties
- dsconfig get-password-generator-prop: Shows Password Generator properties
- dsconfig get-password-policy-prop: Shows Authentication Policy properties
- dsconfig get-password-storage-scheme-prop: Shows Password Storage Scheme properties
- dsconfig get-password-validator-prop: Shows Password Validator properties
- dsconfig get-plugin-prop: Shows Plugin properties
- dsconfig get-plugin-root-prop: Shows Plugin Root properties
- dsconfig get-replication-domain-prop: Shows Replication Domain properties
- dsconfig get-replication-server-prop: Shows Replication Server properties
- dsconfig get-root-dn-prop: Shows Root DN properties
- dsconfig get-root-dse-backend-prop: Shows Root DSE Backend properties
- dsconfig get-sasl-mechanism-handler-prop: Shows SASL Mechanism Handler properties
- dsconfig get-schema-provider-prop: Shows Schema Provider properties
- dsconfig get-service-discovery-mechanism-prop: Shows Service Discovery Mechanism properties
- dsconfig get-synchronization-provider-prop: Shows Synchronization Provider properties

- dsconfig get-trust-manager-provider-prop: Shows Trust Manager Provider properties
- dsconfig get-virtual-attribute-prop: Shows Virtual Attribute properties
- dsconfig get-work-queue-prop: Shows Work Queue properties
- dsconfig list-access-log-filtering-criteria: Lists existing Access Log Filtering Criteria
- dsconfig list-account-status-notification-handlers: Lists existing Account Status Notification Handlers
- dsconfig list-alert-handlers: Lists existing Alert Handlers
- dsconfig list-backend-indexes: Lists existing Backend Indexes
- dsconfig list-backend-vlv-indexes: Lists existing Backend VLV Indexes
- dsconfig list-backends: Lists existing Backends
- dsconfig list-certificate-mappers: Lists existing Certificate Mappers
- dsconfig list-connection-handlers: Lists existing Connection Handlers
- dsconfig list-debug-targets: Lists existing Debug Targets
- dsconfig list-entry-caches: Lists existing Entry Caches
- dsconfig list-extended-operation-handlers: Lists existing Extended Operation Handlers
- dsconfig list-group-implementations: Lists existing Group Implementations
- dsconfig list-http-authorization-mechanisms: Lists existing HTTP Authorization Mechanisms
- dsconfig list-http-endpoints: Lists existing HTTP Endpoints
- dsconfig list-identity-mappers: Lists existing Identity Mappers
- dsconfig list-key-manager-providers: Lists existing Key Manager Providers
- dsconfig list-log-publishers: Lists existing Log Publishers
- dsconfig list-log-retention-policies: Lists existing Log Retention Policies
- dsconfig list-log-rotation-policies: Lists existing Log Rotation Policies
- dsconfig list-monitor-providers: Lists existing Monitor Providers
- dsconfig list-password-generators: Lists existing Password Generators
- dsconfig list-password-policies: Lists existing Password Policies
- dsconfig list-password-storage-schemes: Lists existing Password Storage Schemes
- dsconfig list-password-validators: Lists existing Password Validators
- dsconfig list-plugins: Lists existing Plugins
- dsconfig list-properties: Describes managed objects and their properties
- dsconfig list-replication-domains: Lists existing Replication Domains
- dsconfig list-replication-server: Lists existing Replication Server
- dsconfig list-sasl-mechanism-handlers: Lists existing SASL Mechanism Handlers
- dsconfig list-schema-providers: Lists existing Schema Providers
- dsconfig list-service-discovery-mechanisms: Lists existing Service Discovery Mechanisms

- dsconfig list-synchronization-providers: Lists existing Synchronization Providers
- dsconfig list-trust-manager-providers: Lists existing Trust Manager Providers
- dsconfig list-virtual-attributes: Lists existing Virtual Attributes
- dsconfig set-access-control-handler-prop: Modifies Access Control Handler properties
- dsconfig set-access-log-filtering-criteria-prop: Modifies Access Log Filtering Criteria properties
- dsconfig set-account-status-notification-handler-prop: Modifies Account Status Notification Handler properties
- dsconfig set-administration-connector-prop: Modifies Administration Connector properties
- dsconfig set-alert-handler-prop: Modifies Alert Handler properties
- dsconfig set-backend-index-prop: Modifies Backend Index properties
- dsconfig set-backend-prop: Modifies Backend properties
- dsconfig set-backend-vlv-index-prop: Modifies Backend VLV Index properties
- dsconfig set-certificate-mapper-prop: Modifies Certificate Mapper properties
- dsconfig set-connection-handler-prop: Modifies Connection Handler properties
- dsconfig set-crypto-manager-prop: Modifies Crypto Manager properties
- dsconfig set-debug-target-prop: Modifies Debug Target properties
- dsconfig set-entry-cache-prop: Modifies Entry Cache properties
- dsconfig set-extended-operation-handler-prop: Modifies Extended Operation Handler properties
- dsconfig set-external-changelog-domain-prop: Modifies External Changelog Domain properties
- dsconfig set-global-configuration-prop: Modifies Global Configuration properties
- dsconfig set-group-implementation-prop: Modifies Group Implementation properties
- dsconfig set-http-authorization-mechanism-prop: Modifies HTTP Authorization Mechanism properties
- dsconfig set-http-endpoint-prop: Modifies HTTP Endpoint properties
- dsconfig set-identity-mapper-prop: Modifies Identity Mapper properties
- dsconfig set-key-manager-provider-prop: Modifies Key Manager Provider properties
- dsconfig set-log-publisher-prop: Modifies Log Publisher properties
- dsconfig set-log-retention-policy-prop: Modifies Log Retention Policy properties
- dsconfig set-log-rotation-policy-prop: Modifies Log Rotation Policy properties
- dsconfig set-monitor-provider-prop: Modifies Monitor Provider properties
- dsconfig set-password-generator-prop: Modifies Password Generator properties
- dsconfig set-password-policy-prop: Modifies Authentication Policy properties
- dsconfig set-password-storage-scheme-prop: Modifies Password Storage Scheme properties
- dsconfig set-password-validator-prop: Modifies Password Validator properties
- dsconfig set-plugin-prop: Modifies Plugin properties

- dsconfig set-plugin-root-prop: Modifies Plugin Root properties
- dsconfig set-replication-domain-prop: Modifies Replication Domain properties
- dsconfig set-replication-server-prop: Modifies Replication Server properties
- dsconfig set-root-dn-prop: Modifies Root DN properties
- dsconfig set-root-dse-backend-prop: Modifies Root DSE Backend properties
- dsconfig set-sasl-mechanism-handler-prop: Modifies SASL Mechanism Handler properties
- dsconfig set-schema-provider-prop: Modifies Schema Provider properties
- dsconfig set-service-discovery-mechanism-prop: Modifies Service Discovery Mechanism properties
- dsconfig set-synchronization-provider-prop: Modifies Synchronization Provider properties
- dsconfig set-trust-manager-provider-prop: Modifies Trust Manager Provider properties
- dsconfig set-virtual-attribute-prop: Modifies Virtual Attribute properties
- dsconfig set-work-queue-prop: Modifies Work Queue properties

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

Much of the *OpenDJ Administration Guide* consists of `dsconfig` examples with text in between. This section therefore remains short.

The following example starts `dsconfig` in interactive, menu-driven mode on the default port of the current host.

```
$ dsconfig -h opendj.example.com -p 4444 -D "cn=Directory Manager" -w password

>>>> OpenDJ configuration console main menu

What do you want to configure?

    1)   Access Control Handler               23)  Log Publisher
    2)   Access Log Filtering Criteria        24)  Log Retention Policy
    3)   Account Status Notification Handler  25)  Log Rotation Policy
    4)   Administration Connector             26)  Matching Rule
    5)   Alert Handler                        27)  Monitor Provider
    6)   Attribute Syntax                     28)  Password Generator
    7)   Backend                              29)  Password Policy
```

```
    8)   Backend Index                          30)  Password Storage Scheme
    9)   Backend VLV Index                      31)  Password Validator
    10)  Certificate Mapper                     32)  Plugin
    11)  Connection Handler                     33)  Plugin Root
    12)  Crypto Manager                         34)  Replication Domain
    13)  Debug Target                           35)  Replication Server
    14)  Entry Cache                            36)  Root DN
    15)  Extended Operation Handler             37)  Root DSE Backend
    16)  External Changelog Domain              38)  SASL Mechanism Handler
    17)  Global Configuration                   39)  Schema Provider
    18)  Group Implementation                   40)  Synchronization Provider
    19)  HTTP Authorization Mechanism           41)  Trust Manager Provider
    20)  HTTP Endpoint                          42)  Virtual Attribute
    21)  Identity Mapper                        43)  Work Queue
    22)  Key Manager Provider

    q)   quit

Enter choice:
```

The following example demonstrates generating a batch file that corresponds to an interactive session enabling the debug log. The example then demonstrates using a modified batch file to disable the debug log.

```
$ dsconfig \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --commandFilePath ~/enable-debug-log.batch
 ...
$ cat ~/enable-debug-log.batch
# dsconfig session start date: 19/Oct/2011:08:52:22 +0000

# Session operation number: 1
# Operation date: 19/Oct/2011:08:55:06 +0000
dsconfig set-log-publisher-prop \
          --publisher-name File-Based\ Debug\ Logger \
          --set enabled:true \
          --hostname opendj.example.com \
          --port 4444 \
          --trustStorePath /path/to/opendj/config/admin-truststore \
          --bindDN cn=Directory\ Manager \
          --bindPassword ****** \
          --no-prompt

$ cp ~/enable-debug-log.batch ~/disable-debug-log.batch
$ vi ~/disable-debug-log.batch
$ cat ~/disable-debug-log.batch
set-log-publisher-prop \
```

```
          --publisher-name File-Based\ Debug\ Logger \
          --set enabled:false \
          --hostname opendj.example.com \
          --port 4444 \
          --trustStorePath /path/to/opendj/config/admin-truststore \
          --bindDN cn=Directory\ Manager \
          --bindPassword password \
          --no-prompt

$ dsconfig --batchFilePath ~/disable-debug-log.batch --no-prompt
set-log-publisher-prop
--publisher-name
File-Based Debug Logger
--set
enabled:false
--hostname
opendj.example.com
--port
4444
--trustStorePath
/path/to/opendj/config/admin-truststore
--bindDN
cn=Directory Manager
--bindPassword
password
--no-prompt

$
```

Notice that the original command file looks like a shell script with the bind password value replaced by asterisks. To pass the content as a batch file to `dsconfig`, strip `dsconfig` itself, and include t he bind password for the administrative user or replace that option with an alternative, such as reading the password from a file.

dsjavaproperties(1)

Name

dsjavaproperties - apply OpenDJ Java home and JVM settings

Synopsis

`dsjavaproperties`

Description

This utility can be used to change the java arguments and java home that are used by the different server commands.

Before launching the command, edit the properties file located in /path/to/opendj/config/java.properties to specify the java arguments and java home. When you have edited the properties file, run this command for the changes to be taken into account.

Note that the changes will only apply to this server installation. No modifications will be made to your environment variables.

Options

The `dsjavaproperties` command takes the following options:

Utility input/output options:

`-Q | --quiet`

Use quiet mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Files

This command depends on the content of the `config/java.properties` file.

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following example demonstrates a successful run.

```
$ dsjavaproperties
The operation was successful.  The server commands will use the java arguments
 and java home specified in the properties file located in
 /path/to/opendj/config/java.properties
```

dsreplication(1)

Name

dsreplication - manage OpenDJ directory data replication

Synopsis

`dsreplication {subcommand} {options}`

Description

This utility can be used to configure replication between servers so that the data of the servers is synchronized. For replication to work you must first enable replication using the 'enable' subcommand and then initialize the contents of one of the servers with the contents of the other using the 'initialize' subcommand.

Options

The `dsreplication` command takes the following options:

Command options:

`-b | --baseDN {baseDN}`

Base DN of the data to be replicated, initialized or for which we want to disable replication. Multiple base DNs can be provided by using this option multiple times.

`--commandFilePath {path}`

The full path to the file where the equivalent non-interactive commands will be written when this command is run in interactive mode.

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`--displayCommand`

Display the equivalent non-interactive argument in the standard output when this command is run in interactive mode.

Default: false

`-j | --adminPasswordFile {bindPasswordFile}`

The file containing the password of the global administrator.

`-w | --adminPassword {bindPassword}`

The global administrator password.

Configuration Options

`--advanced`

Allows the configuration of advanced components and properties.

Default: false

LDAP connection options:

`-I | --adminUID {adminUID}`

User ID of the Global Administrator to use to bind to the server. For the 'enable' subcommand if no Global Administrator was defined previously for none of the server the Global Administrator will be created using the provided data.

Default: admin

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Utility input/output options:

`-n | --no-prompt`

Use non-interactive mode. If data in the command is missing, the user is not prompted and the tool will fail.

Default: false

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-Q | --quiet`

Use quiet mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Subcommands

The `dsreplication` command supports the following subcommands:

dsreplication disable

Disables replication on the specified server for the provided base DN and removes references in the other servers with which it is replicating data.

Options

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-D | --bindDN {bindDN}`

DN to use to bind to the server where we want to disable replication. This option must be used when no Global Administrator has been defined on the server or if the user does not want to remove references in the other replicated servers. The password provided for the Global Administrator will be used when specifying this option.

Default: cn=Directory Manager

`-a | --disableReplicationServer`

Disable the replication server. The replication port and change log are disabled on the specified server.

Default: false

`--disableAll`

Disable the replication configuration on the specified server. The contents of the server are no longer replicated and the replication server (changelog and replication port) is disabled if it is configured.

Default: false

dsreplication enable

Updates the configuration of the servers to replicate the data under the specified base DN. If one of the specified servers is already replicating the data under the base DN with other servers, executing this subcommand will update the configuration of all the servers (so it is sufficient to execute the command line once for each server we add to the replication topology).

Options

`-h | --host1 {host}`

Fully qualified host name or IP address of the first server whose contents will be replicated.

Default: localhost.localdomain

`-p | --port1 {port}`

Directory server administration port number of the first server whose contents will be replicated.

Default: 4444

`-D | --bindDN1 {bindDN}`

DN to use to bind to the first server whose contents will be replicated. If not specified the global administrator will be used to bind.

Default: cn=Directory Manager

`--bindPassword1 {bindPassword}`

Password to use to bind to the first server whose contents will be replicated. If no bind DN was specified for the first server the password of the global administrator will be used to bind.

`--bindPasswordFile1 {bindPasswordFile}`

File containing the password to use to bind to the first server whose contents will be replicated. If no bind DN was specified for the first server the password of the global administrator will be used to bind.

`-r | --replicationPort1 {port}`

Port that will be used by the replication mechanism in the first server to communicate with the other servers. You have to specify this option only if replication was not previously configured in the first server.

Default: 8989

`--secureReplication1`

Specifies whether the communication through the replication port of the first server is encrypted or not. This option will only be taken into account the first time replication is configured on the first server.

Default: false

`--noReplicationServer1`

Do not configure a replication port or change log on the first server. The first server will contain replicated data but will not contain a change log of modifications made to the replicated data. Note that each replicated topology must contain at least two servers with a change log to avoid a single point of failure.

Default: false

`--onlyReplicationServer1`

Configure only a change log and replication port on the first server. The first server will not contain replicated data, but will contain a change log of the modifications made to the replicated data on other servers.

Default: false

`-O | --host2 {host}`

Fully qualified host name or IP address of the second server whose contents will be replicated.

Default: localhost.localdomain

`--port2 {port}`

Directory server administration port number of the second server whose contents will be replicated.

Default: 4444

`--bindDN2 {bindDN}`

DN to use to bind to the second server whose contents will be replicated. If not specified the global administrator will be used to bind.

Default: cn=Directory Manager

`--bindPassword2 {bindPassword}`

Password to use to bind to the second server whose contents will be replicated. If no bind DN was specified for the second server the password of the global administrator will be used to bind.

`-F | --bindPasswordFile2 {bindPasswordFile}`

File containing the password to use to bind to the second server whose contents will be replicated. If no bind DN was specified for the second server the password of the global administrator will be used to bind.

`-R | --replicationPort2 {port}`

Port that will be used by the replication mechanism in the second server to communicate with the other servers. You have to specify this option only if replication was not previously configured in the second server.

Default: 8989

`--secureReplication2`

Specifies whether the communication through the replication port of the second server is encrypted or not. This option will only be taken into account the first time replication is configured on the second server.

Default: false

`--noReplicationServer2`

Do not configure a replication port or change log on the second server. The second server will contain replicated data but will not contain a change log of modifications made to the replicated data. Note that each replicated topology must contain at least two servers with a change log to avoid a single point of failure.

Default: false

`--onlyReplicationServer2`

Configure only a change log and replication port on the second server. The second server will not contain replicated data, but will contain a change log of the modifications made to the replicated data on other servers.

Default: false

`-S | --skipPortCheck`

Skip the check to determine whether the specified replication ports are usable.

Default: false

`--noSchemaReplication`

Do not replicate the schema between the servers.

Default: false

`--useSecondServerAsSchemaSource`

Use the second server to initialize the schema of the first server. If this option nor option --noSchemaReplication are specified the schema of the first server will be used to initialize the schema of the second server.

Default: false

dsreplication initialize

Initialize the contents of the data under the specified base DN on the destination server with the contents on the source server. This operation is required after enabling replication in order replication to work ('initialize-all' can also be used for this purpose).

Options

`-h | --hostSource {host}`

Fully qualified host name or IP address of the source server whose contents will be used to initialize the destination server.

Default: localhost.localdomain

`-p | --portSource {port}`

Directory server administration port number of the source server whose contents will be used to initialize the destination server.

Default: 4444

`-O | --hostDestination {host}`

Fully qualified host name or IP address of the destination server whose contents will be initialized.

Default: localhost.localdomain

`--portDestination {port}`

Directory server administration port number of the destination server whose contents will be initialized.

Default: 4444

dsreplication initialize-all

Initialize the contents of the data under the specified base DN on all the servers whose contents are being replicated with the contents on the specified server. This operation is required after enabling

replication for replication to work ('initialize' applied to each server can also be used for this purpose).

Options

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-p | --port {port}`

Directory server administration port number.

Default: 4444

dsreplication post-external-initialization

This subcommand must be called after initializing the contents of all the replicated servers using the tool import-ldif or the binary copy method. You must specify the list of base DNs that have been initialized and you must provide the credentials of any of the servers that are being replicated. See the usage of the subcommand 'pre-external-initialization' for more information.

Options

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-p | --port {port}`

Directory server administration port number.

Default: 4444

dsreplication pre-external-initialization

This subcommand must be called before initializing the contents of all the replicated servers using the tool import-ldif or the binary copy method. You must specify the list of base DNs that will be initialized and you must provide the credentials of any of the servers that are being replicated. After calling this subcommand, initialize the contents of all the servers in the topology (use the same LDIF file/binary copy on each of the servers), then call the subcommand 'post-external-initialization'.

Options

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed

certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-p | --port {port}`

Directory server administration port number.

Default: 4444

dsreplication purge-historical

Launches a purge processing of the historical informations stored in the user entries by replication. Since this processing may take a while, you must specify the maximum duration for this processing.

Options

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`--maximumDuration {maximum duration}`

This argument specifies the maximum duration the purge processing must last expressed in seconds.

Default: 3600

`-t | --start {startTime}`

Indicates the date/time at which this operation will start when scheduled as a server task expressed in YYYYMMDDhhmmssZ format for UTC time or YYYYMMDDhhmmss for local time. A value of '0' will cause the task to be scheduled for immediate execution. When this option is specified the operation will be scheduled to start at the specified time after which this utility will exit immediately.

`--recurringTask {schedulePattern}`

Indicates the task is recurring and will be scheduled according to the value argument expressed in crontab(5) compatible time/date pattern.

`--completionNotify {emailAddress}`

Email address of a recipient to be notified when the task completes. This option may be specified more than once.

`--errorNotify {emailAddress}`

Email address of a recipient to be notified if an error occurs when this task executes. This option may be specified more than once.

`--dependency {taskID}`

ID of a task upon which this task depends. A task will not start execution until all its dependencies have completed execution.

`--failedDependencyAction {action}`

Action this task will take should one if its dependent tasks fail. The value must be one of PROCESS,CANCEL,DISABLE. If not specified defaults to CANCEL.

dsreplication reset-change-number

Re-synchronizes the change-log changenumber on one server with the change-log changenumber of another.

Options

`-h | --hostSource {host}`

Fully qualified host name or IP address of the source server whose contents will be used to initialize the destination server.

Default: localhost.localdomain

`-p | --portSource {port}`

Directory server administration port number of the source server whose contents will be used to initialize the destination server.

Default: 4444

`-O | --hostDestination {host}`

Fully qualified host name or IP address of the destination server whose contents will be initialized.

Default: localhost.localdomain

`--portDestination {port}`

Directory server administration port number of the destination server whose contents will be initialized.

Default: 4444

`--change-number {change number}`

The change number to use as the basis for re-synchronization.

dsreplication status

Displays a list with the basic replication configuration of the base DNs of the servers defined in the

registration information. If no base DNs are specified as parameter the information for all base DNs is displayed.

Options

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-s | --script-friendly`

Use script-friendly mode.

Default: false

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following example enables and then initializes replication for a new replica on `opendj2.example.com` from an existing replica on `opendj.example.com`.

```
$ dsreplication enable -I admin -w password -X -n -b dc=example,dc=com \
 --host1 opendj.example.com --port1 4444 --bindDN1 "cn=Directory Manager" \
 --bindPassword1 password --replicationPort1 8989 \
 --host2 opendj2.example.com --port2 4444 --bindDN2 "cn=Directory Manager" \
 --bindPassword2 password --replicationPort2 8989

Establishing connections ..... Done.
Checking registration information ..... Done.
Updating remote references on server opendj.example.com:4444 ..... Done.
Configuring Replication port on server opendj2.example.com:4444 ..... Done.
Updating replication configuration for baseDN dc=example,dc=com on server
 opendj.example.com:4444 ..... Done.
Updating replication configuration for baseDN dc=example,dc=com on server
 opendj2.example.com:4444 ..... Done.
```

```
Updating registration configuration on server
 opendj.example.com:4444 ..... Done.
Updating registration configuration on server
 opendj2.example.com:4444 ..... Done.
Updating replication configuration for baseDN cn=schema on server
 opendj.example.com:4444 ..... Done.
Updating replication configuration for baseDN cn=schema on server
 opendj2.example.com:4444 ..... Done.
Initializing registration information on server opendj2.example.com:4444 with
 the contents of server opendj.example.com:4444 ..... Done.
Initializing schema on server opendj2.example.com:4444 with the contents of
 server opendj.example.com:4444 ..... Done.

Replication has been successfully enabled.  Note that for replication to
 work you must initialize the contents of the base DN's that are being
  replicated (use dsreplication initialize to do so).

See
/var/.../opends-replication-7958637258600693490.log
for a detailed log of this operation.

$ dsreplication initialize-all -I admin -w password -X -n -b dc=example,dc=com \
 -h opendj.example.com -p 4444

Initializing base DN dc=example,dc=com with the contents from
 opendj.example.com:4444: 160 entries processed (100 % complete).
Base DN initialized successfully.

See
/var/.../opends-replication-5020375834904394170.log
for a detailed log of this operation.
```

encode-password(1)

Name

encode-password - encode a password with an OpenDJ storage scheme

Synopsis

`encode-password`

Description

This utility can be used to encode user passwords with a specified storage scheme, or to determine whether a given clear-text value matches a provided encoded password.

Options

The `encode-password` command takes the following options:

Command options:

`-a | --authPasswordSyntax`

Use the authentication password syntax rather than the user password syntax.

Default: false

`-c | --clearPassword {clearPW}`

Clear-text password to encode or to compare against an encoded password.

`-e | --encodedPassword {encodedPW}`

Encoded password to compare against the clear-text password.

`-E | --encodedPasswordFile {file}`

Encoded password file.

`-f | --clearPasswordFile {file}`

Clear-text password file.

`-i | --interactivePassword`

The password to encode or to compare against an encoded password is interactively asked to the user.

Default: false

`-l | --listSchemes`

List available password storage schemes.

Default: false

`-r | --useCompareResultCode`

Use the LDAP compare result as an exit code for the password comparison.

Default: false

`-s | --storageScheme {scheme}`

Scheme to use for the encoded password.

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

5

The `-r` option was used, and the compare did not match.

6

The `-r` option was used, and the compare did match.

other

An error occurred.

Examples

The following example encodes a password, and also shows comparison of a password with the encoded value.

```
$ encode-password -l
3DES
AES
BASE64
BLOWFISH
CLEAR
CRYPT
MD5
RC4
SHA
```

```
SMD5
SSHA
SSHA256
SSHA384
SSHA512

$ encode-password -c secret12 -s CRYPT
Encoded Password:  "{CRYPT}ZulJ6Dy3TFnrE"

$ encode-password -c secret12 -s CRYPT -e "{CRYPT}ZulJ6Dy3TFnrE" -r
The provided clear-text and encoded passwords match

$ echo $?
6
```

export-ldif(1)

Name

export-ldif - export OpenDJ directory data in LDIF

Synopsis

`export-ldif`

Description

This utility can be used to export data from a Directory Server backend in LDIF form.

Options

The `export-ldif` command takes the following options:

Command options:

`-a | --appendToLDIF`

Append an existing LDIF file rather than overwriting it.

Default: false

`-b | --includeBranch {branchDN}`

Base DN of a branch to include in the LDIF export.

`-B | --excludeBranch {branchDN}`

Base DN of a branch to exclude from the LDIF export.

`-c | --compress`

Compress the LDIF data as it is exported.

Default: false

`-e | --excludeAttribute {attribute}`

Attribute to exclude from the LDIF export.

`-E | --excludeFilter {filter}`

Filter to identify entries to exclude from the LDIF export.

`-i | --includeAttribute {attribute}`

Attribute to include in the LDIF export.

`-I | --includeFilter {filter}`

Filter to identify entries to include in the LDIF export.

`-l | --ldifFile {ldifFile}`

Path to the LDIF file to be written.

`-n | --backendID {backendName}`

Backend ID for the backend to export.

`-O | --excludeOperational`

Exclude operational attributes from the LDIF export.

Default: false

`--offline`

Indicates that the command must be run in offline mode.

Default: false

Task Backend Connection Options

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Task Scheduling Options

`--completionNotify {emailAddress}`

Email address of a recipient to be notified when the task completes. This option may be specified more than once.

`--dependency {taskID}`

ID of a task upon which this task depends. A task will not start execution until all its dependencies have completed execution.

`--errorNotify {emailAddress}`

Email address of a recipient to be notified if an error occurs when this task executes. This option may be specified more than once.

`--failedDependencyAction {action}`

Action this task will take should one if its dependent tasks fail. The value must be one of PROCESS,CANCEL,DISABLE. If not specified defaults to CANCEL.

`--recurringTask {schedulePattern}`

Indicates the task is recurring and will be scheduled according to the value argument expressed in crontab(5) compatible time/date pattern.

`-t | --start {startTime}`

Indicates the date/time at which this operation will start when scheduled as a server task expressed in YYYYMMDDhhmmssZ format for UTC time or YYYYMMDDhhmmss for local time. A value of '0' will cause the task to be scheduled for immediate execution. When this option is specified the operation will be scheduled to start at the specified time after which this utility will exit immediately.

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`--wrapColumn {wrapColumn}`

Column at which to wrap long lines (0 for no wrapping).

Default: 0

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following example exports data to a file, `Example.ldif`, with the server offline.

```
$ export-ldif -b dc=example,dc=com -n userRoot -l ../ldif/Example.ldif
... category=BACKEND severity=INFORMATION ...
...Exported 160 entries and skipped 0 in 0 seconds (average rate 1428.6/sec)
```

import-ldif(1)

Name

import-ldif - import OpenDJ directory data from LDIF

Synopsis

`import-ldif`

Description

This utility can be used to import LDIF data into a Directory Server backend, overwriting existing data. It cannot be used to append data to the backend database.

Options

The `import-ldif` command takes the following options:

Command options:

`-A | --templateFile {templateFile}`

Path to a MakeLDIF template to use to generate the import data.

`-b | --includeBranch {branchDN}`

Base DN of a branch to include in the LDIF import.

`-B | --excludeBranch {branchDN}`

Base DN of a branch to exclude from the LDIF import.

`-c | --isCompressed`

LDIF file is compressed.

Default: false

`--countRejects`

Count the number of entries rejected by the server and return that value as the exit code (values > 255 will be reduced to 255 due to exit code restrictions).

Default: false

`-e | --excludeAttribute {attribute}`

Attribute to exclude from the LDIF import.

`-E | --excludeFilter {filter}`

Filter to identify entries to exclude from the LDIF import.

`-F | --clearBackend`

Remove all entries for all base DNs in the backend before importing. Set to `true` when running in the offline mode (i.e. the `--offline` flag is set).

Default: false

`-i | --includeAttribute {attribute}`

Attribute to include in the LDIF import.

`-I | --includeFilter {filter}`

Filter to identify entries to include in the LDIF import.

`-l | --ldifFile {ldifFile}`

Path to the LDIF file to be imported.

`-n | --backendID {backendName}`

Backend ID for the backend to import.

`-O | --overwrite`

Overwrite an existing rejects and/or skip file rather than appending to it.

Default: false

`--offline`

Indicates that the command must be run in offline mode. Forces old data replacement with imported data.

Default: false

`-R | --rejectFile {rejectFile}`

Write rejected entries to the specified file.

`-s | --randomSeed {seed}`

Seed for the MakeLDIF random number generator.

Default: 0

`-S | --skipSchemaValidation`

Skip schema validation during the LDIF import.

Default: false

`--skipFile {skipFile}`

Write skipped entries to the specified file.

`--threadCount {count}`

Number of threads used to read LDIF file during import. Default value (0) equals: 2 x (number of CPUs).

Default: 0

`--tmpdirectory {directory}`

Path to temporary directory for index scratch files during LDIF import.

Default: import-tmp

Task Backend Connection Options

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Task Scheduling Options

`--completionNotify {emailAddress}`

Email address of a recipient to be notified when the task completes. This option may be specified more than once.

`--dependency {taskID}`

ID of a task upon which this task depends. A task will not start execution until all its dependencies have completed execution.

`--errorNotify {emailAddress}`

Email address of a recipient to be notified if an error occurs when this task executes. This option may be specified more than once.

`--failedDependencyAction {action}`

Action this task will take should one if its dependent tasks fail. The value must be one of PROCESS,CANCEL,DISABLE. If not specified defaults to CANCEL.

`--recurringTask {schedulePattern}`

Indicates the task is recurring and will be scheduled according to the value argument expressed in crontab(5) compatible time/date pattern.

`-t | --start {startTime}`

Indicates the date/time at which this operation will start when scheduled as a server task expressed in YYYYMMDDhhmmssZ format for UTC time or YYYYMMDDhhmmss for local time. A value of '0' will cause the task to be scheduled for immediate execution. When this option is specified the operation will be scheduled to start at the specified time after which this utility will exit immediately.

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-Q | --quiet`

Use quiet mode (no output).

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following example imports the content of a file, `Example.ldif`, with the server offline.

```
$ import-ldif -b dc=example,dc=com -n userRoot -l /path/to/Example.ldif
... category=RUNTIME_INFORMATION severity=NOTICE...
... msg=Import LDIF environment close took 0 seconds
```

ldapcompare(1)

Name

ldapcompare - perform LDAP compare operations

Synopsis

```
ldapcompare attribute:value DN
```

Description

This utility can be used to perform LDAP compare operations in the Directory Server.

Options

The `ldapcompare` command takes the following options:

Command options:

`--assertionFilter {filter}`

Use the LDAP assertion control with the provided filter.

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-J | --control {controloid[:criticality[:value|::b64value|:<filePath]]}`

Use a request control with the provided information.

For some *controloid* values, you can replace object identifiers with user-friendly strings. The strings are listed here in lower case, but the case is not important. You can use camelCase if you prefer, for example.

`accountusable`,`accountusability`

Account Usability Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.8

`authzid`,`authorizationidentity`

Authorization Identity Request Control, Object Identifier: 2.16.840.1.113730.3.4.16

`effectiverights`,`geteffectiverights`

Get Effective Rights Request Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.2

`managedsait`

Manage DSAIT Request Control, Object Identifier: 2.16.840.1.113730.3.4.2

`noop`,`no-op`

No-Op Control, Object Identifier: 1.3.6.1.4.1.4203.1.10.2

`pwpolicy`,`passwordpolicy`

Password Policy Control, Object Identifier: 1.3.6.1.4.1.42.2.27.8.5.1

`realattrsonly`,`realattributesonly`

Real Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.17

`subtreedelete`,`treedelete`

Subtree Delete Request Control, Object Identifier: 1.2.840.113556.1.4.805

`virtualattrsonly`,`virtualattributesonly`

Virtual Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.19

`-m | --useCompareResultCode`

Use the LDAP compare result as an exit code for the LDAP compare operations.

Default: false

`-n | --dry-run`

Show what would be done but do not perform any operation.

Default: false

`-S | --scriptFriendly`

Use script-friendly mode.

Default: false

`-Y | --proxyAs {authzID}`

Use the proxied authorization control with the given authorization ID.

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default:

`-E | --reportAuthzID`

Use the authorization identity control.

Default: false

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server port number.

Default: 389

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-q | --useStartTLS`

Use StartTLS to secure communication with the server.

Default: false

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`--usePasswordPolicyControl`

Use the password policy request control.

Default: false

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

`-Z | --useSSL`

Use SSL for secure communication with the server.

Default: false

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

5

The LDAP compare operation did not match.

6

The `-m` option was used, and the LDAP compare operation did match.

ldap-error

An LDAP error occurred while processing the operation.

LDAP result codes are described in RFC 4511. Also see the additional information for details.

89

An error occurred while parsing the command-line arguments.

Files

You can use `~/.opendj/tools.properties` to set the defaults for bind DN, host name, and port number as in the following example.

```
hostname=directory.example.com
port=1389
bindDN=uid=kvaughan,ou=People,dc=example,dc=com

ldapcompare.port=1389
ldapdelete.port=1389
ldapmodify.port=1389
ldappasswordmodify.port=1389
ldapsearch.port=1389
```

The location on Windows is `%UserProfile%/.opendj/tools.properties`.

Examples

The following examples demonstrate comparing Babs Jensen's UID.

The following example uses a matching UID value.

```
$ ldapcompare -p 1389 uid:bjensen uid=bjensen,ou=people,dc=example,dc=com
Comparing type uid with value bjensen in entry
uid=bjensen,ou=people,dc=example,dc=com
Compare operation returned true for entry
uid=bjensen,ou=people,dc=example,dc=com
```

The following example uses a UID value that does not match.

```
$ ldapcompare -p 1389 uid:beavis uid=bjensen,ou=people,dc=example,dc=com
Comparing type uid with value beavis in entry
uid=bjensen,ou=people,dc=example,dc=com
Compare operation returned false for entry
uid=bjensen,ou=people,dc=example,dc=com
```

ldapdelete(1)

Name

ldapdelete - perform LDAP delete operations

Synopsis

`ldapdelete [DN]`

Description

This utility can be used to perform LDAP delete operations in the Directory Server. If standard input is used to specify entries to remove, end your input with EOF (Ctrl+D on UNIX, Ctrl+Z on Windows).

Options

The `ldapdelete` command takes the following options:

Command options:

`-c | --continueOnError`

Continue processing even if there are errors.

Default: false

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-J | --control {controloid[:criticality[:value|::b64value|:<filePath]]}`

Use a request control with the provided information.

For some *controloid* values, you can replace object identifiers with user-friendly strings. The strings are listed here in lower case, but the case is not important. You can use camelCase if you prefer, for example.

`accountusable`,`accountusability`

Account Usability Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.8

`authzid`,`authorizationidentity`

Authorization Identity Request Control, Object Identifier: 2.16.840.1.113730.3.4.16

`effectiverights`,`geteffectiverights`

Get Effective Rights Request Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.2

`managedsait`

Manage DSAIT Request Control, Object Identifier: 2.16.840.1.113730.3.4.2

`noop`,`no-op`

No-Op Control, Object Identifier: 1.3.6.1.4.1.4203.1.10.2

`pwpolicy`,`passwordpolicy`

Password Policy Control, Object Identifier: 1.3.6.1.4.1.42.2.27.8.5.1

`realattrsonly`,`realattributesonly`

Real Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.17

`subtreedelete`,`treedelete`

Subtree Delete Request Control, Object Identifier: 1.2.840.113556.1.4.805

`virtualattrsonly`,`virtualattributesonly`

Virtual Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.19

`-n | --dry-run`

Show what would be done but do not perform any operation.

Default: false

`-x | --deleteSubtree`

Delete the specified entry and all entries below it.

Default: false

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default:

`-E | --reportAuthzID`

Use the authorization identity control.

Default: false

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server port number.

Default: 389

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-q | --useStartTLS`

Use StartTLS to secure communication with the server.

Default: false

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`--usePasswordPolicyControl`

Use the password policy request control.

Default: false

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

`-Z | --useSSL`

Use SSL for secure communication with the server.

Default: false

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

ldap-error

An LDAP error occurred while processing the operation.

LDAP result codes are described in RFC 4511. Also see the additional information for details.

89

An error occurred while parsing the command-line arguments.

Files

You can use `~/.opendj/tools.properties` to set the defaults for bind DN, host name, and port number as in the following example.

```
hostname=directory.example.com
port=1389
bindDN=uid=kvaughan,ou=People,dc=example,dc=com

ldapcompare.port=1389
ldapdelete.port=1389
ldapmodify.port=1389
ldappasswordmodify.port=1389
ldapsearch.port=1389
```

The location on Windows is `%UserProfile%/.opendj/tools.properties`.

Examples

The following command deletes a user entry from the directory.

```
$ ldapdelete -p 1389 -D "cn=Directory Manager" -w password \
 uid=bjensen,ou=people,dc=example,dc=com
Processing DELETE request for uid=bjensen,ou=people,dc=example,dc=com
DELETE operation successful for DN uid=bjensen,ou=people,dc=example,dc=com
```

The following command deletes the `ou=Groups` entry and all entries underneath `ou=Groups`.

```
$ ldapdelete -p 1389 -D "cn=Directory Manager" -w password -x \
 ou=groups,dc=example,dc=com
Processing DELETE request for ou=groups,dc=example,dc=com
DELETE operation successful for DN ou=groups,dc=example,dc=com
```

ldapmodify(1)

Name

ldapmodify - perform LDAP modify, add, delete, mod DN operations

Synopsis

`ldapmodify [changes_files ⋯]`

Description

This utility can be used to perform LDAP modify, add, delete, and modify DN operations in the Directory Server. When not using file(s) to specify modifications, end your input with EOF (Ctrl+D on UNIX, Ctrl+Z on Windows).

Options

The `ldapmodify` command takes the following options:

Command options:

`-a | --defaultAdd`

Legacy argument for ForgeRock OpenDJ compatibility.

Default: false

`--assertionFilter {filter}`

Use the LDAP assertion control with the provided filter.

`-c | --continueOnError`

Continue processing even if there are errors.

Default: false

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-J | --control {controloid[:criticality[:value|::b64value|:<filePath]]}`

Use a request control with the provided information.

For some *controloid* values, you can replace object identifiers with user-friendly strings. The strings are listed here in lower case, but the case is not important. You can use camelCase if you prefer, for example.

`accountusable`,`accountusability`

Account Usability Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.8

`authzid`,`authorizationidentity`

Authorization Identity Request Control, Object Identifier: 2.16.840.1.113730.3.4.16

`effectiverights`,`geteffectiverights`

Get Effective Rights Request Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.2

`managedsait`

Manage DSAIT Request Control, Object Identifier: 2.16.840.1.113730.3.4.2

`noop`,`no-op`

No-Op Control, Object Identifier: 1.3.6.1.4.1.4203.1.10.2

`pwpolicy`,`passwordpolicy`

Password Policy Control, Object Identifier: 1.3.6.1.4.1.42.2.27.8.5.1

`realattrsonly`,`realattributesonly`

Real Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.17

`subtreedelete`,`treedelete`

Subtree Delete Request Control, Object Identifier: 1.2.840.113556.1.4.805

`virtualattrsonly`,`virtualattributesonly`

Virtual Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.19

`-n | --dry-run`

Show what would be done but do not perform any operation.

Default: false

`--postReadAttributes {attrList}`

Use the LDAP ReadEntry post-read control.

`--preReadAttributes {attrList}`

Use the LDAP ReadEntry pre-read control.

`-Y | --proxyAs {authzID}`

Use the proxied authorization control with the given authorization ID.

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default:

`-E | --reportAuthzID`

Use the authorization identity control.

Default: false

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server port number.

Default: 389

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-q | --useStartTLS`

Use StartTLS to secure communication with the server.

Default: false

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`--usePasswordPolicyControl`

Use the password policy request control.

Default: false

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

`-Z | --useSSL`

Use SSL for secure communication with the server.

Default: false

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

ldap-error

An LDAP error occurred while processing the operation.

LDAP result codes are described in RFC 4511. Also see the additional information for details.

89

An error occurred while parsing the command-line arguments.

Files

You can use `~/.opendj/tools.properties` to set the defaults for bind DN, host name, and port number as in the following example.

```
hostname=directory.example.com
port=1389
bindDN=uid=kvaughan,ou=People,dc=example,dc=com

ldapcompare.port=1389
ldapdelete.port=1389
ldapmodify.port=1389
ldappasswordmodify.port=1389
ldapsearch.port=1389
```

The location on Windows is `%UserProfile%/.opendj/tools.properties`.

Examples

The following example demonstrates use of the command to add an entry to the directory.

```
$ cat newuser.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
uid: newuser
facsimileTelephoneNumber: +1 408 555 1213
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
givenName: New
cn: New User
cn: Real Name
telephoneNumber: +1 408 555 1212
sn: Jensen
roomNumber: 1234
```

```
homeDirectory: /home/newuser
uidNumber: 10389
mail: newuser@example.com
l: South Pole
ou: Product Development
ou: People
gidNumber: 10636

$ ldapmodify -p 1389 -a -f newuser.ldif \
 -D uid=kvaughan,ou=people,dc=example,dc=com -w bribery
Processing ADD request for uid=newuser,ou=People,dc=example,dc=com
ADD operation successful for DN uid=newuser,ou=People,dc=example,dc=com
```

The following listing shows a UNIX shell script that adds a user entry.

```
#!/bin/sh
#
# Add a new user with the ldapmodify utility.
#

usage(){
        echo "Usage: $0 uid firstname lastname"
        exit 1
}
[[ $# -lt 3 ]] && usage

LDAPMODIFY=/path/to/opendj/bin/ldapmodify
HOST=opendj.example.com
PORT=1389
ADMIN=uid=kvaughan,ou=people,dc=example,dc=com
PWD=bribery

$LDAPMODIFY -h $HOST -p $PORT -D $ADMIN -w $PWD -a <<EOF
dn: uid=$1,ou=people,dc=example,dc=com
uid: $1
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: $2 $3
givenName: $2
sn: $3
mail: $1@example.com
EOF
```

The following example demonstrates adding a Description attribute to the new user's entry.

```
$ cat newdesc.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
```

```
changetype: modify
add: description
description: A new user's entry

$ ldapmodify -p 1389 -f newdesc.ldif \
 -D uid=kvaughan,ou=people,dc=example,dc=com -w bribery
Processing MODIFY request for uid=newuser,ou=People,dc=example,dc=com
MODIFY operation successful for DN uid=newuser,ou=People,dc=example,dc=com
```

The following example demonstrates changing the Description attribute for the new user's entry.

```
$ cat moddesc.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
changetype: modify
replace: description
description: Another description

$ ldapmodify -p 1389 -f moddesc.ldif \
 -D uid=kvaughan,ou=people,dc=example,dc=com -w bribery
Processing MODIFY request for uid=newuser,ou=People,dc=example,dc=com
MODIFY operation successful for DN uid=newuser,ou=People,dc=example,dc=com
```

The following example demonstrates deleting the new user's entry.

```
$ cat deluser.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
changetype: delete

$ ldapmodify -p 1389 -f deluser.ldif \
 -D uid=kvaughan,ou=people,dc=example,dc=com -w bribery
Processing DELETE request for uid=newuser,ou=People,dc=example,dc=com
DELETE operation successful for DN uid=newuser,ou=People,dc=example,dc=com
```

ldappasswordmodify(1)

Name

ldappasswordmodify - perform LDAP password modifications

Synopsis

`ldappasswordmodify`

Description

This utility can be used to perform LDAP password modify operations in the Directory Server.

Options

The `ldappasswordmodify` command takes the following options:

Command options:

`-a | --authzID {authzID}`

Authorization ID for the user entry whose password should be changed. The authorization ID is a string having either the prefix "dn:" followed by the user's distinguished name, or the prefix "u:" followed by a user identifier that depends on the identity mapping used to match the user identifier to an entry in the directory. Examples include "dn:uid=bjensen,ou=People,dc=example,dc=com", and, if we assume that "bjensen" is mapped to Barbara Jensen's entry, "u:bjensen".

`-c | --currentPassword {currentPassword}`

Current password for the target user.

`-C | --currentPasswordFile {file}`

Path to a file containing the current password for the target user.

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-F | --newPasswordFile {file}`

Path to a file containing the new password to provide for the target user.

`-J | --control {controloid[:criticality[:value|::b64value|:<filePath]]}`

Use a request control with the provided information.

For some *controloid* values, you can replace object identifiers with user-friendly strings. The strings

are listed here in lower case, but the case is not important. You can use camelCase if you prefer, for example.

`accountusable`,`accountusability`

Account Usability Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.8

`authzid`,`authorizationidentity`

Authorization Identity Request Control, Object Identifier: 2.16.840.1.113730.3.4.16

`effectiverights`,`geteffectiverights`

Get Effective Rights Request Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.2

`managedsait`

Manage DSAIT Request Control, Object Identifier: 2.16.840.1.113730.3.4.2

`noop`,`no-op`

No-Op Control, Object Identifier: 1.3.6.1.4.1.4203.1.10.2

`pwpolicy`,`passwordpolicy`

Password Policy Control, Object Identifier: 1.3.6.1.4.1.42.2.27.8.5.1

`realattrsonly`,`realattributesonly`

Real Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.17

`subtreedelete`,`treedelete`

Subtree Delete Request Control, Object Identifier: 1.2.840.113556.1.4.805

`virtualattrsonly`,`virtualattributesonly`

Virtual Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.19

`-n | --newPassword {newPassword}`

New password to provide for the target user.

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default:

`-E | --reportAuthzID`

Use the authorization identity control.

Default: false

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server port number.

Default: 389

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-q | --useStartTLS`

Use StartTLS to secure communication with the server.

Default: false

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`--usePasswordPolicyControl`

Use the password policy request control.

Default: false

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

`-Z | --useSSL`

Use SSL for secure communication with the server.

Default: false

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

ldap-error

An LDAP error occurred while processing the operation.

LDAP result codes are described in RFC 4511. Also see the additional information for details.

89

An error occurred while parsing the command-line arguments.

Files

You can use `~/.opendj/tools.properties` to set the defaults for bind DN, host name, and port number as in the following example.

```
hostname=directory.example.com
port=1389
bindDN=uid=kvaughan,ou=People,dc=example,dc=com

ldapcompare.port=1389
ldapdelete.port=1389
ldapmodify.port=1389
ldappasswordmodify.port=1389
ldapsearch.port=1389
```

The location on Windows is `%UserProfile%/.opendj/tools.properties`.

Examples

The following example demonstrates a user changing their own password.

```
$ cat /tmp/currpwd.txt /tmp/newpwd.txt
bribery
secret12

$ ldappasswordmodify -p 1389 -C /tmp/currpwd.txt --newPasswordFile /tmp/newpwd.txt \
 -D uid=kvaughan,ou=people,dc=example,dc=com -w bribery
The LDAP password modify operation was successful
```

ldapsearch(1)

Name

ldapsearch - perform LDAP search operations

Synopsis

`ldapsearch filter [attributes ⋯]`

Description

This utility can be used to perform LDAP search operations in the Directory Server.

Options

The `ldapsearch` command takes the following options:

Command options:

`-a | --dereferencePolicy {dereferencePolicy}`

Alias dereference policy ('never', 'always', 'search', or 'find').

Default: never

`-A | --typesOnly`

Only retrieve attribute names but not their values.

Default: false

`--assertionFilter {filter}`

Use the LDAP assertion control with the provided filter.

`-b | --baseDN {baseDN}`

Search base DN.

`-c | --continueOnError`

Continue processing even if there are errors.

Default: false

`-C | --persistentSearch ps[:changetype[:changesonly[:entrychgcontrols]]]`

Use the persistent search control.

A persistent search allows the client to continue receiving new results whenever changes are made to data that is in the scope of the search, thus using the search as a form of change notification.

The optional `changetype` setting defines the kinds of updates that result in notification. If you do not set the `changetype`, the default behavior is to send notifications for all updates.

`add`

Send notifications for LDAP add operations.

`del`,`delete`

Send notifications for LDAP delete operations.

`mod`,`modify`

Send notifications for LDAP modify operations.

`moddn`,`modrdn`,`modifydn`

Send notifications for LDAP modify DN (rename and move) operations.

`all`,`any`

Send notifications for all LDAP update operations.

The optional `changesonly` setting defines whether the server returns existing entries as well as changes.

`true`

Do not return existing entries, but instead only notifications about changes.

This is the default setting.

`false`

Also return existing entries.

The optional `entrychgcontrols` setting defines whether the server returns an Entry Change Notification control with each entry notification. The Entry Change Notification control provides additional information about the change that caused the entry to be returned by the search. In particular, it indicates the change type, the change number if available, and the previous DN if the change type was a modify DN operation.

`true`

Do request the Entry Change Notification control.

This is the default setting.

`false`

Do not request the Entry Change Notification control.

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`--countEntries`

Count the number of entries returned by the server.

Default: false

`-e | --getEffectiveRightsAttribute {attribute}`

Specifies geteffectiverights control specific attribute list.

`-g | --getEffectiveRightsAuthzid {authzID}`

Use geteffectiverights control with the provided authzid.

`-G | --virtualListView {before:after:index:count | before:after:value}`

Use the virtual list view control to retrieve the specified results page.

`-J | --control {controloid[:criticality[:value|::b64value|:<filePath]]}`

Use a request control with the provided information.

For some *controloid* values, you can replace object identifiers with user-friendly strings. The strings are listed here in lower case, but the case is not important. You can use camelCase if you prefer, for example.

`accountusable`,`accountusability`

Account Usability Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.8

`authzid`,`authorizationidentity`

Authorization Identity Request Control, Object Identifier: 2.16.840.1.113730.3.4.16

`effectiverights`,`geteffectiverights`

Get Effective Rights Request Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.2

`managedsait`

Manage DSAIT Request Control, Object Identifier: 2.16.840.1.113730.3.4.2

`noop`,`no-op`

No-Op Control, Object Identifier: 1.3.6.1.4.1.4203.1.10.2

`pwpolicy`,`passwordpolicy`

Password Policy Control, Object Identifier: 1.3.6.1.4.1.42.2.27.8.5.1

`realattrsonly`,`realattributesonly`

Real Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.17

`subtreedelete`,`treedelete`

Subtree Delete Request Control, Object Identifier: 1.2.840.113556.1.4.805

`virtualattrsonly`,`virtualattributesonly`

Virtual Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.19

`-l | --timeLimit {timeLimit}`

Maximum length of time in seconds to allow for the search.

Default: 0

`--matchedValuesFilter {filter}`

Use the LDAP matched values control with the provided filter.

`-n | --dry-run`

Show what would be done but do not perform any operation.

Default: false

`-s | --searchScope {searchScope}`

Search scope ('base', 'one', 'sub', or 'subordinates'). Note: 'subordinates' is an LDAP extension that might not work with all LDAP servers.

Default: sub

`-S | --sortOrder {sortOrder}`

Sort the results using the provided sort order.

`--simplePageSize {numEntries}`

Use the simple paged results control with the given page size.

Default: 1000

`--subEntries`

Use subentries control to specify that subentries are visible and normal entries are not.

Default: false

`-Y | --proxyAs {authzID}`

Use the proxied authorization control with the given authorization ID.

`-z | --sizeLimit {sizeLimit}`

Maximum number of entries to return from the search.

Default: 0

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default:

`-E | --reportAuthzID`

Use the authorization identity control.

Default: false

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server port number.

Default: 389

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-q | --useStartTLS`

Use StartTLS to secure communication with the server.

Default: false

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`--usePasswordPolicyControl`

Use the password policy request control.

Default: false

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the

password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

`-Z | --useSSL`

Use SSL for secure communication with the server.

Default: false

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-t | --wrapColumn {wrapColumn}`

Maximum length of an output line (0 for no wrapping).

Default: 0

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Filters

The filter argument is a string representation of an LDAP search filter as in `(cn=Babs Jensen)`,

`(&(objectClass=Person)(|(sn=Jensen)(cn=Babs J*)))`, or `(cn:caseExactMatch:=Fred Flintstone)`.

Attributes

The optional attribute list specifies the attributes to return in the entries found by the search. In addition to identifying attributes by name such as `cn sn mail` and so forth, you can use the following notations, too.

`*`

Return all user attributes such as `cn`, `sn`, and `mail`.

`+`

Return all operational attributes such as `etag` and `pwdPolicySubentry`.

`@objectclass`

Return all attributes of the specified object class, where *objectclass* is one of the object classes on the entries returned by the search.

`1.1`

Return no attributes, only the DNs of matching entries.

Exit Codes

0

The command completed successfully.

ldap-error

An LDAP error occurred while processing the operation.

LDAP result codes are described in RFC 4511. Also see the additional information for details.

89

An error occurred while parsing the command-line arguments.

Files

You can use `~/.opendj/tools.properties` to set the defaults for bind DN, host name, and port number as in the following example.

```
hostname=directory.example.com
port=1389
bindDN=uid=kvaughan,ou=People,dc=example,dc=com

ldapcompare.port=1389
ldapdelete.port=1389
ldapmodify.port=1389
ldappasswordmodify.port=1389
```

```
ldapsearch.port=1389
```

The location on Windows is `%UserProfile%/.opendj/tools.properties`.

Examples

The following example searches for entries with UID containing `jensen`, returning only DNs and uid values.

```
$ ldapsearch -p 1389 -b dc=example,dc=com "(uid=*jensen*)" uid
dn: uid=ajensen,ou=People,dc=example,dc=com
uid: ajensen

dn: uid=bjensen,ou=People,dc=example,dc=com
uid: bjensen

dn: uid=gjensen,ou=People,dc=example,dc=com
uid: gjensen

dn: uid=jjensen,ou=People,dc=example,dc=com
uid: jjensen

dn: uid=kjensen,ou=People,dc=example,dc=com
uid: kjensen

dn: uid=rjensen,ou=People,dc=example,dc=com
uid: rjensen

dn: uid=tjensen,ou=People,dc=example,dc=com
uid: tjensen


Result Code:  0 (Success)
```

You can also use `@objectclass` notation in the attribute list to return the attributes of a particular object class. The following example shows how to return attributes of the `inetOrgPerson` object class.

```
$ ldapsearch -p 1389 -b dc=example,dc=com "(uid=bjensen)" @inetorgperson
dn: uid=bjensen,ou=People,dc=example,dc=com
givenName: Barbara
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
uid: bjensen
cn: Barbara Jensen
cn: Babs Jensen
```

```
telephoneNumber: +1 408 555 1862
sn: Jensen
roomNumber: 0209
mail: bjensen@example.com
l: San Francisco
ou: Product Development
ou: People
facsimileTelephoneNumber: +1 408 555 1992
```

You can use + in the attribute list to return all operational attributes, as in the following example.

```
$ ldapsearch -p 1389 -b dc=example,dc=com "(uid=bjensen)" +
dn: uid=bjensen,ou=People,dc=example,dc=com
numSubordinates: 0
structuralObjectClass: inetOrgPerson
etag: 0000000073c29972
pwdPolicySubentry: cn=Default Password Policy,cn=Password Policies,cn=config
subschemaSubentry: cn=schema
hasSubordinates: false
entryDN: uid=bjensen,ou=people,dc=example,dc=com
entryUUID: fc252fd9-b982-3ed6-b42a-c76d2546312c
```

ldifdiff(1)

Name

ldifdiff - compare small LDIF files

Synopsis

```
ldifdiff source target
```

Description

This utility can be used to compare two LDIF files and report the differences in LDIF format. If standard input is used to specify source or target, end your input with EOF (Ctrl+D on UNIX, Ctrl+Z on Windows).

Options

The `ldifdiff` command takes the following options:

Command options:

`-o | --outputLDIF {file}`

Write differences to {file} instead of stdout.

Default: stdout

Utility input/output options:

`-t | --wrapColumn {wrapColumn}`

Maximum length of an output line (0 for no wrapping).

Default: 0

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

No differences were found.

1

Differences were found.

other

An error occurred.

Examples

The following example demonstrates use of the command with two small LDIF files.

```
$ cat /path/to/newuser.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
uid: newuser
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
cn: New User
sn: User
ou: People
mail: newuser@example.com
userPassword: changeme

$ cat /path/to/neweruser.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
uid: newuser
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
cn: New User
sn: User
ou: People
mail: newuser@example.com
userPassword: secret12
description: A new description.

$ ldifdiff -s /path/to/newuser.ldif -t /path/to/neweruser.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
changetype: modify
add: userPassword
userPassword: secret12
-
delete: userPassword
userPassword: changeme
-
```

```
add: description
description: A new description.
```

ldifmodify(1)

Name

ldifmodify - apply LDIF changes to LDIF

Synopsis

`ldifmodify source_file [changes_files…]`

Description

This utility can be used to apply a set of modify, add, and delete operations to entries contained in an LDIF file. If standard input is used to specify source or changes, end your input with EOF (Ctrl+D on UNIX, Ctrl+Z on Windows).

Options

The `ldifmodify` command takes the following options:

Command options:

`-c | --continueOnError`

Continue processing even if there are errors.

Default: false

`-o | --outputLDIF {file}`

Write updated entries to {file} instead of stdout.

Default: stdout

Utility input/output options:

`-t | --wrapColumn {wrapColumn}`

Maximum length of an output line (0 for no wrapping).

Default: 0

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following example demonstrates use of the command.

```
$ cat /path/to/newuser.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
uid: newuser
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
cn: New User
sn: User
ou: People
mail: newuser@example.com
userPassword: changeme

$ cat /path/to/newdiff.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
changetype: modify
add: userPassword
userPassword: secret12
-
delete: userPassword
userPassword: changeme
-
add: description
description: A new description.

$ ldifmodify -o neweruser.ldif /path/to/newuser.ldif /path/to/newdiff.ldif

$ cat neweruser.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
uid: newuser
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
cn: New User
```

```
sn: User
ou: People
mail: newuser@example.com
userPassword: secret12
description: A new description.
```

ldifsearch(1)

Name

ldifsearch - search LDIF with LDAP filters

Synopsis

`ldifsearch source filter [attributes …]`

Description

This utility can be used to perform search operations against entries contained in an LDIF file. If standard input is used to specify source, end your input with EOF (Ctrl+D on UNIX, Ctrl+Z on Windows).

Options

The `ldifsearch` command takes the following options:

Command options:

`-A | --typesOnly`

Only retrieve attribute names but not their values.

Default: false

`-b | --baseDN {baseDN}`

The base DN for the search. If no base DN is provided, then the root DSE will be used.

Default:

`-l | --timeLimit {timeLimit}`

Maximum length of time in seconds to allow for the search.

Default: 0

`-o | --outputLDIF {file}`

Write search results to {file} instead of stdout.

Default: stdout

`-s | --searchScope {searchScope}`

Search scope ('base', 'one', 'sub', or 'subordinates'). Note: 'subordinates' is an LDAP extension that might not work with all LDAP servers.

Default: sub

`-z | --sizeLimit {sizeLimit}`

Maximum number of entries to return from the search.

Default: 0

Utility input/output options:

`-t | --wrapColumn {wrapColumn}`

Maximum length of an output line (0 for no wrapping).

Default: 0

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following example demonstrates use of the command.

```
$ ldifsearch -b dc=example,dc=com Example.ldif uid=bjensen
dn: uid=bjensen,ou=People,dc=example,dc=com
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
uid: bjensen
userpassword: hifalutin
facsimiletelephonenumber: +1 408 555 1992
givenname: Barbara
cn: Barbara Jensen
cn: Babs Jensen
telephonenumber: +1 408 555 1862
```

```
sn: Jensen
roomnumber: 0209
homeDirectory: /home/bjensen
mail: bjensen@example.com
l: San Francisco
ou: Product Development
ou: People
uidNumber: 1076
gidNumber: 1000
```

You can also use `@objectclass` notation in the attribute list to return the attributes of a particular object class. The following example shows how to return attributes of the `posixAccount` object class.

```
$ ldifsearch -b dc=example,dc=com Example.ldif "(uid=bjensen)" @posixaccount
dn: uid=bjensen,ou=People,dc=example,dc=com
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
uid: bjensen
userpassword: hifalutin
cn: Barbara Jensen
cn: Babs Jensen
homeDirectory: /home/bjensen
uidNumber: 1076
gidNumber: 1000
```

list-backends(1)

Name

list-backends - list OpenDJ backends and base DNs

Synopsis

`list-backends`

Description

This utility can be used to list the backends and base DNs configured in the Directory Server.

Options

The `list-backends` command takes the following options:

Command options:

`-b | --baseDN {baseDN}`

Base DN for which to list the backend ID.

`-n | --backendID {backendName}`

Backend ID of the backend for which to list the base DNs.

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following example demonstrates a successful run.

```
$ list-backends
Backend ID         : Base DN
-------------------:----------------------
adminRoot          : cn=admin data
ads-truststore     : cn=ads-truststore
backup             : cn=backups
config             : cn=config
monitor            : cn=monitor
myCompanyRoot      : "dc=myCompany,dc=com"
myOrgRoot          : o=myOrg
schema             : cn=schema
tasks              : cn=tasks
userRoot           : "dc=example,dc=com"
```

makeldif(1)

Name

makeldif - generate test LDIF

Synopsis

`makeldif template-file-path`

Description

This utility can be used to generate LDIF data based on a definition in a template file.

Options

The `makeldif` command takes the following options:

Command options:

`-c | --constant {name=value}`

A constant that overrides the value set in the template file.

`-o | --outputLDIF {file}`

The path to the LDIF file to be written.

`-r | --resourcePath {path}`

Path to look for MakeLDIF resources (e.g., data files).

`-s | --randomSeed {seed}`

The seed to use to initialize the random number generator.

Default: 0

Utility input/output options:

`-t | --wrapColumn {wrapColumn}`

Maximum length of an output line (0 for no wrapping).

Default: 0

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

1

An error occurred.

Examples

The following example uses the default template to generate LDIF.

```
$ makeldif -o ../ldif/generated.ldif ../config/MakeLDIF/example.template
Processed 1000 entries
Processed 2000 entries
...
Processed 10000 entries
LDIF processing complete.  10003 entries written
```

See Also

makeldif-template(5)

makeldif-template(5)

Name

makeldif-template - template file for the make-ldif command

Synopsis

```
# Comment lines start with #.
#
# Notice that this synopsis includes blank lines after entries.
# In the same way you would use blank lines after entries in normal LDIF,
# leave empty lines after "entries" in template files.

# Optionally include classes that define custom tags.
# Custom tag classes extend org.opends.server.tools.makeldif.Tag and
# must be on the class path when you run make-ldif.
#
include custom.makeldif.tag.ClassName
...

# Optionally define constants used in the template.
# To reference constants later, put brackets around the name: [constant-name]
#
define constant-name=value
...

# Define branches by suffix DN, such as the following:
#
#  dc=example,dc=com
#  ou=People,dc=example,dc=com
#  ou=Groups,dc=example,dc=com
#
# make-ldif generates the necessary object class definitions and RDNs.
#
# A branch can have subordinateTemplates that define templates to use for
# the branch entry.
#
# A branch can have additional attributes generated on the branch entry. See
# the Description below for more information on specifying attribute values.
#
branch: suffix-dn
[subordinateTemplate: template-name:number
...]
[attribute: attr-value
...]

...
```

```
# Define entries using templates.
#
# A template can extend another template.
# A template defines the RDN attribute(s) used for generated entries.
# A template can have a subordinateTemplate that defines a template to use for
# the generated entries.
#
# A template then defines attributes. See the Description below for more
# information on specifying attribute values.
#
template: template-name
[extends: template-name]
rdnAttr: attribute[+attribute ...]
[subordinateTemplate: template-name:number]
[attribute: attr-value
...]

...
```

Description

Template files specify how to build LDIF. They allow you to define variables, insert random values from other files, and generally build arbitrarily large LDIF files for testing purposes. You pass template files to the `make-ldif` command when generating LDIF.

The Synopsis above shows the layout for a `make-ldif` template file. This section focuses on what you can do to specify entry attribute values, called *attr-value* in the Synopsis section. .Specifying Attribute Values

When specifying attribute values in `make-ldif` templates, you can use static text and constants that you have defined, enclosing names for constants in brackets, `[myConstant]`. You can use more than one constant per line, as in the following example.

```
description: Description for [org] under [suffix]
```

You can also use two kinds of tags when specifying attribute values. One kind of tag gets replaced with the value of another attribute in the generated entry. Such tags are delimited with braces, `{ }`. For example, if your template includes definitions for first name and last name attributes:

```
givenName: <first>
sn: <last>
```

Then you can define a mail attribute that uses the values of both attributes, and an initials attribute that takes the first character of each.

```
mail: {givenName}.{sn}@[myDomain]
initials: {givenName:1}{sn:1}
```

The other kind of tag is delimited with < and >, as shown above in the example with <first> and <last>. Tag names are not case sensitive. Many tags can take arguments separated by colons, :, from the tag names within the tag.

Use backslashes to escape literal start tag characters (< [{) as shown in the following example, and to escape literal end tag characters within tags (>] }).

```
scimMail: \{"emails": \[\{"value": "{mail}", "type": "work", "primary": true}]}
xml: \<id>{uid}\</id>
```

OpenDJ supports the following tags.

<DN>

The DN tag gets replaced by the distinguished name of the current entry. An optional integer argument specifies the subcomponents of the DN to generate. For example, if the DN of the entry is uid=bjensen,ou=People,dc=example,dc=com <DN:1> gets replaced by uid=bjensen, and <DN:-2> gets replaced by dc=example,dc=com.

<File>

The File tag gets replaced by a line from a text file you specify. The File tag takes a required argument, the path to the text file, and an optional second argument, either random or sequential. For the file argument, either you specify an absolute path to the file such as <file:/path/to/myDescriptions>, or you specify a path relative to the /path/to/opendj/config/MakeLDIF/ directory such as <file:streets>. For the second argument, if you specify sequential then lines from the file are read in sequential order. Otherwise, lines from the file are read in random order.

<First>

The first name tag gets replaced by a random line from /path/to/opendj/config/MakeLDIF/first.names. Combinations of generated first and last names are unique, with integers appended to the name strings if not enough combinations are available.

<GUID>

The GUID tag gets replaced by a 128-bit, type 4 (random) universally unique identifier such as f47ac10b-58cc-4372-a567-0e02b2c3d479.

<IfAbsent>

The IfAbsent tag takes as its first argument the name of another attribute, and optionally as its second argument a value to use. This tag causes the attribute to be generated only if the named attribute is not present on the generated entry. Use this tag when you have used <Presence> to define another attribute that is not always present on generated entries.

<IfPresent>

The IfPresent takes as its first argument the name of another attribute, and optionally as its second argument a value to use. This tag causes the attribute to be generated only if the named attribute is also present on the generated entry. Use this tag when you have used `<Presence>` to define another attribute that is sometimes present on generated entries.

<Last>

The last name tag gets replaced by a random line from `/path/to/opendj/config/MakeLDIF/last.names`. Combinations of generated first and last names are unique, with integers appended to the name strings if not enough combinations are available.

<List>

The List tag gets replaced by one of the values from the list of arguments you provide. For example, `<List:bronze:silver:gold>` gets replaced with `bronze`, `silver`, or `gold`.

You can weight arguments to ensure some arguments are selected more often than others. For example, if you want two bronze for one silver and one gold, use `<List:bronze;2:silver;1:gold;1>`.

<ParentDN>

The ParentDN tag gets replaced by the distinguished name of the parent entry. For example, if the DN of the entry is `uid=bjensen,ou=People,dc=example,dc=com`, `<ParentDN>` gets replaced by `ou=People,dc=example,dc=com`.

<Presence>

The Presence tag takes a percent argument. It does not get replaced by a value itself, but instead results in the attribute being generated on the percentage of entries you specify in the argument. For example, `description: <Presence:50>A description` generates `description: A description` on half the entries.

<Random>

The Random tag lets you generate a variety of random numbers and strings. The Random tag has the following subtypes, which you include as arguments, that is `<Random:subtype>`.

- `alpha:length`
- `alpha:minlength:maxlength`
- `numeric:length`
- `numeric:minvalue:maxvalue`
- `numeric:minvalue:maxvalue:format`, where *format* is a java.text.DecimalFormat pattern
- `alphanumeric:length`
- `alphanumeric:minlength:maxlength`
- `chars:characters:length`
- `chars:characters:minlength:maxlength`
- `hex:length`

- `hex:minlength:maxlength`
- `base64:length`
- `base64:minlength:maxlength`
- `month`
- `month:maxlength`
- `telephone`, a telephone number starting with the country code `+1`

<RDN>

The RDN tag gets replaced with the RDN of the entry. Use this in the template after you have specified `rdnAttr` so that the RDN has already been generated when this tag is replaced.

An optional integer argument specifies the subcomponents of the RDN to generate.

<Sequential>

The Sequential tag gets replaced by a sequentially increasing generated integer. The first optional integer argument specifies the starting number. The second optional boolean argument specifies whether to start over when generating entries for a new parent entry. For example, `<Sequential>:42:true` starts counting from 42, and starts over when the parent entry changes from `o=Engineering` to `o=Marketing`.

<_DN>

The _DN tag gets replaced by the DN of the current entry with underscores in the place of commas.

<_ParentDN>

The _ParentDN tag gets replaced by the DN the parent entry with underscores in the place of commas.

Examples

The following example generates 10 organization units, each containing 50 entries.

```
define suffix=dc=example,dc=com
define maildomain=example.com
define numusers=50
define numorgs=10

branch: [suffix]

branch: ou=People,[suffix]
subordinateTemplate: orgunit:[numorgs]
description: This is the People container
telephoneNumber: +33 00010002

template: orgunit
subordinateTemplate: person:[numusers]
rdnAttr: ou
```

```
ou: Org-<sequential:0>
objectClass: top
objectClass: organizationalUnit
description: This is the {ou} organizational unit

template: person
rdnAttr: uid
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
givenName: <first>
sn: <last>
cn: {givenName} {sn}
initials: {givenName:1}<random:chars:ABCDEFGHIJKLMNOPQRSTUVWXYZ:1>{sn:1}
employeeNumber: <sequential:0>
uid: user.{employeeNumber}
mail: {uid}@[maildomain]
userPassword: password
telephoneNumber: <random:telephone>
homePhone: <random:telephone>
pager: <random:telephone>
mobile: <random:telephone>
street: <random:numeric:5> <file:streets> Street
l: <file:cities>
st: <file:states>
postalCode: <random:numeric:5>
postalAddress: {cn}${street}${l}, {st}  {postalCode}
description: This is the description for {cn}.
```

See Also

makeldif(1), the OpenDJ directory server template file /path/to/opendj/config/MakeLDIF/example.template

manage-account(1)

Name

manage-account - manage state of OpenDJ server accounts

Synopsis

`manage-account {subcommand} {options}`

Description

This utility can be used to retrieve and manipulate the values of password policy state variables.

Options

The `manage-account` command takes the following options:

Command options:

`-b | --targetDN {targetDN}`

The DN of the user entry for which to get and set password policy state information.

LDAP connection options:

`-D | --bindDN {bindDN}`

The DN to use to bind to the server.

`-h | --hostname {host}`

Directory server hostname or IP address.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

The path to the file containing the bind password.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of certificate for SSL client authentication.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

The password to use to bind to the server.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Utility input/output options:

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Subcommands

The `manage-account` command supports the following subcommands:

manage-account clear-account-is-disabled

Clear account disabled state information from the user account.

manage-account get-account-expiration-time

Display when the user account will expire.

manage-account get-account-is-disabled

Display information about whether the user account has been administratively disabled.

manage-account get-all

Display all password policy state information for the user.

manage-account get-authentication-failure-times

Display the authentication failure times for the user.

manage-account get-grace-login-use-times

Display the grace login use times for the user.

manage-account get-last-login-time

Display the time that the user last authenticated to the server.

manage-account get-password-changed-by-required-time

Display the required password change time with which the user last complied.

manage-account get-password-changed-time

Display the time that the user's password was last changed.

manage-account get-password-expiration-warned-time

Display the time that the user first received an expiration warning notice.

manage-account get-password-history

Display password history state values for the user.

manage-account get-password-is-reset

Display information about whether the user will be required to change his or her password on the next successful authentication.

manage-account get-password-policy-dn

Display the DN of the password policy for the user.

manage-account get-remaining-authentication-failure-count

Display the number of remaining authentication failures until the user's account is locked.

manage-account get-remaining-grace-login-count

Display the number of grace logins remaining for the user.

manage-account get-seconds-until-account-expiration

Display the length of time in seconds until the user account expires.

manage-account get-seconds-until-authentication-failure-unlock

Display the length of time in seconds until the authentication failure lockout expires.

manage-account get-seconds-until-idle-lockout

Display the length of time in seconds until user's account is locked because it has remained idle for too long.

manage-account get-seconds-until-password-expiration

Display length of time in seconds until the user's password expires.

manage-account get-seconds-until-password-expiration-warning

Display the length of time in seconds until the user should start receiving password expiration warning notices.

manage-account get-seconds-until-password-reset-lockout

Display the length of time in seconds until user's account is locked because the user failed to change the password in a timely manner after an administrative reset.

manage-account get-seconds-until-required-change-time

Display the length of time in seconds that the user has remaining to change his or her password before the account becomes locked due to the required change time.

manage-account set-account-is-disabled

Specify whether the user account has been administratively disabled.

Options

`-O | --operationValue {true|false}`

'true' to indicate that the account is disabled, or 'false' to indicate that it is not disabled.

Exit Codes

0

The command completed successfully.

89

An error occurred while parsing the command-line arguments.

Examples

For the following examples the directory admin user, Kirsten Vaughan, has `ds-privilege-name: password-reset` and the following ACI on `ou=People,dc=example,dc=com`.

```
(target="ldap:///ou=People,dc=example,dc=com") (targetattr ="*||+")(
 version 3.0;acl "Admins can run amok"; allow(all) groupdn =
 "ldap:///cn=Directory Administrators,ou=Groups,dc=example,dc=com";)
```

The following command locks a user account.

```
$ manage-account -p 4444 -D "uid=kvaughan,ou=people,dc=example,dc=com" \
 -w bribery set-account-is-disabled -O true \
 -b uid=bjensen,ou=people,dc=example,dc=com -X
Account Is Disabled:  true
```

The following command unlocks a user account.

```
$ manage-account -p 4444 -D "uid=kvaughan,ou=people,dc=example,dc=com" \
 -w bribery clear-account-is-disabled \
 -b uid=bjensen,ou=people,dc=example,dc=com -X
Account Is Disabled:  false
```

manage-tasks(1)

Name

manage-tasks - manage OpenDJ server administration tasks

Synopsis

`manage-tasks`

Description

This utility can be used to obtain a list of tasks scheduled to run within the Directory Server as well as information about individual tasks.

Options

The `manage-tasks` command takes the following options:

Command options:

`-c | --cancel {taskID}`

ID of a particular task to cancel.

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-i | --info {taskID}`

ID of a particular task about which this tool will display information.

`-s | --summary`

Print a summary of tasks.

Default: false

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Utility input/output options:

`-n | --no-prompt`

Use non-interactive mode. If data in the command is missing, the user is not prompted and the tool will fail.

Default: false

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following example demonstrates use of the command with a server that does daily backups at 2:00 AM.

```
$ manage-tasks -p 4444 -h opendj.example.com -D "cn=Directory Manager" \
 -w password -s

  ID                               Type    Status
  ---------------------------------------------------------------
  example-backup                   Backup  Recurring
  example-backup-20110622020000000 Backup  Waiting on start time
```

rebuild-index(1)

Name

rebuild-index - rebuild index after configuration change

Synopsis

`rebuild-index`

Description

This utility can be used to rebuild index data within an indexed backend database.

Options

The `rebuild-index` command takes the following options:

Command options:

`-b | --baseDN {baseDN}`

Base DN of a backend supporting indexing. Rebuild is performed on indexes within the scope of the given base DN.

`--clearDegradedState`

Indicates that indexes do not need rebuilding because they are known to be empty and forcefully marks them as valid. This is an advanced option which must only be used in cases where a degraded index is known to be empty and does not therefore need rebuilding. This situation typically arises when an index is created for an attribute which has just been added to the schema.

Default: false

`-i | --index {index}`

Names of index(es) to rebuild. For an attribute index this is simply an attribute name. At least one index must be specified for rebuild. Cannot be used with the "--rebuildAll" option.

`--offline`

Indicates that the command must be run in offline mode.

Default: false

`--rebuildAll`

Rebuild all indexes, including any DN2ID, DN2URI, VLV and extensible indexes. Cannot be used with the "-i" option or the "--rebuildDegraded" option.

Default: false

`--rebuildDegraded`

Rebuild all degraded indexes, including any DN2ID, DN2URI, VLV and extensible indexes. Cannot be used with the "-i" option or the "--rebuildAll" option.

Default: false

`--tmpdirectory {directory}`

Path to temporary directory for index scratch files during index rebuilding.

Default: import-tmp

Task Backend Connection Options

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Task Scheduling Options

`--completionNotify {emailAddress}`

Email address of a recipient to be notified when the task completes. This option may be specified more than once.

`--dependency {taskID}`

ID of a task upon which this task depends. A task will not start execution until all its dependencies have completed execution.

`--errorNotify {emailAddress}`

Email address of a recipient to be notified if an error occurs when this task executes. This option may be specified more than once.

`--failedDependencyAction {action}`

Action this task will take should one if its dependent tasks fail. The value must be one of PROCESS,CANCEL,DISABLE. If not specified defaults to CANCEL.

`--recurringTask {schedulePattern}`

Indicates the task is recurring and will be scheduled according to the value argument expressed in crontab(5) compatible time/date pattern.

`-t | --start {startTime}`

Indicates the date/time at which this operation will start when scheduled as a server task expressed in YYYYMMDDhhmmssZ format for UTC time or YYYYMMDDhhmmss for local time. A value of '0' will cause the task to be scheduled for immediate execution. When this option is

specified the operation will be scheduled to start at the specified time after which this utility will exit immediately.

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following example schedules a task to start immediately that rebuilds the `cn` (common name) index.

```
$ rebuild-index -p 4444 -h opendj.example.com -D "cn=Directory Manager" \
 -w password -b dc=example,dc=com -i cn -t 0
Rebuild Index task 20110607160349596 scheduled to start Jun 7, 2011 4:03:49 PM
```

restore(1)

Name

restore - restore OpenDJ directory data backups

Synopsis

`restore`

Description

This utility can be used to restore a backup of a Directory Server backend.

Options

The `restore` command takes the following options:

Command options:

`-d | --backupDirectory {backupDir}`

Path to the directory containing the backup file(s).

`-I | --backupID {backupID}`

Backup ID of the backup to restore.

`-l | --listBackups`

List available backups in the backup directory.

Default: false

`-n | --dry-run`

Verify the contents of the backup but do not restore it.

Default: false

`--offline`

Indicates that the command must be run in offline mode.

Default: false

Task Backend Connection Options

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Task Scheduling Options

`--completionNotify {emailAddress}`

Email address of a recipient to be notified when the task completes. This option may be specified more than once.

`--dependency {taskID}`

ID of a task upon which this task depends. A task will not start execution until all its dependencies have completed execution.

`--errorNotify {emailAddress}`

Email address of a recipient to be notified if an error occurs when this task executes. This option may be specified more than once.

`--failedDependencyAction {action}`

Action this task will take should one if its dependent tasks fail. The value must be one of PROCESS,CANCEL,DISABLE. If not specified defaults to CANCEL.

`--recurringTask {schedulePattern}`

Indicates the task is recurring and will be scheduled according to the value argument expressed in crontab(5) compatible time/date pattern.

`-t | --start {startTime}`

Indicates the date/time at which this operation will start when scheduled as a server task expressed in YYYYMMDDhhmmssZ format for UTC time or YYYYMMDDhhmmss for local time. A value of '0' will cause the task to be scheduled for immediate execution. When this option is specified the operation will be scheduled to start at the specified time after which this utility will exit immediately.

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following example schedules a restore as a task to begin immediately while OpenDJ directory server is online.

```
$ restore -p 4444 -D "cn=Directory Manager" -w password
 -d /path/to/opendj/bak -I 20110613080032 -t 0
Restore task 20110613155052932 scheduled to start Jun 13, 2011 3:50:52 PM CEST
```

The following example restores data while OpenDJ is offline.

```
$ stop-ds
Stopping Server...
...

$ restore --backupDirectory /path/to/opendj/bak/userRoot \
 --listBackups
Backup ID:          20120928102414Z
Backup Date:        28/Sep/2012:12:24:17 +0200
Is Incremental:     false
Is Compressed:      false
Is Encrypted:       false
Has Unsigned Hash:  false
Has Signed Hash:    false
Dependent Upon:     none

$ restore --backupDirectory /path/to/opendj/bak/userRoot \
 --backupID 20120928102414Z
[28/Sep/2012:12:26:20 +0200] ... msg=Restored: 00000000.jdb (size 355179)

$ start-ds
[28/Sep/2012:12:27:29 +0200] ... The Directory Server has started successfully
```

setup(1)

Name

setup - install OpenDJ directory server

Synopsis

`setup`

Description

This utility can be used to setup the Directory Server.

Options

The `setup` command takes the following options:

Command options:

`-a | --addBaseEntry`

Indicates whether to create the base entry in the Directory Server database.

Default: false

`--acceptLicense`

Automatically accepts the product license (if present).

Default: false

`--adminConnectorPort {port}`

Port on which the Administration Connector should listen for communication.

Default: 4444

`-b | --baseDN {baseDN}`

Base DN for user information in the Directory Server. Multiple base DNs may be provided by using this option multiple times.

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-d | --sampleData {numEntries}`

Specifies that the database should be populated with the specified number of sample entries.

Default: 0

`-D | --rootUserDN {rootUserDN}`

DN for the initial root user for the Directory Server.

Default: cn=Directory Manager

`--generateSelfSignedCertificate`

Generate a self-signed certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

Default: false

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-i | --cli`

Use the command line install. If not specified the graphical interface will be launched. The rest of the options (excluding help and version) will only be taken into account if this option is specified.

Default: false

`-j | --rootUserPasswordFile {rootUserPasswordFile}`

Path to a file containing the password for the initial root user for the Directory Server.

`-l | --ldifFile {ldifFile}`

Path to an LDIF file containing data that should be added to the Directory Server database. Multiple LDIF files may be provided by using this option multiple times.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-O | --doNotStart`

Do not start the server when the configuration is completed.

Default: false

`-p | --ldapPort {port}`

Port on which the Directory Server should listen for LDAP communication.

Default: 1389

`-q | --enableStartTLS`

Enable StartTLS to allow secure communication with the server using the LDAP port.

Default: false

`-R | --rejectFile {rejectFile}`

Write rejected entries to the specified file.

`-S | --skipPortCheck`

Skip the check to determine whether the specified ports are usable.

Default: false

`--skipFile {skipFile}`

Write skipped entries to the specified file.

`-t | --backendType {backendType}`

The type of the userRoot backend.

Default: `je` for standard edition, `pdb` for OEM edition.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate (JKS, JCEKS, PKCS#12 or PKCS#11) as server certificate.

`--useBcfksKeystore {keyStorePath}`

Path of a BCFKS key store containing the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`--useJavaKeystore {keyStorePath}`

Path of a Java Key Store (JKS) containing a certificate to be used as the server certificate. This does not apply to the administration connector, which uses its own key store and certificate (default: config/admin-keystore and admin-cert).

`--useJCEKS {keyStorePath}`

Path of a JCEKS containing a certificate to be used as the server certificate.

`--usePkcs11Keystore`

Use a certificate in a PKCS#11 token that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

Default: false

`--usePkcs12keyStore {keyStorePath}`

Path of a PKCS#12 key store containing the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-w | --rootUserPassword {rootUserPassword}`

Password for the initial root user for the Directory Server.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate (JKS,

JCEKS, PKCS#12 or PKCS#11) as server certificate.

`-x | --jmxPort {jmxPort}`

Port on which the Directory Server should listen for JMX communication.

Default: 1689

`-Z | --ldapsPort {port}`

Port on which the Directory Server should listen for LDAPS communication. The LDAPS port will be configured and SSL will be enabled only if this argument is explicitly specified.

Default: 1636

Utility input/output options:

`-n | --no-prompt`

Use non-interactive mode. If data in the command is missing, the user is not prompted and the tool will fail.

Default: false

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-Q | --quiet`

Use quiet mode.

Default: false

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following command installs OpenDJ directory server, enabling StartTLS and importing 100 example entries without interaction.

```
$ /path/to/opendj/setup --cli -b dc=example,dc=com -d 100 \
 -D "cn=Directory Manager" -w password -h opendj.example.com -p 1389 \
 --generateSelfSignedCertificate --enableStartTLS -n

OpenDJ version
 Please wait while the setup program initializes...

See /var/.../opends-setup-484...561.log for a detailed log of this operation.

Configuring Directory Server ..... Done.
Configuring Certificates ..... Done.
Importing Automatically-Generated Data (100 Entries) ......... Done.
Starting Directory Server .......... Done.

To see basic server configuration status and configuration you can launch
 /path/to/opendj/bin/status
```

start-ds(1)

Name

start-ds - start OpenDJ directory server

Synopsis

`start-ds`

Description

This utility can be used to start the Directory Server, as well as to obtain the server version and other forms of general server information.

Options

The `start-ds` command takes the following options:

Command options:

`-L | --useLastKnownGoodConfig`

Attempt to start using the configuration that was in place at the last successful startup (if it is available) rather than using the current active configuration.

Default: false

`-N | --nodetach`

Do not detach from the terminal and continue running in the foreground. This option cannot be used with the -t, --timeout option.

Default: false

`-s | --systemInfo`

Display general system information.

Default: false

`-t | --timeout {seconds}`

Maximum time (in seconds) to wait before the command returns (the server continues the startup process, regardless). A value of '0' indicates an infinite timeout, which means that the command returns only when the server startup is completed. The default value is 60 seconds. This option cannot be used with the -N, --nodetach option.

Default: 200

Utility input/output options:

`-Q | --quiet`

Use quiet mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following command starts the server without displaying information about the startup process.

```
$ start-ds -Q
```

status(1)

Name

status - display basic OpenDJ server information

Synopsis

`status {options}`

Description

This utility can be used to display basic server information.

Options

The `status` command takes the following options:

Command options:

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Utility input/output options:

`-n | --no-prompt`

Use non-interactive mode. If data in the command is missing, the user is not prompted and the tool will fail.

Default: false

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-r | --refresh {period}`

When this argument is specified, the status command will display its contents periodically. Used to specify the period (in seconds) between two displays of the status.

`-s | --script-friendly`

Use script-friendly mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

```
$ status -D "cn=Directory Manager" -w password

          --- Server Status ---
Server Run Status:        Started
Open Connections:         1

          --- Server Details ---
Host Name:                localhost.localdomain
Administrative Users:     cn=Directory Manager
Installation Path:        /path/to/opendj
Version:                  OpenDJ version
Java Version:             version
Administration Connector: Port 4444 (LDAPS)

          --- Connection Handlers ---
Address:Port : Protocol    : State
-------------:-------------:---------
--           : LDIF        : Disabled
8989         : Replication : Enabled
0.0.0.0:161  : SNMP        : Disabled
0.0.0.0:636  : LDAPS       : Disabled
0.0.0.0:1389 : LDAP        : Enabled
0.0.0.0:1689 : JMX         : Disabled

          --- Data Sources ---
Base DN:                     dc=example,dc=com
Backend ID:                  userRoot
```

```
Entries:                      160
Replication:                  Enabled
Missing Changes:              0
Age of Oldest Missing Change: <not available>

Base DN:     dc=myCompany,dc=com
Backend ID:  myCompanyRoot
Entries:     3
Replication: Disabled

Base DN:     o=myOrg
Backend ID:  myOrgRoot
Entries:     3
Replication: Disabled
```

stop-ds(1)

Name

stop-ds - stop OpenDJ directory server

Synopsis

`stop-ds`

Description

This utility can be used to request that the Directory Server stop running or perform a restart. When run without connection options, this utility sends a signal to the OpenDJ process to stop the server. When run with connection options, this utility connects to the OpenDJ administration port and creates a shutdown task to stop the server.

Options

The `stop-ds` command takes the following options:

Command options:

`-r | --stopReason {stopReason}`

Reason the server is being stopped or restarted.

`-R | --restart`

Attempt to automatically restart the server once it has stopped.

Default: false

`-t | --stopTime {stopTime}`

Indicates the date/time at which the shutdown operation will begin as a server task expressed in format YYYYMMDDhhmmssZ for UTC time or YYYYMMDDhhmmss for local time. A value of '0' will cause the shutdown to be scheduled for immediate execution. When this option is specified the operation will be scheduled to start at the specified time after which this utility will exit immediately.

`-Y | --proxyAs {authzID}`

Use the proxied authorization control with the given authorization ID.

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

`-h | --hostname {host}`

Directory server hostname or IP address.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of certificate for SSL client authentication.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-Q | --quiet`

Use quiet mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following example restarts OpenDJ directory server.

```
$ stop-ds --restart
Stopping Server...

...The Directory Server has started successfully
```

uninstall(1)

Name

uninstall - remove OpenDJ directory server software

Synopsis

`uninstall {options}`

Description

This utility can be used to uninstall the Directory Server.

Options

The `uninstall` command takes the following options:

Command options:

`-a | --remove-all`

Remove all components of the server (this option is not compatible with the rest of remove options).

Default: false

`-b | --backup-files`

Remove backup files.

Default: false

`-c | --configuration-files`

Remove configuration files.

Default: false

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-d | --databases`

Remove database contents.

Default: false

`-e | --ldif-files`

Remove LDIF files.

Default: false

`-f | --forceOnError`

Specifies whether the uninstall should continue if there is an error updating references to this server in remote server instances or not. This option can only be used with the --no-prompt no prompt option.

Default: false

`-i | --cli`

Use the command line install. If not specified the graphical interface will be launched. The rest of the options (excluding help and version) will only be taken into account if this option is specified.

Default: false

`-l | --server-libraries`

Remove Server Libraries and Administrative Tools.

Default: false

`-L | --log-files`

Remove log files.

Default: false

LDAP connection options:

`-h | --referencedHostName {host}`

The name of this host (or IP address) as it is referenced in remote servers for replication.

Default: localhost.localdomain

`-I | --adminUID {adminUID}`

User ID of the Global Administrator to use to bind to the server.

Default: admin

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Utility input/output options:

`-n | --no-prompt`

Use non-interactive mode. If data in the command is missing, the user is not prompted and the tool will fail.

Default: false

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-Q | --quiet`

Use quiet mode.

Default: false

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Examples

The following command removes OpenDJ directory server without interaction.

```
$ /path/to/opendj/uninstall -a --cli -I admin -w password -n

Stopping Directory Server ..... Done.
Deleting Files under the Installation Path ..... Done.

The Uninstall Completed Successfully.
To complete the uninstallation, you must delete manually the following files
and directories:
/path/to/opendj/lib
See /var/.../opends-uninstall-3...0.log for a detailed log of this operation.

$ rm -rf /path/to/opendj
```

upgrade(1)

Name

upgrade - upgrade OpenDJ configuration and application data

Synopsis

`upgrade {options}`

Description

Upgrades OpenDJ configuration and application data so that it is compatible with the installed binaries.

This tool should be run immediately after upgrading the OpenDJ binaries and before restarting the server.

NOTE	this tool does not provide backup or restore capabilities. Therefore, it is the responsibility of the OpenDJ administrator to take necessary precautions before performing the upgrade.

<xinclude:include href="description-upgrade.xml" />

Options

The `upgrade` command takes the following options:

Command options:

`--acceptLicense`

Automatically accepts the product license (if present).

Default: false

`--force`

Forces a non-interactive upgrade to continue even if it requires user interaction. In particular, long running or critical upgrade tasks, such as re-indexing, which require user confirmation will be skipped. This option may only be used with the 'no-prompt' option.

Default: false

`--ignoreErrors`

Ignores any errors which occur during the upgrade. This option should be used with caution and may be useful in automated deployments where potential errors are known in advance and resolved after the upgrade has completed.

Default: false

Utility input/output options:

`-n | --no-prompt`

Use non-interactive mode. If data in the command is missing, the user is not prompted and the tool will fail.

Default: false

`-Q | --quiet`

Use quiet mode.

Default: false

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

2

The command was run in non-interactive mode, but could not complete because confirmation was required to run a long or critical task.

See the error message or the log for details.

other

An error occurred.

See the OpenDJ Installation Guide for an example upgrade process for OpenDJ directory server installed from the cross-platform (.zip) delivery.

Native packages (.deb, .rpm) perform more of the upgrade process, stopping OpenDJ if it is running, overwriting older files with newer files, running this utility, and starting OpenDJ if it was running

when you upgraded the package(s).

verify-index(1)

Name

verify-index - check index for consistency or errors

Synopsis

`verify-index`

Description

This utility can be used to ensure that index data is consistent within an indexed backend database.

Options

The `verify-index` command takes the following options:

Command options:

`-b | --baseDN {baseDN}`

Base DN of a backend supporting indexing. Verification is performed on indexes within the scope of the given base DN.

`-c | --clean`

Specifies that a single index should be verified to ensure it is clean. An index is clean if each index value references only entries containing that value. Only one index at a time may be verified in this way.

Default: false

`--countErrors`

Count the number of errors found during the verification and return that value as the exit code (values > 255 will be reduced to 255 due to exit code restrictions).

Default: false

`-i | --index {index}`

Name of an index to be verified. For an attribute index this is simply an attribute name. Multiple indexes may be verified for completeness, or all indexes if no indexes are specified. An index is complete if each index value references all entries containing that value.

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

Exit Codes

0

The command completed successfully.

1

The command was run in non-interactive mode, but could not complete because confirmation was required to run a long or critical task.

See the error message or the log for details.

0-255

The number of errors in the index, as indicated for the `--countErrors` option.

Examples

The following example shows how to verify the `sn` (surname) index for completeness and for errors. The messages shown are for a backend of type `pdb`. The output is similar for other backend types:

```
$ verify-index -b dc=example,dc=com -i sn --clean --countErrors
[20/05/2015:14:24:18 +0200] category=...PDBStorage seq=0 severity=INFO
 msg=The PDB storage for backend 'userRoot' initialized
 to use 57528 buffers of 16384 bytes (total 920448kb)
[20/05/2015:14:24:18 +0200] category=...pluggable.VerifyJob seq=1 severity=INFO
 msg=Checked 478 records and found 0 error(s) in 0 seconds
 (average rate 3594.0/sec)
[20/05/2015:14:24:18 +0200] category=...pluggable.VerifyJob seq=2 severity=FINE
 msg=Number of records referencing more than one entry: 224
[20/05/2015:14:24:18 +0200] category=...pluggable.VerifyJob seq=3 severity=FINE
 msg=Number of records that exceed the entry limit: 0
[20/05/2015:14:24:18 +0200] category=...pluggable.VerifyJob seq=4 severity=FINE
 msg=Average number of entries referenced is 2.00/record
[20/05/2015:14:24:18 +0200] category=...pluggable.VerifyJob seq=5 severity=FINE
 msg=Maximum number of entries referenced by any record is 32
```

windows-service(1)

Name

windows-service - register OpenDJ as a Windows Service

Synopsis

`windows-service` {options}

Description

This utility can be used to run OpenDJ directory server as a Windows Service.

Service Options

`-c, --cleanupService serviceName`

Disable the service and clean up the windows registry information associated with the provided service name

`-d, --disableService`

Disable the server as a Windows service and stop the server

`-e, --enableService`

Enable the server as a Windows service

`-s, --serviceState`

Provide information about the state of the server as a Windows service

General Options

`-V, --version`

Display version information

`-?, -H, --help`

Display usage information

Exit Codes

0

The command completed successfully.

> 0

An error occurred.

Example

The following command registers OpenDJ directory server as a Windows Service.

```
C:\path\to\opendj\bat> windows-service.bat --enableService
```

After running this command, you can manage the service using Windows administration tools.

---

dsconfig Subcommands Reference

This section covers `dsconfig` subcommands.

dsconfig create-access-log-filtering-criteria(1)

Name

dsconfig create-access-log-filtering-criteria - Creates Access Log Filtering Criteria

Synopsis

`dsconfig create-access-log-filtering-criteria` {options}

Description

Creates Access Log Filtering Criteria.

Options

The `dsconfig create-access-log-filtering-criteria` command takes the following options:

`--publisher-name {name}`

The name of the Access Log Publisher.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

`--criteria-name {name}`

The name of the new Access Log Filtering Criteria.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the `--criteria-name {name}` option.

Access Log Filtering Criteria

Access Log Filtering Criteria of type access-log-filtering-criteria have the following properties:

connection-client-address-equal-to

Description

Filters log records associated with connections which match at least one of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-client-address-not-equal-to

Description

Filters log records associated with connections which do not match any of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-port-equal-to

Description

Filters log records associated with connections to any of the specified listener port numbers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-protocol-equal-to

Description

Filters log records associated with connections which match any of the specified protocols. Typical values include "ldap", "ldaps", or "jmx".

Default Value

None

Allowed Values

The protocol name as reported in the access log.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-type

Description

Filters log records based on their type.

Default Value

None

Allowed Values

abandon

Abandon operations

add

Add operations

bind

Bind operations

compare

Compare operations

connect

Client connections

delete

Delete operations

disconnect

Client disconnections

extended

Extended operations

modify

Modify operations

rename

Rename operations

search

Search operations

unbind

Unbind operations

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-equal-to

Description

Filters operation log records associated with operations which target entries matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-not-equal-to

Description

Filters operation log records associated with operations which target entries matching none of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-greater-than

Description

Filters operation response log records associated with operations which took longer than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-less-than

Description

Filters operation response log records associated with operations which took less than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-equal-to

Description

Filters operation response log records associated with operations which include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-not-equal-to

Description

Filters operation response log records associated with operations which do not include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-is-indexed

Description

Filters search operation response log records associated with searches which were either indexed or unindexed. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-greater-than

Description

Filters search operation response log records associated with searches which returned more than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-less-than

Description

Filters search operation response log records associated with searches which returned less than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-equal-to

Description

Filters log records associated with users matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-not-equal-to

Description

Filters log records associated with users which do not match any of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-member-of

Description

Filters log records associated with users which are members of at least one of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-not-member-of

Description

Filters log records associated with users which are not members of any of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-account-status-notification-handler(1)

Name

dsconfig create-account-status-notification-handler - Creates Account Status Notification Handlers

Synopsis

`dsconfig create-account-status-notification-handler` {options}

Description

Creates Account Status Notification Handlers.

Options

The `dsconfig create-account-status-notification-handler` command takes the following options:

`--handler-name {name}`

The name of the new Account Status Notification Handler.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

`error-log-account-status-notification-handler`

Default {name}: Error Log Account Status Notification Handler

Enabled by default: true

See Error Log Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`smtp-account-status-notification-handler`

Default {name}: SMTP Account Status Notification Handler

Enabled by default: true

See SMTP Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single

value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the `--handler-name {name}` option.

`-t | --type {type}`

The type of Account Status Notification Handler which should be created. The value for TYPE can be one of: custom | error-log | smtp.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

`error-log-account-status-notification-handler`

Default {type}: Error Log Account Status Notification Handler

Enabled by default: true

See Error Log Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`smtp-account-status-notification-handler`

Default {type}: SMTP Account Status Notification Handler

Enabled by default: true

See SMTP Account Status Notification Handler for the properties of this Account Status Notification Handler type.

Error Log Account Status Notification Handler

Account Status Notification Handlers of type error-log-account-status-notification-handler have the following properties:

account-status-notification-type

Description

Indicates which types of event can trigger an account status notification.

Default Value

None

Allowed Values

account-disabled

Generate a notification whenever a user account has been disabled by an administrator.

account-enabled

Generate a notification whenever a user account has been enabled by an administrator.

account-expired

Generate a notification whenever a user authentication has failed because the account has expired.

account-idle-locked

Generate a notification whenever a user account has been locked because it was idle for too long.

account-permanently-locked

Generate a notification whenever a user account has been permanently locked after too many failed attempts.

account-reset-locked

Generate a notification whenever a user account has been locked, because the password had been reset by an administrator but not changed by the user within the required interval.

account-temporarily-locked

Generate a notification whenever a user account has been temporarily locked after too many failed attempts.

account-unlocked

Generate a notification whenever a user account has been unlocked by an administrator.

password-changed

Generate a notification whenever a user changes his/her own password.

password-expired

Generate a notification whenever a user authentication has failed because the password has expired.

password-expiring

Generate a notification whenever a password expiration warning is encountered for a user password for the first time.

password-reset

Generate a notification whenever a user's password is reset by an administrator.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Error Log Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.ErrorLogAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

SMTP Account Status Notification Handler

Account Status Notification Handlers of type smtp-account-status-notification-handler have the following properties:

email-address-attribute-type

Description

Specifies which attribute in the user's entries may be used to obtain the email address when notifying the end user. You can specify more than one email address as separate values. In this case, the OpenDJ server sends a notification to all email addresses identified.

Default Value

If no email address attribute types are specified, then no attempt is made to send email notification messages to end users. Only those users specified in the set of additional recipient addresses are sent the notification messages.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.SMTPAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this

setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this account status notification handler. The values for this property should begin with the name of an account status notification type followed by a colon and the subject that should be used for the associated notification message. If an email message is generated for an account status notification type for which no subject is defined, then that message is given a generic subject.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-template-file

Description

Specifies the path to the file containing the message template to generate the email notification messages. The values for this property should begin with the name of an account status notification type followed by a colon and the path to the template file that should be used for that notification type. If an account status notification has a notification type that is not associated with a message template file, then no email message is generated for that notification.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which notification messages are sent, either instead of or in addition to the end user for whom the notification has been generated. This may be used to ensure that server administrators also receive a copy of any notification messages that are generated.

Default Value

If no additional recipient addresses are specified, then only the end users that are the subjects of the account status notifications receive the notification messages.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

send-email-as-html

Description

Indicates whether an email notification message should be sent as HTML. If this value is true, email notification messages are marked as text/html. Otherwise outgoing email messages are assumed to be plaintext and marked as text/plain.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-message-without-end-user-address

Description

Indicates whether an email notification message should be generated and sent to the set of notification recipients even if the user entry does not contain any values for any of the email address attributes (that is, in cases when it is not be possible to notify the end user). This is only applicable if both one or more email address attribute types and one or more additional recipient addresses are specified.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

sender-address

Description

Specifies the email address from which the message is sent. Note that this does not necessarily have to be a legitimate email address.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-alert-handler(1)

Name

dsconfig create-alert-handler - Creates Alert Handlers

Synopsis

`dsconfig create-alert-handler` {options}

Description

Creates Alert Handlers.

Options

The `dsconfig create-alert-handler` command takes the following options:

`--handler-name {name}`

The name of the new Alert Handler.

Alert Handler properties depend on the Alert Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

`jmx-alert-handler`

Default {name}: JMX Alert Handler

Enabled by default: true

See JMX Alert Handler for the properties of this Alert Handler type.

`smtp-alert-handler`

Default {name}: SMTP Alert Handler

Enabled by default: true

See SMTP Alert Handler for the properties of this Alert Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Alert Handler properties depend on the Alert Handler type, which depends on the `--handler-name {name}` option.

`-t | --type {type}`

The type of Alert Handler which should be created. The value for TYPE can be one of: custom | jmx | smtp.

Alert Handler properties depend on the Alert Handler type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

`jmx-alert-handler`

Default {type}: JMX Alert Handler

Enabled by default: true

See JMX Alert Handler for the properties of this Alert Handler type.

`smtp-alert-handler`

Default {type}: SMTP Alert Handler

Enabled by default: true

See SMTP Alert Handler for the properties of this Alert Handler type.

JMX Alert Handler

Alert Handlers of type jmx-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Alert Handler implementation.

Default Value

org.opends.server.extensions.JMXAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

SMTP Alert Handler

Alert Handlers of type smtp-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Alert Handler implementation.

Default Value

org.opends.server.extensions.SMTPAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-body

Description

Specifies the body that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which the messages should be sent. Multiple values may be provided if there should be more than one recipient.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

sender-address

Description

Specifies the email address to use as the sender for messages generated by this alert handler.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-backend(1)

Name

dsconfig create-backend - Creates Backends

Synopsis

`dsconfig create-backend` {options}

Description

Creates Backends.

Options

The `dsconfig create-backend` command takes the following options:

`--backend-name {STRING}`

The name of the new Backend which will also be used as the value of the "backend-id" property: Specifies a name to identify the associated backend.

Backend properties depend on the Backend type, which depends on the {STRING} you provide.

By default, OpenDJ directory server supports the following Backend types:

`backup-backend`

Default {STRING}: Backup Backend

Enabled by default: true

See Backup Backend for the properties of this Backend type.

`cas-backend`

Default {STRING}: CAS Backend

Enabled by default: true

See CAS Backend for the properties of this Backend type.

`jdbc-backend`

Default {STRING}: JDBC Backend

Enabled by default: true

See JDBC Backend for the properties of this Backend type.

`je-backend`

Default {STRING}: JE Backend

Enabled by default: true

See JE Backend for the properties of this Backend type.

`ldif-backend`

Default {STRING}: LDIF Backend

Enabled by default: true

See LDIF Backend for the properties of this Backend type.

`memory-backend`

Default {STRING}: Memory Backend

Enabled by default: true

See Memory Backend for the properties of this Backend type.

`monitor-backend`

Default {STRING}: Monitor Backend

Enabled by default: true

See Monitor Backend for the properties of this Backend type.

`null-backend`

Default {STRING}: Null Backend

Enabled by default: true

See Null Backend for the properties of this Backend type.

`pdb-backend`

Default {STRING}: PDB Backend

Enabled by default: true

See PDB Backend for the properties of this Backend type.

`schema-backend`

Default {STRING}: Schema Backend

Enabled by default: true

See Schema Backend for the properties of this Backend type.

`task-backend`

Default {STRING}: Task Backend

Enabled by default: true

See Task Backend for the properties of this Backend type.

`trust-store-backend`

Default {STRING}: Trust Store Backend

Enabled by default: true

See Trust Store Backend for the properties of this Backend type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Backend properties depend on the Backend type, which depends on the `--backend-name {STRING}` option.

`-t | --type {type}`

The type of Backend which should be created. The value for TYPE can be one of: backup | cas | custom | custom-local | jdbc | je | ldif | memory | monitor | null | pdb | schema | task | trust-store.

Backend properties depend on the Backend type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Backend types:

`backup-backend`

Default {type}: Backup Backend

Enabled by default: true

See Backup Backend for the properties of this Backend type.

`cas-backend`

Default {type}: CAS Backend

Enabled by default: true

See CAS Backend for the properties of this Backend type.

`jdbc-backend`

Default {type}: JDBC Backend

Enabled by default: true

See JDBC Backend for the properties of this Backend type.

`je-backend`

Default {type}: JE Backend

Enabled by default: true

See JE Backend for the properties of this Backend type.

`ldif-backend`

Default {type}: LDIF Backend

Enabled by default: true

See LDIF Backend for the properties of this Backend type.

`memory-backend`

Default {type}: Memory Backend

Enabled by default: true

See Memory Backend for the properties of this Backend type.

`monitor-backend`

Default {type}: Monitor Backend

Enabled by default: true

See Monitor Backend for the properties of this Backend type.

`null-backend`

Default {type}: Null Backend

Enabled by default: true

See Null Backend for the properties of this Backend type.

`pdb-backend`

Default {type}: PDB Backend

Enabled by default: true

See PDB Backend for the properties of this Backend type.

`schema-backend`

Default {type}: Schema Backend

Enabled by default: true

See Schema Backend for the properties of this Backend type.

`task-backend`

Default {type}: Task Backend

Enabled by default: true

See Task Backend for the properties of this Backend type.

`trust-store-backend`

Default {type}: Trust Store Backend

Enabled by default: true

See Trust Store Backend for the properties of this Backend type.

Backup Backend

Backends of type backup-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

backup-directory

Description

Specifies the path to a backup directory containing one or more backups for a particular backend. This is a multivalued property. Each value may specify a different backup directory if desired (one for each backend for which backups are taken). Values may be either absolute paths or paths that are relative to the base of the OpenDJ directory server installation.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.BackupBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

CAS Backend

Backends of type cas-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to

supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-directory

Description

Specifies the keyspace name The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

ldap_opendj

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.cassandra.Backend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

JDBC Backend

Backends of type jdbc-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using

NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-directory

Description

Specifies the connection string jdbc:postgresql://localhost/test

Default Value

jdbc:postgresql://localhost/test

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained

in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.jdbc.Backend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

JE Backend

Backends of type je-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-bytes-interval

Description

Specifies the maximum number of bytes that may be written to the database before it is forced to perform a checkpoint. This can be used to bound the recovery time that may be required if the database environment is opened without having been properly closed. If this property is set to a non-zero value, the checkpointer wakeup interval is not used. To use time-based checkpointing, set this property to zero.

Default Value

500mb

Allowed Values

Upper value is 9223372036854775807.

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. Note that this is only used if the value of the checkpointer bytes interval is zero.

Default Value

30s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.Upper limit is 4294 seconds.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-cleaner-min-utilization

Description

Specifies the occupancy percentage for "live" data in this backend's database. When the amount of "live" data in the database drops below this value, cleaners will act to increase the occupancy percentage by compacting the database.

Default Value

50

Allowed Values

An integer value. Lower value is 0. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Berkeley DB Java Edition database files containing the data for this backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-core-threads

Description

Specifies the core number of threads in the eviction thread pool. Specifies the core number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-

threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

1

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-keep-alive

Description

The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

600s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.Upper limit is 86400 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-lru-only

Description

Indicates whether the database should evict existing data from the cache based on an LRU policy (where the least recently used information will be evicted first). If set to "false", then the eviction keeps internal nodes of the underlying Btree in the cache over leaf nodes, even if the leaf nodes have been accessed more recently. This may be a better configuration for databases in which only a very small portion of the data is cached.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-max-threads

Description

Specifies the maximum number of threads in the eviction thread pool. Specifies the maximum number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-nodes-per-scan

Description

Specifies the number of Btree nodes that should be evicted from the cache in a single pass if it is determined that it is necessary to free existing data in order to make room for new information. Changes to this property do not take effect until the backend is restarted. It is recommended that you also change this property when you set db-evictor-lru-only to false. This setting controls the number of Btree nodes that are considered, or sampled, each time a node is evicted. A setting of 10 often produces good results, but this may vary from application to application. The larger the nodes per scan, the more accurate the algorithm. However, don't set it too high. When considering larger numbers of nodes for each eviction, the evictor may delay the completion of a given database operation, which impacts the response time of the application thread. In JE 4.1 and later, setting this value too high in an application that is largely CPU bound can reduce the effectiveness of cache eviction. It's best to start with the default value, and increase it gradually to see if it is beneficial for your application.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 1000.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-file-max

Description

Specifies the maximum size for a database log file.

Default Value

100mb

Allowed Values

Lower value is 1000000.Upper value is 4294967296.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-filecache-size

Description

Specifies the size of the file handle cache. The file handle cache is used to keep as much opened log files as possible. When the cache is smaller than the number of logs, the database needs to close some handles and open log files it needs, resulting in less optimal performances. Ideally, the size of the cache should be higher than the number of files contained in the database. Make sure the OS number of open files per process is also tuned appropriately.

Default Value

100

Allowed Values

An integer value. Lower value is 3. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-file-handler-on

Description

Indicates whether the database should maintain a je.info file in the same directory as the database log directory. This file contains information about the internal processing performed by the underlying database.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-level

Description

Specifies the log level that should be used by the database when it is writing information into the je.info file. The database trace logging level is (in increasing order of verbosity) chosen from:

OFF, SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST, ALL.

Default Value

CONFIG

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-cleaner-threads

Description

Specifies the number of threads that the backend should maintain to keep the database log files at or near the desired utilization. In environments with high write throughput, multiple cleaner threads may be required to maintain the desired utilization.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-lock-tables

Description

Specifies the number of lock tables that are used by the underlying database. This can be particularly important to help improve scalability by avoiding contention on systems with large numbers of CPUs. The value of this configuration property should be set to a prime number that is less than or equal to the number of worker threads configured for use in the server.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 32767.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-run-cleaner

Description

Indicates whether the cleaner threads should be enabled to compact the database. The cleaner threads are used to periodically compact the database when it reaches a percentage of occupancy lower than the amount specified by the db-cleaner-min-utilization property. They identify database files with a low percentage of live data, and relocate their remaining live data to the end of the log.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-write-no-sync

Description

Indicates whether the database should synchronously flush data as it is written to disk. If this value is set to "false", then all data written to disk is synchronously flushed to persistent storage and thereby providing full durability. If it is set to "true", then data may be cached for a period of time by the underlying operating system before actually being written to disk. This may improve performance, but could cause the most recent changes to be lost in the event of an underlying OS or hardware failure (but not in the case that the OpenDJ directory server or the JVM exits abnormally).

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.jeb.JEBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

je-property

Description

Specifies the database and environment properties for the Berkeley DB Java Edition database serving the data for this backend. Any Berkeley DB Java Edition property can be specified using

the following form: property-name=property-value. Refer to OpenDJ documentation for further information on related properties, their implications, and range values. The definitive identification of all the property parameters is available in the example.properties file of Berkeley DB Java Edition distribution.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

LDIF Backend

Backends of type ldif-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

is-private-backend

Description

Indicates whether the backend should be considered a private backend, which indicates that it is used for storing operational data rather than user-defined information.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.LDIFBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-file

Description

Specifies the path to the LDIF file containing the data for this backend.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Memory Backend

Backends of type memory-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base

DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MemoryBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Monitor Backend

Backends of type monitor-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MonitorBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Null Backend

Backends of type null-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.NullBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

PDB Backend

Backends of type pdb-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. This setting controls the elapsed time between attempts to write a checkpoint to the journal. A longer interval allows more updates to accumulate in buffers before they are required to be written to disk, but also potentially causes recovery from an abrupt termination (crash) to take more time.

Default Value

15s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 10 seconds.Upper limit is 3600 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Persistit database files containing the data for this backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the

directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the

index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.pdb.PDBBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Schema Backend

Backends of type schema-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.SchemaBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

schema-entry-dn

Description

Defines the base DNs of the subtrees in which the schema information is published in addition to the value included in the base-dn property. The value provided in the base-dn property is the only one that appears in the subschemaSubentry operational attribute of the server's root DSE (which is necessary because that is a single-valued attribute) and as a virtual attribute in other entries. The schema-entry-dn attribute may be used to make the schema information available in other locations to accommodate certain client applications that have been hard-coded to expect the schema to reside in a specific location.

Default Value

cn=schema

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

show-all-attributes

Description

Indicates whether to treat all attributes in the schema entry as if they were user attributes regardless of their configuration. This may provide compatibility with some applications that expect schema attributes like attributeTypes and objectClasses to be included by default even if they are not requested. Note that the ldapSyntaxes attribute is always treated as operational in order to avoid problems with attempts to modify the schema over protocol.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Task Backend

Backends of type task-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.task.TaskBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

notification-sender-address

Description

Specifies the email address to use as the sender (that is, the "From:" address) address for notification mail messages generated when a task completes execution.

Default Value

The default sender address used is "opendj-task-notification@" followed by the canonical address of the system on which the server is running.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

task-backing-file

Description

Specifies the path to the backing file for storing information about the tasks configured in the server. It may be either an absolute path or a relative path to the base of the OpenDJ directory server instance.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

task-retention-time

Description

Specifies the length of time that task entries should be retained after processing on the associated task has been completed.

Default Value

24 hours

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Trust Store Backend

Backends of type trust-store-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base

DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.TrustStoreBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file that stores the trust information. It may be an absolute path, or a path that is relative to the OpenDJ instance root.

Default Value

config/ads-truststore

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the

Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well.

Default Value

The JVM default value is used.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect the next time that the key manager is accessed.

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-backend-index(1)

Name

dsconfig create-backend-index - Creates Backend Indexes

Synopsis

`dsconfig create-backend-index` {options}

Description

Creates Backend Indexes.

Options

The `dsconfig create-backend-index` command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend Index properties depend on the Backend Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default {name}: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

`--index-name {OID}`

The name of the new Backend Index which will also be used as the value of the "attribute" property: Specifies the name of the attribute for which the index is to be maintained.

Backend Index properties depend on the Backend Index type, which depends on the {OID} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default {OID}: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Backend Index properties depend on the Backend Index type, which depends on the `--index-name {OID}` option.

Backend Index

Backend Indexes of type backend-index have the following properties:

attribute

Description

Specifies the name of the attribute for which the index is to be maintained.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

confidentiality-enabled

Description

Specifies whether contents of the index should be confidential. Setting the flag to true will hash keys for equality type indexes using SHA-1 and encrypt the list of entries matching a substring key for substring indexes.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

If the index for the attribute must be protected for security purposes and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate. The property cannot be set on a backend for which confidentiality is not enabled.

Advanced Property

No

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that are allowed to match a given index key before that particular index key is no longer maintained. This is analogous to the ALL IDs threshold in the Sun Java System Directory Server. If this is specified, its value overrides the JE backend-wide configuration. For no limit, use 0 for the value.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

If any index keys have already reached this limit, indexes must be rebuilt before they will be allowed to use the new limit.

Advanced Property

No

Read-only

No

index-extensible-matching-rule

Description

The extensible matching rule in an extensible index. An extensible matching rule must be specified using either LOCALE or OID of the matching rule.

Default Value

No extensible matching rules will be indexed.

Allowed Values

A Locale or an OID.

Multi-valued

Yes

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

No

Read-only

No

index-type

Description

Specifies the type(s) of indexing that should be performed for the associated attribute. For equality, presence, and substring index types, the associated attribute type must have a corresponding matching rule.

Default Value

None

Allowed Values

approximate

This index type is used to improve the efficiency of searches using approximate matching search filters.

equality

This index type is used to improve the efficiency of searches using equality search filters.

extensible

This index type is used to improve the efficiency of searches using extensible matching search filters.

ordering

This index type is used to improve the efficiency of searches using "greater than or equal to" or "less then or equal to" search filters.

presence

This index type is used to improve the efficiency of searches using the presence search filters.

substring

This index type is used to improve the efficiency of searches using substring search filters.

Multi-valued

Yes

Required

Yes

Admin Action Required

If any new index types are added for an attribute, and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate.

Advanced Property

No

Read-only

No

substring-length

Description

The length of substrings in a substring index.

Default Value

6

Allowed Values

An integer value. Lower value is 3.

Multi-valued

No

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-backend-vlv-index(1)

Name

dsconfig create-backend-vlv-index - Creates Backend VLV Indexes

Synopsis

`dsconfig create-backend-vlv-index` {options}

Description

Creates Backend VLV Indexes.

Options

The `dsconfig create-backend-vlv-index` command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default {name}: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

`--index-name {STRING}`

The name of the new Backend VLV Index which will also be used as the value of the "name" property: Specifies a unique name for this VLV index.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {STRING} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default {STRING}: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the `--index-name {STRING}` option.

Backend VLV Index

Backend VLV Indexes of type backend-vlv-index have the following properties:

base-dn

Description

Specifies the base DN used in the search query that is being indexed.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

filter

Description

Specifies the LDAP filter used in the query that is being indexed.

Default Value

None

Allowed Values

A valid LDAP search filter.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

name

Description

Specifies a unique name for this VLV index.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

NoneThe VLV index name cannot be altered after the index is created.

Advanced Property

No

Read-only

Yes

scope

Description

Specifies the LDAP scope of the query that is being indexed.

Default Value

None

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

sort-order

Description

Specifies the names of the attributes that are used to sort the entries for the query being indexed. Multiple attributes can be used to determine the sort order by listing the attribute names from highest to lowest precedence. Optionally, + or - can be prefixed to the attribute name to sort the attribute in ascending order or descending order respectively.

Default Value

None

Allowed Values

Valid attribute types defined in the schema, separated by a space and optionally prefixed by + or -.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

dsconfig create-certificate-mapper(1)

Name

dsconfig create-certificate-mapper - Creates Certificate Mappers

Synopsis

`dsconfig create-certificate-mapper` {options}

Description

Creates Certificate Mappers.

Options

The `dsconfig create-certificate-mapper` command takes the following options:

`--mapper-name {name}`

The name of the new Certificate Mapper.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

`fingerprint-certificate-mapper`

Default {name}: Fingerprint Certificate Mapper

Enabled by default: true

See Fingerprint Certificate Mapper for the properties of this Certificate Mapper type.

`subject-attribute-to-user-attribute-certificate-mapper`

Default {name}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See Subject Attribute To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-dn-to-user-attribute-certificate-mapper`

Default {name}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See Subject DN To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-equals-dn-certificate-mapper`

Default {name}: Subject Equals DN Certificate Mapper

Enabled by default: true

See Subject Equals DN Certificate Mapper for the properties of this Certificate Mapper type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the `--mapper-name {name}` option.

`-t | --type {type}`

The type of Certificate Mapper which should be created. The value for TYPE can be one of: custom | fingerprint | subject-attribute-to-user-attribute | subject-dn-to-user-attribute | subject-equals-dn.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

`fingerprint-certificate-mapper`

Default {type}: Fingerprint Certificate Mapper

Enabled by default: true

See Fingerprint Certificate Mapper for the properties of this Certificate Mapper type.

`subject-attribute-to-user-attribute-certificate-mapper`

Default {type}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See Subject Attribute To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-dn-to-user-attribute-certificate-mapper`

Default {type}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See Subject DN To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-equals-dn-certificate-mapper`

Default {type}: Subject Equals DN Certificate Mapper

Enabled by default: true

See Subject Equals DN Certificate Mapper for the properties of this Certificate Mapper type.

Fingerprint Certificate Mapper

Certificate Mappers of type fingerprint-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-algorithm

Description

Specifies the name of the digest algorithm to compute the fingerprint of client certificates.

Default Value

None

Allowed Values

md5

Use the MD5 digest algorithm to compute certificate fingerprints.

sha1

Use the SHA-1 digest algorithm to compute certificate fingerprints.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-attribute

Description

Specifies the attribute in which to look for the fingerprint. Values of the fingerprint attribute should exactly match the MD5 or SHA1 representation of the certificate fingerprint.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fingerprint Certificate Mapper implementation.

Default Value

org.opends.server.extensions.FingerprintCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs are used when performing searches to map the client certificates to a user entry.

Default Value

The server performs the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subject Attribute To User Attribute Certificate Mapper

Certificate Mappers of type subject-attribute-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Attribute To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectAttributeToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute-mapping

Description

Specifies a mapping between certificate attributes and user attributes. Each value should be in the form "certattr:userattr" where certattr is the name of the attribute in the certificate subject and userattr is the name of the corresponding attribute in user entries. There may be multiple mappings defined, and when performing the mapping values for all attributes present in the certificate subject that have mappings defined must be present in the corresponding user entries.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subject DN To User Attribute Certificate Mapper

Certificate Mappers of type subject-dn-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject DN To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectDNToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute

Description

Specifies the name or OID of the attribute whose value should exactly match the certificate subject DN.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subject Equals DN Certificate Mapper

Certificate Mappers of type subject-equals-dn-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Equals DN Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectEqualsDNCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-connection-handler(1)

Name

dsconfig create-connection-handler - Creates Connection Handlers

Synopsis

`dsconfig create-connection-handler` {options}

Description

Creates Connection Handlers.

Options

The `dsconfig create-connection-handler` command takes the following options:

`--handler-name {name}`

The name of the new Connection Handler.

Connection Handler properties depend on the Connection Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

`http-connection-handler`

Default {name}: HTTP Connection Handler

Enabled by default: true

See HTTP Connection Handler for the properties of this Connection Handler type.

`jmx-connection-handler`

Default {name}: JMX Connection Handler

Enabled by default: true

See JMX Connection Handler for the properties of this Connection Handler type.

`ldap-connection-handler`

Default {name}: LDAP Connection Handler

Enabled by default: true

See LDAP Connection Handler for the properties of this Connection Handler type.

`ldif-connection-handler`

Default {name}: LDIF Connection Handler

Enabled by default: true

See LDIF Connection Handler for the properties of this Connection Handler type.

`snmp-connection-handler`

Default {name}: SNMP Connection Handler

Enabled by default: true

See SNMP Connection Handler for the properties of this Connection Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Connection Handler properties depend on the Connection Handler type, which depends on the `--handler-name {name}` option.

`-t | --type {type}`

The type of Connection Handler which should be created. The value for TYPE can be one of: custom | http | jmx | ldap | ldif | snmp.

Connection Handler properties depend on the Connection Handler type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

`http-connection-handler`

Default {type}: HTTP Connection Handler

Enabled by default: true

See HTTP Connection Handler for the properties of this Connection Handler type.

`jmx-connection-handler`

Default {type}: JMX Connection Handler

Enabled by default: true

See JMX Connection Handler for the properties of this Connection Handler type.

`ldap-connection-handler`

Default {type}: LDAP Connection Handler

Enabled by default: true

See LDAP Connection Handler for the properties of this Connection Handler type.

`ldif-connection-handler`

Default {type}: LDIF Connection Handler

Enabled by default: true

See LDIF Connection Handler for the properties of this Connection Handler type.

`snmp-connection-handler`

Default {type}: SNMP Connection Handler

Enabled by default: true

See SNMP Connection Handler for the properties of this Connection Handler type.

HTTP Connection Handler

Connection Handlers of type http-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the HTTP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the HTTP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer HTTP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or

more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Connection Handler implementation.

Default Value

org.opends.server.protocols.http.HTTPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the HTTP Connection Handler should keep statistics. If enabled, the HTTP Connection Handler maintains statistics about the number and types of operations requested over HTTP and the amount of data sent and received.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this HTTP Connection Handler should listen for connections from HTTP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the HTTP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the HTTP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to HTTP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-concurrent-ops-per-connection

Description

Specifies the maximum number of internal operations that each HTTP client connection can execute concurrently. This property allow to limit the impact that each HTTP request can have on the whole server by limiting the number of internal operations that each HTTP request can execute concurrently. A value of 0 means that no limit is enforced.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest HTTP request message that will be allowed by the HTTP Connection Handler. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The HTTP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck

when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the HTTP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the HTTP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the HTTP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the HTTP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the HTTP Connection Handler should use SSL. If enabled, the HTTP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the HTTP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the HTTP Connection Handler should use TCP no-delay. If enabled, the

TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

JMX Connection Handler

Connection Handlers of type jmx-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Connection Handler implementation.

Default Value

org.opends.server.protocols.jmx.JmxConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this JMX Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the JMX Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address on which this JMX Connection Handler should listen for connections from JMX clients. If no value is provided, then the JMX Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the JMX Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

rmi-port

Description

Specifies the port number on which the JMX RMI service will listen for connections from clients. A value of 0 indicates the service to choose a port of its own. If the value provided is different than 0, the value will be used as the RMI port. Otherwise, the RMI service will choose a port of its own.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the JMX Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the JMX Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the JMX Connection Handler should use SSL. If enabled, the JMX Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

LDAP Connection Handler

Connection Handlers of type ldap-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-ldap-v2

Description

Indicates whether connections from LDAPv2 clients are allowed. If LDAPv2 clients are allowed, then only a minimal degree of special support are provided for them to ensure that LDAPv3-specific protocol elements (for example, Configuration Guide 25 controls, extended response messages, intermediate response messages, referrals) are not sent to an LDAPv2 client.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-start-tls

Description

Indicates whether clients are allowed to use StartTLS. If enabled, the LDAP Connection Handler allows clients to use the StartTLS extended operation to initiate secure communication over an otherwise insecure channel. Note that this is only allowed if the LDAP Connection Handler is not configured to use SSL, and if the server is configured with a valid key manager provider and a valid trust manager provider.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the LDAP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the LDAP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer LDAP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDAP Connection Handler implementation.

Default Value

org.opends.server.protocols.ldap.LDAPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the LDAP Connection Handler should keep statistics. If enabled, the LDAP Connection Handler maintains statistics about the number and types of operations requested over LDAP and the amount of data sent and received.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this LDAP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this LDAP Connection Handler should listen for connections from LDAP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the LDAP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the LDAP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to LDAP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest LDAP request message that will be allowed by this LDAP Connection handler. This property is analogous to the maxBERSize configuration attribute of the Sun Java System Directory Server. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The LDAP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-rejection-notice

Description

Indicates whether the LDAP Connection Handler should send a notice of disconnection extended response message to the client if a new connection is rejected for some reason. The extended response message may provide an explanation indicating the reason that the connection was rejected.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the LDAP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the LDAP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the LDAP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the LDAP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Connection Handler should use SSL. If enabled, the LDAP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the LDAP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the LDAP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

LDIF Connection Handler

Connection Handlers of type ldif-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDIF Connection Handler implementation.

Default Value

org.opends.server.protocols.LDIFConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-directory

Description

Specifies the path to the directory in which the LDIF files should be placed.

Default Value

config/auto-process-ldif

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

poll-interval

Description

Specifies how frequently the LDIF connection handler should check the LDIF directory to determine whether a new LDIF file has been added.

Default Value

5 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

SNMP Connection Handler

Connection Handlers of type snmp-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

allowed-manager

Description

Specifies the hosts of the managers to be granted the access rights. This property is required for SNMP v1 and v2 security configuration. An asterisk (*) opens access to all managers.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

allowed-user

Description

Specifies the users to be granted the access rights. This property is required for SNMP v3 security configuration. An asterisk (*) opens access to all users.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

community

Description

Specifies the v1,v2 community or the v3 context name allowed to access the MIB 2605 monitoring information or the USM MIB. The mapping between "community" and "context name" is set.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SNMP Connection Handler implementation.

Default Value

org.opends.server.snmp.SNMPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this SNMP Connection Handler should listen for connections from SNMP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the SNMP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

Yes

listen-port

Description

Specifies the port number on which the SNMP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

opendmk-jarfile

Description

Indicates the OpenDMK runtime jar file location

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

registered-mbean

Description

Indicates whether the SNMP objects have to be registered in the directory server MBeanServer or not allowing to access SNMP Objects with RMI connector if enabled.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-agent-file

Description

Specifies the USM security configuration to receive authenticated only SNMP requests.

Default Value

config/snmp/security/opendj-snmp.security

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-level

Description

Specifies the type of security level : NoAuthNoPriv : No security mechanisms activated, AuthNoPriv : Authentication activated with no privacy, AuthPriv : Authentication with privacy activated. This property is required for SNMP V3 security configuration.

Default Value

authnopriv

Allowed Values

authnopriv

Authentication activated with no privacy.

authpriv

Authentication with privacy activated.

noauthnopriv

No security mechanisms activated.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trap-port

Description

Specifies the port to use to send SNMP Traps.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-community

Description

Specifies the community string that must be included in the traps sent to define managers (trap-destinations). This property is used in the context of SNMP v1, v2 and v3.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-destination

Description

Specifies the hosts to which V1 traps will be sent. V1 Traps are sent to every host listed. If this list is empty, V1 traps are sent to "localhost". Each host in the list must be identifed by its name or complete IP Addess.

Default Value

If the list is empty, V1 traps are sent to "localhost".

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig create-debug-target(1)

Name

dsconfig create-debug-target - Creates Debug Targets

Synopsis

`dsconfig create-debug-target` {options}

Description

Creates Debug Targets.

Options

The `dsconfig create-debug-target` command takes the following options:

`--publisher-name {name}`

The name of the Debug Log Publisher.

Debug Target properties depend on the Debug Target type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default {name}: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

`--target-name {STRING}`

The name of the new Debug Target which will also be used as the value of the "debug-scope" property: Specifies the fully-qualified OpenDJ Java package, class, or method affected by the settings in this target definition. Use the number character (#) to separate the class name and the method name (that is, org.opends.server.core.DirectoryServer#startUp).

Debug Target properties depend on the Debug Target type, which depends on the {STRING} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default {STRING}: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Debug Target properties depend on the Debug Target type, which depends on the `--target-name {STRING}` option.

Debug Target

Debug Targets of type debug-target have the following properties:

debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

debug-scope

Description

Specifies the fully-qualified OpenDJ Java package, class, or method affected by the settings in this target definition. Use the number character (#) to separate the class name and the method name (that is, org.opends.server.core.DirectoryServer#startUp).

Default Value

None

Allowed Values

The fully-qualified OpenDJ Java package, class, or method name.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the Debug Target is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

include-throwable-cause

Description

Specifies the property to indicate whether to include the cause of exceptions in exception thrown and caught messages.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-entry-arguments

Description

Specifies the property to indicate whether to include method arguments in debug messages.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-return-value

Description

Specifies the property to indicate whether to include the return value in debug messages.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

throwable-stack-frames

Description

Specifies the property to indicate the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

0

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-entry-cache(1)

Name

dsconfig create-entry-cache - Creates Entry Caches

Synopsis

`dsconfig create-entry-cache` {options}

Description

Creates Entry Caches.

Options

The `dsconfig create-entry-cache` command takes the following options:

`--cache-name {name}`

The name of the new Entry Cache.

Entry Cache properties depend on the Entry Cache type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

`fifo-entry-cache`

Default {name}: FIFO Entry Cache

Enabled by default: true

See FIFO Entry Cache for the properties of this Entry Cache type.

`soft-reference-entry-cache`

Default {name}: Soft Reference Entry Cache

Enabled by default: true

See Soft Reference Entry Cache for the properties of this Entry Cache type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Entry Cache properties depend on the Entry Cache type, which depends on the `--cache-name {name}` option.

`-t | --type {type}`

The type of Entry Cache which should be created. The value for TYPE can be one of: custom | fifo | soft-reference.

Entry Cache properties depend on the Entry Cache type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

`fifo-entry-cache`

Default {type}: FIFO Entry Cache

Enabled by default: true

See FIFO Entry Cache for the properties of this Entry Cache type.

`soft-reference-entry-cache`

Default {type}: Soft Reference Entry Cache

Enabled by default: true

See Soft Reference Entry Cache for the properties of this Entry Cache type.

FIFO Entry Cache

Entry Caches of type fifo-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the FIFO Entry Cache implementation.

Default Value

org.opends.server.extensions.FIFOEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time to wait while attempting to acquire a read or write lock.

Default Value

2000.0ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-entries

Description

Specifies the maximum number of entries that we will allow in the cache.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-memory-percent

Description

Specifies the maximum percentage of JVM memory used by the server before the entry caches stops caching and begins purging itself. Very low settings such as 10 or 20 (percent) can prevent this entry cache from having enough space to hold any of the entries to cache, making it appear that the server is ignoring or skipping the entry cache entirely.

Default Value

90

Allowed Values

An integer value. Lower value is 1. Upper value is 100.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Soft Reference Entry Cache

Entry Caches of type soft-reference-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Soft Reference Entry Cache implementation.

Default Value

org.opends.server.extensions.SoftReferenceEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time in milliseconds to wait while attempting to acquire a read or write lock.

Default Value

3000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-extended-operation-handler(1)

Name

dsconfig create-extended-operation-handler - Creates Extended Operation Handlers

Synopsis

`dsconfig create-extended-operation-handler` {options}

Description

Creates Extended Operation Handlers.

Options

The `dsconfig create-extended-operation-handler` command takes the following options:

`--handler-name {name}`

The name of the new Extended Operation Handler.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

`cancel-extended-operation-handler`

Default {name}: Cancel Extended Operation Handler

Enabled by default: true

See Cancel Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-connection-id-extended-operation-handler`

Default {name}: Get Connection Id Extended Operation Handler

Enabled by default: true

See Get Connection Id Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-symmetric-key-extended-operation-handler`

Default {name}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See Get Symmetric Key Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-modify-extended-operation-handler`

Default {name}: Password Modify Extended Operation Handler

Enabled by default: true

See Password Modify Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-policy-state-extended-operation-handler`

Default {name}: Password Policy State Extended Operation Handler

Enabled by default: true

See Password Policy State Extended Operation Handler for the properties of this Extended Operation Handler type.

`start-tls-extended-operation-handler`

Default {name}: Start TLS Extended Operation Handler

Enabled by default: true

See Start TLS Extended Operation Handler for the properties of this Extended Operation Handler type.

`who-am-i-extended-operation-handler`

Default {name}: Who Am I Extended Operation Handler

Enabled by default: true

See Who Am I Extended Operation Handler for the properties of this Extended Operation Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the `--handler-name {name}` option.

`-t | --type {type}`

The type of Extended Operation Handler which should be created. The value for TYPE can be one of: cancel | custom | get-connection-id | get-symmetric-key | password-modify | password-policy-state | start-tls | who-am-i.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

`cancel-extended-operation-handler`

Default {type}: Cancel Extended Operation Handler

Enabled by default: true

See Cancel Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-connection-id-extended-operation-handler`

Default {type}: Get Connection Id Extended Operation Handler

Enabled by default: true

See Get Connection Id Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-symmetric-key-extended-operation-handler`

Default {type}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See Get Symmetric Key Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-modify-extended-operation-handler`

Default {type}: Password Modify Extended Operation Handler

Enabled by default: true

See Password Modify Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-policy-state-extended-operation-handler`

Default {type}: Password Policy State Extended Operation Handler

Enabled by default: true

See Password Policy State Extended Operation Handler for the properties of this Extended Operation Handler type.

`start-tls-extended-operation-handler`

Default {type}: Start TLS Extended Operation Handler

Enabled by default: true

See Start TLS Extended Operation Handler for the properties of this Extended Operation Handler type.

`who-am-i-extended-operation-handler`

Default {type}: Who Am I Extended Operation Handler

Enabled by default: true

See Who Am I Extended Operation Handler for the properties of this Extended Operation Handler type.

Cancel Extended Operation Handler

Extended Operation Handlers of type cancel-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Cancel Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.CancelExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Get Connection Id Extended Operation Handler

Extended Operation Handlers of type get-connection-id-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Connection Id Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.GetConnectionIDExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Get Symmetric Key Extended Operation Handler

Extended Operation Handlers of type get-symmetric-key-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Symmetric Key Extended Operation Handler implementation.

Default Value

org.opends.server.crypto.GetSymmetricKeyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Modify Extended Operation Handler

Extended Operation Handlers of type password-modify-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that should be used in conjunction with the password modify extended operation. This property is used to identify a user based on an authorization ID in the 'u:' form. Changes to this property take effect immediately.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Password Modify Extended Operation Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Modify Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordModifyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Policy State Extended Operation Handler

Extended Operation Handlers of type password-policy-state-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Policy State Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordPolicyStateExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Start TLS Extended Operation Handler

Extended Operation Handlers of type start-tls-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Start TLS Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.StartTLSExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Who Am I Extended Operation Handler

Extended Operation Handlers of type who-am-i-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Who Am I Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.WhoAmIExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-group-implementation(1)

Name

dsconfig create-group-implementation - Creates Group Implementations

Synopsis

`dsconfig create-group-implementation` {options}

Description

Creates Group Implementations.

Options

The `dsconfig create-group-implementation` command takes the following options:

`--implementation-name {name}`

The name of the new Group Implementation.

Group Implementation properties depend on the Group Implementation type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

`dynamic-group-implementation`

Default {name}: Dynamic Group Implementation

Enabled by default: true

See Dynamic Group Implementation for the properties of this Group Implementation type.

`static-group-implementation`

Default {name}: Static Group Implementation

Enabled by default: true

See Static Group Implementation for the properties of this Group Implementation type.

`virtual-static-group-implementation`

Default {name}: Virtual Static Group Implementation

Enabled by default: true

See Virtual Static Group Implementation for the properties of this Group Implementation type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Group Implementation properties depend on the Group Implementation type, which depends on the `--implementation-name {name}` option.

`-t | --type {type}`

The type of Group Implementation which should be created. The value for TYPE can be one of: custom | dynamic | static | virtual-static.

Group Implementation properties depend on the Group Implementation type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

`dynamic-group-implementation`

Default {type}: Dynamic Group Implementation

Enabled by default: true

See Dynamic Group Implementation for the properties of this Group Implementation type.

`static-group-implementation`

Default {type}: Static Group Implementation

Enabled by default: true

See Static Group Implementation for the properties of this Group Implementation type.

`virtual-static-group-implementation`

Default {type}: Virtual Static Group Implementation

Enabled by default: true

See Virtual Static Group Implementation for the properties of this Group Implementation type.

Dynamic Group Implementation

Group Implementations of type dynamic-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Dynamic Group Implementation implementation.

Default Value

org.opends.server.extensions.DynamicGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Static Group Implementation

Group Implementations of type static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Group Implementation implementation.

Default Value

org.opends.server.extensions.StaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Virtual Static Group Implementation

Group Implementations of type virtual-static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Virtual Static Group Implementation implementation.

Default Value

org.opends.server.extensions.VirtualStaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-http-authorization-mechanism(1)

Name

dsconfig create-http-authorization-mechanism - Creates HTTP Authorization Mechanisms

Synopsis

`dsconfig create-http-authorization-mechanism` {options}

Description

Creates HTTP Authorization Mechanisms.

Options

The `dsconfig create-http-authorization-mechanism` command takes the following options:

`--mechanism-name {name}`

The name of the new HTTP Authorization Mechanism.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

`http-anonymous-authorization-mechanism`

Default {name}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See HTTP Anonymous Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-basic-authorization-mechanism`

Default {name}: HTTP Basic Authorization Mechanism

Enabled by default: true

See HTTP Basic Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-cts-authorization-mechanism`

Default {name}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Cts Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-file-authorization-mechanism`

Default {name}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 File Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-openam-authorization-mechanism`

Default {name}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Openam Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-token-introspection-authorization-mechanism`

Default {name}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Token Introspection Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the `--mechanism-name {name}` option.

`-t | --type {type}`

The type of HTTP Authorization Mechanism which should be created. The value for TYPE can be one of: http-anonymous-authorization-mechanism | http-basic-authorization-mechanism | http-oauth2-cts-authorization-mechanism | http-oauth2-file-authorization-mechanism | http-oauth2-openam-authorization-mechanism | http-oauth2-token-introspection-authorization-mechanism.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

`http-anonymous-authorization-mechanism`

Default {type}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See HTTP Anonymous Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-basic-authorization-mechanism`

Default {type}: HTTP Basic Authorization Mechanism

Enabled by default: true

See HTTP Basic Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-cts-authorization-mechanism`

Default {type}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Cts Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-file-authorization-mechanism`

Default {type}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 File Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-openam-authorization-mechanism`

Default {type}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Openam Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-token-introspection-authorization-mechanism`

Default {type}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Token Introspection Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

HTTP Anonymous Authorization Mechanism

HTTP Authorization Mechanisms of type http-anonymous-authorization-mechanism have the following properties:

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Anonymous Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpAnonymousAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-dn

Description

The authorization DN which will be used for performing anonymous operations.

Default Value

By default, operations will be performed using an anonymously bound connection.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

HTTP Basic Authorization Mechanism

HTTP Authorization Mechanisms of type http-basic-authorization-mechanism have the following properties:

alt-authentication-enabled

Description

Specifies whether user credentials may be provided using alternative headers to the standard 'Authorize' header.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-password-header

Description

Alternate HTTP headers to get the user's password from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-username-header

Description

Alternate HTTP headers to get the user's name from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper used to get the user's entry corresponding to the user-id provided in the HTTP authentication header.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Basic Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Basic Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpBasicAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

HTTP Oauth2 Cts Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-cts-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

The base DN of the Core Token Service where access token are stored. (example: ou=famrecords,ou=openam-session,ou=tokens,dc=example,dc=com)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Cts Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2CtsAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

HTTP Oauth2 File Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-file-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-directory

Description

Directory containing token files. File names must be equal to the token strings. The file content must a JSON object with the following attributes: 'scope', 'expireTime' and all the field(s) needed to resolve the authzIdTemplate.

Default Value

oauth2-demo/

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 File Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2FileAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

HTTP Oauth2 Openam Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-openam-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Openam Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2OpenAmAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Openam Authorization Mechanism .

Default Value

By default the system key manager(s) will be used.

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-info-url

Description

Defines the OpenAM endpoint URL where the access-token resolution request should be sent.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only impact subsequent SSL

connection negotiations.

Advanced Property

No

Read-only

No

HTTP Oauth2 Token Introspection Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-token-introspection-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-id

Description

Client's ID to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-secret

Description

Client's secret to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Token Introspection Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2TokenIntrospectionAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Token Introspection Authorization Mechanism .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-introspection-url

Description

Defines the token introspection endpoint URL where the access-token resolution request should be sent. (example: http://example.com/introspect)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

dsconfig create-http-endpoint(1)

Name

dsconfig create-http-endpoint - Creates HTTP Endpoints

Synopsis

`dsconfig create-http-endpoint` {options}

Description

Creates HTTP Endpoints.

Options

The `dsconfig create-http-endpoint` command takes the following options:

`--endpoint-name {STRING}`

The name of the new HTTP Endpoint which will also be used as the value of the "base-path" property: All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {STRING} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

`admin-endpoint`

Default {STRING}: Admin Endpoint

Enabled by default: true

See Admin Endpoint for the properties of this HTTP Endpoint type.

`rest2ldap-endpoint`

Default {STRING}: Rest2ldap Endpoint

Enabled by default: true

See Rest2ldap Endpoint for the properties of this HTTP Endpoint type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the `--endpoint-name {STRING}` option.

`-t | --type {type}`

The type of HTTP Endpoint which should be created (Default: generic). The value for TYPE can be one of: admin-endpoint | generic | rest2ldap-endpoint.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

`admin-endpoint`

Default {type}: Admin Endpoint

Enabled by default: true

See Admin Endpoint for the properties of this HTTP Endpoint type.

`rest2ldap-endpoint`

Default {type}: Rest2ldap Endpoint

Enabled by default: true

See Rest2ldap Endpoint for the properties of this HTTP Endpoint type.

Admin Endpoint

HTTP Endpoints of type admin-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Admin Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.AdminEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Rest2ldap Endpoint

HTTP Endpoints of type rest2ldap-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

config-directory

Description

The directory containing the Rest2Ldap configuration file(s) for this specific endpoint. The directory must be readable by the server and may contain multiple configuration files, one for each supported version of the REST endpoint. If a relative path is used then it will be resolved against the server's instance directory.

Default Value

None

Allowed Values

A directory that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Rest2ldap Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.Rest2LdapEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-identity-mapper(1)

Name

dsconfig create-identity-mapper - Creates Identity Mappers

Synopsis

`dsconfig create-identity-mapper` {options}

Description

Creates Identity Mappers.

Options

The `dsconfig create-identity-mapper` command takes the following options:

`--mapper-name {name}`

The name of the new Identity Mapper.

Identity Mapper properties depend on the Identity Mapper type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

`exact-match-identity-mapper`

Default {name}: Exact Match Identity Mapper

Enabled by default: true

See Exact Match Identity Mapper for the properties of this Identity Mapper type.

`regular-expression-identity-mapper`

Default {name}: Regular Expression Identity Mapper

Enabled by default: true

See Regular Expression Identity Mapper for the properties of this Identity Mapper type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Identity Mapper properties depend on the Identity Mapper type, which depends on the `--mapper-name {name}` option.

`-t | --type {type}`

The type of Identity Mapper which should be created. The value for TYPE can be one of: custom | exact-match | regular-expression.

Identity Mapper properties depend on the Identity Mapper type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

`exact-match-identity-mapper`

Default {type}: Exact Match Identity Mapper

Enabled by default: true

See Exact Match Identity Mapper for the properties of this Identity Mapper type.

`regular-expression-identity-mapper`

Default {type}: Regular Expression Identity Mapper

Enabled by default: true

See Regular Expression Identity Mapper for the properties of this Identity Mapper type.

Exact Match Identity Mapper

Identity Mappers of type exact-match-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Exact Match Identity Mapper implementation.

Default Value

org.opends.server.extensions.ExactMatchIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the attribute whose value should exactly match the ID string provided to this identity mapper. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry. The internal search performed includes a logical OR across all of these values.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs will be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Regular Expression Identity Mapper

Identity Mappers of type regular-expression-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Regular Expression Identity Mapper implementation.

Default Value

org.opends.server.extensions.RegularExpressionIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name or OID of the attribute whose value should match the provided identifier string after it has been processed by the associated regular expression. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the base DN(s) that should be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all the specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

match-pattern

Description

Specifies the regular expression pattern that is used to identify portions of the ID string that will be replaced. Any portion of the ID string that matches this pattern is replaced in accordance with the provided replace pattern (or is removed if no replace pattern is specified). If multiple substrings within the given ID string match this pattern, all occurrences are replaced. If no part of the given ID string matches this pattern, the ID string is not altered. Exactly one match pattern value must be provided, and it must be a valid regular expression as described in the API documentation for the java.util.regex.Pattern class, including support for capturing groups.

Default Value

None

Allowed Values

Any valid regular expression pattern which is supported by the javax.util.regex.Pattern class (see http://download.oracle.com/docs/cd/E17409_01/javase/6/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 6).

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replace-pattern

Description

Specifies the replacement pattern that should be used for substrings in the ID string that match the provided regular expression pattern. If no replacement pattern is provided, then any

matching portions of the ID string will be removed (i.e., replaced with an empty string). The replacement pattern may include a string from a capturing group by using a dollar sign ($) followed by an integer value that indicates which capturing group should be used.

Default Value

The replace pattern will be the empty string.

Allowed Values

Any valid replacement string that is allowed by the javax.util.regex.Matcher class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-key-manager-provider(1)

Name

dsconfig create-key-manager-provider - Creates Key Manager Providers

Synopsis

`dsconfig create-key-manager-provider` {options}

Description

Creates Key Manager Providers.

Options

The `dsconfig create-key-manager-provider` command takes the following options:

`--provider-name {name}`

The name of the new Key Manager Provider.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

`file-based-key-manager-provider`

Default {name}: File Based Key Manager Provider

Enabled by default: true

See File Based Key Manager Provider for the properties of this Key Manager Provider type.

`ldap-key-manager-provider`

Default {name}: LDAP Key Manager Provider

Enabled by default: true

See LDAP Key Manager Provider for the properties of this Key Manager Provider type.

`pkcs11-key-manager-provider`

Default {name}: PKCS11 Key Manager Provider

Enabled by default: true

See PKCS11 Key Manager Provider for the properties of this Key Manager Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the `--provider-name {name}` option.

`-t | --type {type}`

The type of Key Manager Provider which should be created. The value for TYPE can be one of: custom | file-based | ldap | pkcs11.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

`file-based-key-manager-provider`

Default {type}: File Based Key Manager Provider

Enabled by default: true

See File Based Key Manager Provider for the properties of this Key Manager Provider type.

`ldap-key-manager-provider`

Default {type}: LDAP Key Manager Provider

Enabled by default: true

See LDAP Key Manager Provider for the properties of this Key Manager Provider type.

`pkcs11-key-manager-provider`

Default {type}: PKCS11 Key Manager Provider

Enabled by default: true

See PKCS11 Key Manager Provider for the properties of this Key Manager Provider type.

File Based Key Manager Provider

Key Manager Providers of type file-based-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Key Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS'

and 'PKCS12', but different implementations may allow other values as well. If no value is provided, the JVM-default value is used. Changes to this configuration attribute will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

LDAP Key Manager Provider

Key Manager Providers of type ldap-key-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Key Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

PKCS11 Key Manager Provider

Key Manager Providers of type pkcs11-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Key Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11KeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig create-log-publisher(1)

Name

dsconfig create-log-publisher - Creates Log Publishers

Synopsis

`dsconfig create-log-publisher` {options}

Description

Creates Log Publishers.

Options

The `dsconfig create-log-publisher` command takes the following options:

`--publisher-name {name}`

The name of the new Log Publisher.

Log Publisher properties depend on the Log Publisher type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

`csv-file-access-log-publisher`

Default {name}: Csv File Access Log Publisher

Enabled by default: true

See Csv File Access Log Publisher for the properties of this Log Publisher type.

`csv-file-http-access-log-publisher`

Default {name}: Csv File HTTP Access Log Publisher

Enabled by default: true

See Csv File HTTP Access Log Publisher for the properties of this Log Publisher type.

`external-access-log-publisher`

Default {name}: External Access Log Publisher

Enabled by default: true

See External Access Log Publisher for the properties of this Log Publisher type.

`external-http-access-log-publisher`

Default {name}: External HTTP Access Log Publisher

Enabled by default: true

See External HTTP Access Log Publisher for the properties of this Log Publisher type.

`file-based-access-log-publisher`

Default {name}: File Based Access Log Publisher

Enabled by default: true

See File Based Access Log Publisher for the properties of this Log Publisher type.

`file-based-audit-log-publisher`

Default {name}: File Based Audit Log Publisher

Enabled by default: true

See File Based Audit Log Publisher for the properties of this Log Publisher type.

`file-based-debug-log-publisher`

Default {name}: File Based Debug Log Publisher

Enabled by default: true

See File Based Debug Log Publisher for the properties of this Log Publisher type.

`file-based-error-log-publisher`

Default {name}: File Based Error Log Publisher

Enabled by default: true

See File Based Error Log Publisher for the properties of this Log Publisher type.

`file-based-http-access-log-publisher`

Default {name}: File Based HTTP Access Log Publisher

Enabled by default: true

See File Based HTTP Access Log Publisher for the properties of this Log Publisher type.

`json-file-access-log-publisher`

Default {name}: Json File Access Log Publisher

Enabled by default: true

See Json File Access Log Publisher for the properties of this Log Publisher type.

`json-file-http-access-log-publisher`

Default {name}: Json File HTTP Access Log Publisher

Enabled by default: true

See Json File HTTP Access Log Publisher for the properties of this Log Publisher type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Log Publisher properties depend on the Log Publisher type, which depends on the `--publisher-name {name}` option.

`-t | --type {type}`

The type of Log Publisher which should be created. The value for TYPE can be one of: csv-file-access | csv-file-http-access | custom-access | custom-debug | custom-error | custom-http-access | external-access | external-http-access | file-based-access | file-based-audit | file-based-debug | file-based-error | file-based-http-access | json-file-access | json-file-http-access.

Log Publisher properties depend on the Log Publisher type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

`csv-file-access-log-publisher`

Default {type}: Csv File Access Log Publisher

Enabled by default: true

See Csv File Access Log Publisher for the properties of this Log Publisher type.

`csv-file-http-access-log-publisher`

Default {type}: Csv File HTTP Access Log Publisher

Enabled by default: true

See Csv File HTTP Access Log Publisher for the properties of this Log Publisher type.

`external-access-log-publisher`

Default {type}: External Access Log Publisher

Enabled by default: true

See External Access Log Publisher for the properties of this Log Publisher type.

`external-http-access-log-publisher`

Default {type}: External HTTP Access Log Publisher

Enabled by default: true

See External HTTP Access Log Publisher for the properties of this Log Publisher type.

`file-based-access-log-publisher`

Default {type}: File Based Access Log Publisher

Enabled by default: true

See File Based Access Log Publisher for the properties of this Log Publisher type.

`file-based-audit-log-publisher`

Default {type}: File Based Audit Log Publisher

Enabled by default: true

See File Based Audit Log Publisher for the properties of this Log Publisher type.

`file-based-debug-log-publisher`

Default {type}: File Based Debug Log Publisher

Enabled by default: true

See File Based Debug Log Publisher for the properties of this Log Publisher type.

`file-based-error-log-publisher`

Default {type}: File Based Error Log Publisher

Enabled by default: true

See File Based Error Log Publisher for the properties of this Log Publisher type.

`file-based-http-access-log-publisher`

Default {type}: File Based HTTP Access Log Publisher

Enabled by default: true

See File Based HTTP Access Log Publisher for the properties of this Log Publisher type.

`json-file-access-log-publisher`

Default {type}: Json File Access Log Publisher

Enabled by default: true

See Json File Access Log Publisher for the properties of this Log Publisher type.

`json-file-http-access-log-publisher`

Default {type}: Json File HTTP Access Log Publisher

Enabled by default: true

See Json File HTTP Access Log Publisher for the properties of this Log Publisher type.

Csv File Access Log Publisher

Log Publishers of type csv-file-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writting in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CsvFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Csv File Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when the tamper-evident option is enabled.

Default Value

3s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Csv File HTTP Access Log Publisher

Log Publishers of type csv-file-http-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File HTTP Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Csv File HTTP Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when secure option is enabled.

Default Value

3s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

External Access Log Publisher

Log Publishers of type external-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External Access Log Publisher implementation.

Default Value

org.opends.server.loggers.ExternalAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

External HTTP Access Log Publisher

Log Publishers of type external-http-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External HTTP Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Access Log Publisher

Log Publishers of type file-based-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the access log.

Default Value

multi-line

Allowed Values

combined

Combine log records for operation requests and responses into a single record. This format should be used when log records are to be filtered based on response criteria (e.g. result code).

multi-line

Outputs separate log records for operation requests and responses.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Audit Log Publisher

Log Publishers of type file-based-audit-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Audit Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Audit Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAuditLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Audit Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Audit Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Audit Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Audit Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Debug Log Publisher

Log Publishers of type file-based-debug-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Debug Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-include-throwable-cause

Description

Indicates whether to include the cause of exceptions in exception thrown and caught messages logged by default.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-entry-arguments

Description

Indicates whether to include method arguments in debug messages logged by default.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-return-value

Description

Indicates whether to include the return value in debug messages logged by default.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-throwable-stack-frames

Description

Indicates the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Debug Log Publisher implementation.

Default Value

org.opends.server.loggers.TextDebugLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Debug Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Debug Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Debug Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Debug Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Error Log Publisher

Log Publishers of type file-based-error-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Error Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer will be flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-severity

Description

Specifies the default severity levels for the logger.

Default Value

error warning

Allowed Values

all

Messages of all severity levels are logged.

debug

The error log severity that is used for messages that provide debugging information triggered during processing.

error

The error log severity that is used for messages that provide information about errors which may force the server to shut down or operate in a significantly degraded state.

info

The error log severity that is used for messages that provide information about significant events within the server that are not warnings or errors.

none

No messages of any severity are logged by default. This value is intended to be used in conjunction with the override-severity property to define an error logger that will publish no error message beside the errors of a given category.

notice

The error log severity that is used for the most important informational messages (i.e., information that should almost always be logged but is not associated with a warning or error condition).

warning

The error log severity that is used for messages that provide information about warnings triggered during processing.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Error Log Publisher implementation.

Default Value

org.opends.server.loggers.TextErrorLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Error Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Error Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

override-severity

Description

Specifies the override severity levels for the logger based on the category of the messages. Each override severity level should include the category and the severity levels to log for that category, for example, core=error,info,warning. Valid categories are: core, extensions, protocol, config, log, util, schema, plugin, jeb, backend, tools, task, access-control, admin, sync, version, quicksetup, admin-tool, dsconfig, user-defined. Valid severities are: all, error, info, warning, notice, debug.

Default Value

All messages with the default severity levels are logged.

Allowed Values

A string in the form category=severity1,severity2...

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Error Log Publisher . When multiple policies are used, log files will be cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files will never be cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Error Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based HTTP Access Log Publisher

Log Publishers of type file-based-http-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based HTTP Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based HTTP Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the HTTP access log.

Default Value

cs-host c-ip cs-username x-datetime cs-method cs-uri-stem cs-uri-query cs-version sc-status cs(User-Agent) x-connection-id x-etime x-transaction-id

Allowed Values

A space separated list of fields describing the extended log format to be used for logging HTTP accesses. Available values are listed on the W3C working draft http://www.w3.org/TR/WD-logfile.html and Microsoft website http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/676400bc-8969-4aa7-851a-9319490a9bbb.mspx?mfr=true
OpenDJ supports the following standard fields: "c-ip", "c-port", "cs-host", "cs-method", "cs-uri", "cs-uri-stem", "cs-uri-query", "cs(User-Agent)", "cs-username", "cs-version", "s-computername", "s-ip", "s-port", "sc-status". OpenDJ supports the following application specific field extensions: "x-connection-id" displays the internal connection ID assigned to the HTTP client connection, "x-datetime" displays the completion date and time for the logged HTTP request and its ouput is controlled by the "ds-cfg-log-record-time-format" property, "x-etime" displays the total execution time for the logged HTTP request, "x-transaction-id" displays the transaction id associated to a request

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Json File Access Log Publisher

Log Publishers of type json-file-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.JsonFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Json File HTTP Access Log Publisher

Log Publishers of type json-file-http-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-log-retention-policy(1)

Name

dsconfig create-log-retention-policy - Creates Log Retention Policies

Synopsis

`dsconfig create-log-retention-policy` {options}

Description

Creates Log Retention Policies.

Options

The `dsconfig create-log-retention-policy` command takes the following options:

`--policy-name {name}`

The name of the new Log Retention Policy.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

`file-count-log-retention-policy`

Default {name}: File Count Log Retention Policy

Enabled by default: false

See File Count Log Retention Policy for the properties of this Log Retention Policy type.

`free-disk-space-log-retention-policy`

Default {name}: Free Disk Space Log Retention Policy

Enabled by default: false

See Free Disk Space Log Retention Policy for the properties of this Log Retention Policy type.

`size-limit-log-retention-policy`

Default {name}: Size Limit Log Retention Policy

Enabled by default: false

See Size Limit Log Retention Policy for the properties of this Log Retention Policy type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the `--policy-name {name}` option.

`-t | --type {type}`

The type of Log Retention Policy which should be created. The value for TYPE can be one of: custom | file-count | free-disk-space | size-limit.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

`file-count-log-retention-policy`

Default {type}: File Count Log Retention Policy

Enabled by default: false

See File Count Log Retention Policy for the properties of this Log Retention Policy type.

`free-disk-space-log-retention-policy`

Default {type}: Free Disk Space Log Retention Policy

Enabled by default: false

See Free Disk Space Log Retention Policy for the properties of this Log Retention Policy type.

`size-limit-log-retention-policy`

Default {type}: Size Limit Log Retention Policy

Enabled by default: false

See Size Limit Log Retention Policy for the properties of this Log Retention Policy type.

File Count Log Retention Policy

Log Retention Policies of type file-count-log-retention-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the File Count Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FileNumberRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

number-of-files

Description

Specifies the number of archived log files to retain before the oldest ones are cleaned.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Free Disk Space Log Retention Policy

Log Retention Policies of type free-disk-space-log-retention-policy have the following properties:

free-disk-space

Description

Specifies the minimum amount of free disk space that should be available on the file system on which the archived log files are stored.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Free Disk Space Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FreeDiskSpaceRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Size Limit Log Retention Policy

Log Retention Policies of type size-limit-log-retention-policy have the following properties:

disk-space-used

Description

Specifies the maximum total disk space used by the log files.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Retention Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-log-rotation-policy(1)

Name

dsconfig create-log-rotation-policy - Creates Log Rotation Policies

Synopsis

`dsconfig create-log-rotation-policy` {options}

Description

Creates Log Rotation Policies.

Options

The `dsconfig create-log-rotation-policy` command takes the following options:

`--policy-name {name}`

The name of the new Log Rotation Policy.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

`fixed-time-log-rotation-policy`

Default {name}: Fixed Time Log Rotation Policy

Enabled by default: false

See Fixed Time Log Rotation Policy for the properties of this Log Rotation Policy type.

`size-limit-log-rotation-policy`

Default {name}: Size Limit Log Rotation Policy

Enabled by default: false

See Size Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`time-limit-log-rotation-policy`

Default {name}: Time Limit Log Rotation Policy

Enabled by default: false

See Time Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the `--policy-name {name}` option.

`-t | --type {type}`

The type of Log Rotation Policy which should be created. The value for TYPE can be one of: custom | fixed-time | size-limit | time-limit.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

`fixed-time-log-rotation-policy`

Default {type}: Fixed Time Log Rotation Policy

Enabled by default: false

See Fixed Time Log Rotation Policy for the properties of this Log Rotation Policy type.

`size-limit-log-rotation-policy`

Default {type}: Size Limit Log Rotation Policy

Enabled by default: false

See Size Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`time-limit-log-rotation-policy`

Default {type}: Time Limit Log Rotation Policy

Enabled by default: false

See Time Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

Fixed Time Log Rotation Policy

Log Rotation Policies of type fixed-time-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fixed Time Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.FixedTimeRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-of-day

Description

Specifies the time of day at which log rotation should occur.

Default Value

None

Allowed Values

24 hour time of day in HHmm format.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Size Limit Log Rotation Policy

Log Rotation Policies of type size-limit-log-rotation-policy have the following properties:

file-size-limit

Description

Specifies the maximum size that a log file can reach before it is rotated.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Time Limit Log Rotation Policy

Log Rotation Policies of type time-limit-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Time Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.TimeLimitRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

rotation-interval

Description

Specifies the time interval between rotations.

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-monitor-provider(1)

Name

dsconfig create-monitor-provider - Creates Monitor Providers

Synopsis

`dsconfig create-monitor-provider` {options}

Description

Creates Monitor Providers.

Options

The `dsconfig create-monitor-provider` command takes the following options:

`--provider-name {name}`

The name of the new Monitor Provider.

Monitor Provider properties depend on the Monitor Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

`client-connection-monitor-provider`

Default {name}: Client Connection Monitor Provider

Enabled by default: true

See Client Connection Monitor Provider for the properties of this Monitor Provider type.

`entry-cache-monitor-provider`

Default {name}: Entry Cache Monitor Provider

Enabled by default: true

See Entry Cache Monitor Provider for the properties of this Monitor Provider type.

`memory-usage-monitor-provider`

Default {name}: Memory Usage Monitor Provider

Enabled by default: true

See Memory Usage Monitor Provider for the properties of this Monitor Provider type.

`stack-trace-monitor-provider`

Default {name}: Stack Trace Monitor Provider

Enabled by default: true

See Stack Trace Monitor Provider for the properties of this Monitor Provider type.

`system-info-monitor-provider`

Default {name}: System Info Monitor Provider

Enabled by default: true

See System Info Monitor Provider for the properties of this Monitor Provider type.

`version-monitor-provider`

Default {name}: Version Monitor Provider

Enabled by default: true

See Version Monitor Provider for the properties of this Monitor Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Monitor Provider properties depend on the Monitor Provider type, which depends on the `--provider-name {name}` option.

`-t | --type {type}`

The type of Monitor Provider which should be created. The value for TYPE can be one of: client-connection | custom | entry-cache | memory-usage | stack-trace | system-info | version.

Monitor Provider properties depend on the Monitor Provider type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

`client-connection-monitor-provider`

Default {type}: Client Connection Monitor Provider

Enabled by default: true

See Client Connection Monitor Provider for the properties of this Monitor Provider type.

`entry-cache-monitor-provider`

Default {type}: Entry Cache Monitor Provider

Enabled by default: true

See Entry Cache Monitor Provider for the properties of this Monitor Provider type.

`memory-usage-monitor-provider`

Default {type}: Memory Usage Monitor Provider

Enabled by default: true

See Memory Usage Monitor Provider for the properties of this Monitor Provider type.

`stack-trace-monitor-provider`

Default {type}: Stack Trace Monitor Provider

Enabled by default: true

See Stack Trace Monitor Provider for the properties of this Monitor Provider type.

`system-info-monitor-provider`

Default {type}: System Info Monitor Provider

Enabled by default: true

See System Info Monitor Provider for the properties of this Monitor Provider type.

`version-monitor-provider`

Default {type}: Version Monitor Provider

Enabled by default: true

See Version Monitor Provider for the properties of this Monitor Provider type.

Client Connection Monitor Provider

Monitor Providers of type client-connection-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Client Connection Monitor Provider implementation.

Default Value

org.opends.server.monitors.ClientConnectionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Entry Cache Monitor Provider

Monitor Providers of type entry-cache-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Entry Cache Monitor Provider implementation.

Default Value

org.opends.server.monitors.EntryCacheMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Memory Usage Monitor Provider

Monitor Providers of type memory-usage-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Memory Usage Monitor Provider implementation.

Default Value

org.opends.server.monitors.MemoryUsageMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Stack Trace Monitor Provider

Monitor Providers of type stack-trace-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Stack Trace Monitor Provider implementation.

Default Value

org.opends.server.monitors.StackTraceMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

System Info Monitor Provider

Monitor Providers of type system-info-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the System Info Monitor Provider implementation.

Default Value

org.opends.server.monitors.SystemInfoMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Version Monitor Provider

Monitor Providers of type version-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Version Monitor Provider implementation.

Default Value

org.opends.server.monitors.VersionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-password-generator(1)

Name

dsconfig create-password-generator - Creates Password Generators

Synopsis

`dsconfig create-password-generator` {options}

Description

Creates Password Generators.

Options

The `dsconfig create-password-generator` command takes the following options:

`--generator-name {name}`

The name of the new Password Generator.

Password Generator properties depend on the Password Generator type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

`random-password-generator`

Default {name}: Random Password Generator

Enabled by default: true

See Random Password Generator for the properties of this Password Generator type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Password Generator properties depend on the Password Generator type, which depends on the `--generator-name {name}` option.

`-t | --type {type}`

The type of Password Generator which should be created. The value for TYPE can be one of: custom | random.

Password Generator properties depend on the Password Generator type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

`random-password-generator`

Default {type}: Random Password Generator

Enabled by default: true

See Random Password Generator for the properties of this Password Generator type.

Random Password Generator

Password Generators of type random-password-generator have the following properties:

enabled

Description

Indicates whether the Password Generator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Random Password Generator implementation.

Default Value

org.opends.server.extensions.RandomPasswordGenerator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordGenerator

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

password-character-set

Description

Specifies one or more named character sets. This is a multi-valued property, with each value defining a different character set. The format of the character set is the name of the set followed by a colon and the characters that are in that set. For example, the value "alpha:abcdefghijklmnopqrstuvwxyz" defines a character set named "alpha" containing all of the lower-case ASCII alphabetic characters.

Default Value

None

Allowed Values

A character set name (consisting of ASCII letters) followed by a colon and the set of characters that are included in that character set.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-format

Description

Specifies the format to use for the generated password. The value is a comma-delimited list of elements in which each of those elements is comprised of the name of a character set defined in the password-character-set property, a colon, and the number of characters to include from that set. For example, a value of "alpha:3,numeric:2,alpha:3" generates an 8-character password in which the first three characters are from the "alpha" set, the next two are from the "numeric" set, and the final three are from the "alpha" set.

Default Value

None

Allowed Values

A comma-delimited list whose elements comprise a valid character set name, a colon, and a positive integer indicating the number of characters from that set to be included.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-password-policy(1)

Name

dsconfig create-password-policy - Creates Authentication Policies

Synopsis

`dsconfig create-password-policy` {options}

Description

Creates Authentication Policies.

Options

The `dsconfig create-password-policy` command takes the following options:

`--policy-name {name}`

The name of the new Authentication Policy.

Authentication Policy properties depend on the Authentication Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

`ldap-pass-through-authentication-policy`

Default {name}: LDAP Pass Through Authentication Policy

Enabled by default: false

See LDAP Pass Through Authentication Policy for the properties of this Authentication Policy type.

`password-policy`

Default {name}: Password Policy

Enabled by default: false

See Password Policy for the properties of this Authentication Policy type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Authentication Policy properties depend on the Authentication Policy type, which depends on

the `--policy-name {name}` option.

`-t | --type {type}`

The type of Authentication Policy which should be created. The value for TYPE can be one of: ldap-pass-through | password-policy.

Authentication Policy properties depend on the Authentication Policy type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

`ldap-pass-through-authentication-policy`

Default {type}: LDAP Pass Through Authentication Policy

Enabled by default: false

See LDAP Pass Through Authentication Policy for the properties of this Authentication Policy type.

`password-policy`

Default {type}: Password Policy

Enabled by default: false

See Password Policy for the properties of this Authentication Policy type.

LDAP Pass Through Authentication Policy

Authentication Policies of type ldap-pass-through-authentication-policy have the following properties:

cached-password-storage-scheme

Description

Specifies the name of a password storage scheme which should be used for encoding cached passwords. Changing the password storage scheme will cause all existing cached passwords to be discarded.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cached-password-ttl

Description

Specifies the maximum length of time that a locally cached password may be used for authentication before it is refreshed from the remote LDAP service. This property represents a cache timeout. Increasing the timeout period decreases the frequency that bind operations are delegated to the remote LDAP service, but increases the risk of users authenticating using stale passwords. Note that authentication attempts which fail because the provided password does not match the locally cached password will always be retried against the remote LDAP service.

Default Value

8 hours

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-timeout

Description

Specifies the timeout used when connecting to remote LDAP directory servers, performing SSL negotiation, and for individual search and bind requests. If the timeout expires then the current

operation will be aborted and retried against another LDAP server if one is available.

Default Value

3 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the LDAP Pass Through Authentication Policy implementation.

Default Value

org.opends.server.extensions.LDAPPassThroughAuthenticationPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

mapped-attribute

Description

Specifies one or more attributes in the user's entry whose value(s) will determine the bind DN used when authenticating to the remote LDAP directory service. This property is mandatory when using the "mapped-bind" or "mapped-search" mapping policies. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. At least one of the named attributes must exist in a user's local entry in order for authentication to proceed. When multiple attributes or values are found in the user's entry then the behavior is determined by the mapping policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-base-dn

Description

Specifies the set of base DNs below which to search for users in the remote LDAP directory service. This property is mandatory when using the "mapped-search" mapping policy. If multiple values are given, searches are performed below all specified base DNs.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-dn

Description

Specifies the bind DN which should be used to perform user searches in the remote LDAP directory service.

Default Value

Searches will be performed anonymously.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password

Description

Specifies the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-environment-variable

Description

Specifies the name of an environment variable containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-file

Description

Specifies the name of a file containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-property

Description

Specifies the name of a Java property containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-filter-template

Description

If defined, overrides the filter used when searching for the user, substituting %s with the value of the local entry's "mapped-attribute". The filter-template may include ZERO or ONE %s substitutions. If multiple mapped-attributes are configured, multiple renditions of this template will be aggregated into one larger filter using an OR (|) operator. An example use-case for this property would be to use a different attribute type on the mapped search. For example, mapped-attribute could be set to "uid" and filter-template to "(samAccountName=%s)". You can also use the filter to restrict search results. For example: "(&(uid=%s)(objectclass=student))"

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapping-policy

Description

Specifies the mapping algorithm for obtaining the bind DN from the user's entry.

Default Value

unmapped

Allowed Values

mapped-bind

Bind to the remote LDAP directory service using a DN obtained from an attribute in the user's entry. This policy will check each attribute named in the "mapped-attribute" property. If more than one attribute or value is present then the first one will be used.

mapped-search

Bind to the remote LDAP directory service using the DN of an entry obtained using a search against the remote LDAP directory service. The search filter will comprise of an equality matching filter whose attribute type is the "mapped-attribute" property, and whose assertion value is the attribute value obtained from the user's entry. If more than one attribute or value is present then the filter will be composed of multiple equality filters combined using a logical OR (union).

unmapped

Bind to the remote LDAP directory service using the DN of the user's entry in this directory server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

primary-remote-ldap-server

Description

Specifies the primary list of remote LDAP servers which should be used for pass through authentication. If more than one LDAP server is specified then operations may be distributed across them. If all of the primary LDAP servers are unavailable then operations will fail-over to the set of secondary LDAP servers, if defined.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-remote-ldap-server

Description

Specifies the secondary list of remote LDAP servers which should be used for pass through authentication in the event that the primary LDAP servers are unavailable. If more than one LDAP server is specified then operations may be distributed across them. Operations will be rerouted to the primary LDAP servers as soon as they are determined to be available.

Default Value

No secondary LDAP servers.

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The

address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols which are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with remote LDAP directory servers.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

use-password-caching

Description

Indicates whether passwords should be cached locally within the user's entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Pass Through Authentication Policy should use SSL. If enabled, the LDAP Pass Through Authentication Policy will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether LDAP connections should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether LDAP connections should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Policy

Authentication Policies of type password-policy have the following properties:

account-status-notification-handler

Description

Specifies the names of the account status notification handlers that are used with the associated password storage scheme.

Default Value

None

Allowed Values

The DN of any Account Status Notification Handler. The referenced account status notification handlers must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-expired-password-changes

Description

Indicates whether a user whose password is expired is still allowed to change that password using the password modify extended operation.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-multiple-password-values

Description

Indicates whether user entries can have multiple distinct values for the password attribute. This is potentially dangerous because many mechanisms used to change the password do not work well with such a configuration. If multiple password values are allowed, then any of them can be used to authenticate, and they are all subject to the same policy constraints.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-pre-encoded-passwords

Description

Indicates whether users can change their passwords by providing a pre-encoded value. This can cause a security risk because the clear-text version of the password is not known and therefore validation checks cannot be applied to it.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-user-password-changes

Description

Indicates whether users can change their own passwords. This check is made in addition to access control evaluation. Both must allow the password change for it to occur.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-password-storage-scheme

Description

Specifies the names of the password storage schemes that are used to encode clear-text passwords for this password policy.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

deprecated-password-storage-scheme

Description

Specifies the names of the password storage schemes that are considered deprecated for this password policy. If a user with this password policy authenticates to the server and his/her password is encoded with a deprecated scheme, those values are removed and replaced with values encoded using the default password storage scheme(s).

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

expire-passwords-without-warning

Description

Indicates whether the directory server allows a user's password to expire even if that user has never seen an expiration warning notification. If this property is true, accounts always expire when the expiration time arrives. If this property is false or disabled, the user always receives at

least one warning notification, and the password expiration is set to the warning time plus the warning interval.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-add

Description

Indicates whether users are forced to change their passwords upon first authenticating to the directory server after their account has been created.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-reset

Description

Indicates whether users are forced to change their passwords if they are reset by an administrator. For this purpose, anyone with permission to change a given user's password other than that user is considered an administrator.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

grace-login-count

Description

Specifies the number of grace logins that a user is allowed after the account has expired to allow that user to choose a new password. A value of 0 indicates that no grace logins are allowed.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

idle-lockout-interval

Description

Specifies the maximum length of time that an account may remain idle (that is, the associated user does not authenticate to the server) before that user is locked out. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that idle accounts are not automatically locked out. This feature is available only if the last login time is maintained.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the Password Policy implementation.

Default Value

org.opends.server.core.PasswordPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

last-login-time-attribute

Description

Specifies the name or OID of the attribute type that is used to hold the last login time for users with the associated password policy. This attribute type must be defined in the directory server schema and must either be defined as an operational attribute or must be allowed by the set of objectClasses for all users with the associated password policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

last-login-time-format

Description

Specifies the format string that is used to generate the last login time value for users with the associated password policy. This format string conforms to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-duration

Description

Specifies the length of time that an account is locked after too many authentication failures. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the account must remain locked until an administrator resets the password.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-count

Description

Specifies the maximum number of authentication failures that a user is allowed before the account is locked out. A value of 0 indicates that accounts are never locked out due to failed attempts.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-expiration-interval

Description

Specifies the length of time before an authentication failure is no longer counted against a user for the purposes of account lockout. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the authentication failures must never expire. The failure count is always cleared upon a successful authentication.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-age

Description

Specifies the maximum length of time that a user can continue using the same password before it must be changed (that is, the password expiration interval). The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables password expiration.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-reset-age

Description

Specifies the maximum length of time that users have to change passwords after they have been reset by an administrator before they become locked. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables this feature.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-age

Description

Specifies the minimum length of time after a password change before the user is allowed to change the password again. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. This setting can be used to prevent users from changing their passwords repeatedly over a short period of time to flush an old password from the history so that it can be re-used.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-attribute

Description

Specifies the attribute type used to hold user passwords. This attribute type must be defined in the server schema, and it must have either the user password or auth password syntax.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-change-requires-current-password

Description

Indicates whether user password changes must use the password modify extended operation and must include the user's current password before the change is allowed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-expiration-warning-interval

Description

Specifies the maximum length of time before a user's password actually expires that the server begins to include warning notifications in bind responses for that user. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables the warning interval.

Default Value

5 days

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-generator

Description

Specifies the name of the password generator that is used with the associated password policy. This is used in conjunction with the password modify extended operation to generate a new password for a user when none was provided in the request.

Default Value

None

Allowed Values

The DN of any Password Generator. The referenced password generator must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-count

Description

Specifies the maximum number of former passwords to maintain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero indicates that either no password history is to be maintained (if the password history duration has a value of zero seconds), or that there is no maximum number of passwords to maintain in the history (if the password history duration has a value greater than zero seconds).

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-duration

Description

Specifies the maximum length of time that passwords remain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero seconds indicates that either no password history is to be maintained (if the password history count has a value of zero), or that there is no maximum duration for passwords in the history (if the password history count has a value greater than zero).

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-validator

Description

Specifies the names of the password validators that are used with the associated password storage scheme. The password validators are invoked when a user attempts to provide a new password, to determine whether the new password is acceptable.

Default Value

None

Allowed Values

The DN of any Password Validator. The referenced password validators must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

previous-last-login-time-format

Description

Specifies the format string(s) that might have been used with the last login time at any point in the past for users associated with the password policy. These values are used to make it possible to parse previous values, but are not used to set new values. The format strings conform to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-change-by-time

Description

Specifies the time by which all users with the associated password policy must change their passwords. The value is expressed in a generalized time format. If this time is equal to the current time or is in the past, then all users are required to change their passwords immediately. The behavior of the server in this mode is identical to the behavior observed when users are forced to change their passwords after an administrative reset.

Default Value

None

Allowed Values

A valid timestamp in generalized time form (for example, a value of "20070409185811Z" indicates a value of April 9, 2007 at 6:58:11 pm GMT).

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-authentication

Description

Indicates whether users with the associated password policy are required to authenticate in a secure manner. This might mean either using a secure communication channel between the client and the server, or using a SASL mechanism that does not expose the credentials.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-password-changes

Description

Indicates whether users with the associated password policy are required to change their password in a secure manner that does not expose the credentials.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

skip-validation-for-administrators

Description

Indicates whether passwords set by administrators are allowed to bypass the password validation process that is required for user password changes.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

state-update-failure-policy

Description

Specifies how the server deals with the inability to update password policy state information during an authentication attempt. In particular, this property can be used to control whether an otherwise successful bind operation fails if a failure occurs while attempting to update password policy state information (for example, to clear a record of previous authentication failures or to update the last login time). It can also be used to control whether to reject a bind request if it is known ahead of time that it will not be possible to update the authentication failure times in the event of an unsuccessful bind attempt (for example, if the backend writability mode is disabled).

Default Value

reactive

Allowed Values

ignore

If a bind attempt would otherwise be successful, then do not reject it if a problem occurs while attempting to update the password policy state information for the user.

proactive

Proactively reject any bind attempt if it is known ahead of time that it would not be possible to update the user's password policy state information.

reactive

Even if a bind attempt would otherwise be successful, reject it if a problem occurs while attempting to update the password policy state information for the user.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-password-storage-scheme(1)

Name

dsconfig create-password-storage-scheme - Creates Password Storage Schemes

Synopsis

`dsconfig create-password-storage-scheme` {options}

Description

Creates Password Storage Schemes.

Options

The `dsconfig create-password-storage-scheme` command takes the following options:

`--scheme-name {name}`

The name of the new Password Storage Scheme.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

`aes-password-storage-scheme`

Default {name}: AES Password Storage Scheme

Enabled by default: true

See AES Password Storage Scheme for the properties of this Password Storage Scheme type.

`base64-password-storage-scheme`

Default {name}: Base64 Password Storage Scheme

Enabled by default: true

See Base64 Password Storage Scheme for the properties of this Password Storage Scheme type.

`bcrypt-password-storage-scheme`

Default {name}: Bcrypt Password Storage Scheme

Enabled by default: true

See Bcrypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`blowfish-password-storage-scheme`

Default {name}: Blowfish Password Storage Scheme

Enabled by default: true

See Blowfish Password Storage Scheme for the properties of this Password Storage Scheme type.

`clear-password-storage-scheme`

Default {name}: Clear Password Storage Scheme

Enabled by default: true

See Clear Password Storage Scheme for the properties of this Password Storage Scheme type.

`crypt-password-storage-scheme`

Default {name}: Crypt Password Storage Scheme

Enabled by default: true

See Crypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`md5-password-storage-scheme`

Default {name}: MD5 Password Storage Scheme

Enabled by default: true

See MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha256-password-storage-scheme`

Default {name}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha512-password-storage-scheme`

Default {name}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pkcs5s2-password-storage-scheme`

Default {name}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See PKCS5S2 Password Storage Scheme for the properties of this Password Storage Scheme

type.

`rc4-password-storage-scheme`

Default {name}: RC4 Password Storage Scheme

Enabled by default: true

See RC4 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-md5-password-storage-scheme`

Default {name}: Salted MD5 Password Storage Scheme

Enabled by default: true

See Salted MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha1-password-storage-scheme`

Default {name}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See Salted SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha256-password-storage-scheme`

Default {name}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See Salted SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha384-password-storage-scheme`

Default {name}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See Salted SHA384 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha512-password-storage-scheme`

Default {name}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See Salted SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`sha1-password-storage-scheme`

Default {name}: SHA1 Password Storage Scheme

Enabled by default: true

See SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`triple-des-password-storage-scheme`

Default {name}: Triple DES Password Storage Scheme

Enabled by default: true

See Triple DES Password Storage Scheme for the properties of this Password Storage Scheme type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the `--scheme-name {name}` option.

`-t | --type {type}`

The type of Password Storage Scheme which should be created. The value for TYPE can be one of: aes | base64 | bcrypt | blowfish | clear | crypt | custom | md5 | pbkdf2 | pbkdf2-hmac-sha256 | pbkdf2-hmac-sha512 | pkcs5s2 | rc4 | salted-md5 | salted-sha1 | salted-sha256 | salted-sha384 | salted-sha512 | sha1 | triple-des.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

`aes-password-storage-scheme`

Default {type}: AES Password Storage Scheme

Enabled by default: true

See AES Password Storage Scheme for the properties of this Password Storage Scheme type.

`base64-password-storage-scheme`

Default {type}: Base64 Password Storage Scheme

Enabled by default: true

See Base64 Password Storage Scheme for the properties of this Password Storage Scheme type.

`bcrypt-password-storage-scheme`

Default {type}: Bcrypt Password Storage Scheme

Enabled by default: true

See Bcrypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`blowfish-password-storage-scheme`

Default {type}: Blowfish Password Storage Scheme

Enabled by default: true

See Blowfish Password Storage Scheme for the properties of this Password Storage Scheme type.

`clear-password-storage-scheme`

Default {type}: Clear Password Storage Scheme

Enabled by default: true

See Clear Password Storage Scheme for the properties of this Password Storage Scheme type.

`crypt-password-storage-scheme`

Default {type}: Crypt Password Storage Scheme

Enabled by default: true

See Crypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`md5-password-storage-scheme`

Default {type}: MD5 Password Storage Scheme

Enabled by default: true

See MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha256-password-storage-scheme`

Default {type}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha512-password-storage-scheme`

Default {type}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pkcs5s2-password-storage-scheme`

Default {type}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See PKCS5S2 Password Storage Scheme for the properties of this Password Storage Scheme type.

`rc4-password-storage-scheme`

Default {type}: RC4 Password Storage Scheme

Enabled by default: true

See RC4 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-md5-password-storage-scheme`

Default {type}: Salted MD5 Password Storage Scheme

Enabled by default: true

See Salted MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha1-password-storage-scheme`

Default {type}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See Salted SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha256-password-storage-scheme`

Default {type}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See Salted SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha384-password-storage-scheme`

Default {type}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See Salted SHA384 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha512-password-storage-scheme`

Default {type}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See Salted SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`sha1-password-storage-scheme`

Default {type}: SHA1 Password Storage Scheme

Enabled by default: true

See SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`triple-des-password-storage-scheme`

Default {type}: Triple DES Password Storage Scheme

Enabled by default: true

See Triple DES Password Storage Scheme for the properties of this Password Storage Scheme type.

AES Password Storage Scheme

Password Storage Schemes of type aes-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the AES Password Storage

Scheme implementation.

Default Value

org.opends.server.extensions.AESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Base64 Password Storage Scheme

Password Storage Schemes of type base64-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Base64 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.Base64PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Bcrypt Password Storage Scheme

Password Storage Schemes of type bcrypt-password-storage-scheme have the following properties:

bcrypt-cost

Description

The cost parameter specifies a key expansion iteration count as a power of two. A default value of 12 (2^12 iterations) is considered in 2016 as a reasonable balance between responsiveness and security for regular users.

Default Value

12

Allowed Values

An integer value. Lower value is 1. Upper value is 30.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Bcrypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BcryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Blowfish Password Storage Scheme

Password Storage Schemes of type blowfish-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Blowfish Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BlowfishPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Clear Password Storage Scheme

Password Storage Schemes of type clear-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Clear Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.ClearPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Crypt Password Storage Scheme

Password Storage Schemes of type crypt-password-storage-scheme have the following properties:

crypt-password-storage-encryption-algorithm

Description

Specifies the algorithm to use to encrypt new passwords. Select the crypt algorithm to use to encrypt new passwords. The value can either be "unix", which means the password is encrypted with the weak Unix crypt algorithm, or "md5" which means the password is encrypted with the BSD MD5 algorithm and has a 1 prefix, or "sha256" which means the password is encrypted with the SHA256 algorithm and has a 5 prefix, or "sha512" which means the password is encrypted with the SHA512 algorithm and has a 6 prefix.

Default Value

unix

Allowed Values

md5

New passwords are encrypted with the BSD MD5 algorithm.

sha256

New passwords are encrypted with the Unix crypt SHA256 algorithm.

sha512

New passwords are encrypted with the Unix crypt SHA512 algorithm.

unix

New passwords are encrypted with the Unix crypt algorithm. Passwords are truncated at 8 characters and the top bit of each character is ignored.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Crypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.CryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

MD5 Password Storage Scheme

Password Storage Schemes of type md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.MD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

PBKDF2 Hmac SHA256 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

PBKDF2 Hmac SHA512 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha512-password-storage-scheme have the

following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

PKCS5S2 Password Storage Scheme

Password Storage Schemes of type pkcs5s2-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PKCS5S2 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PKCS5S2PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

RC4 Password Storage Scheme

Password Storage Schemes of type rc4-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the RC4 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.RC4PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted MD5 Password Storage Scheme

Password Storage Schemes of type salted-md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedMD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA1 Password Storage Scheme

Password Storage Schemes of type salted-sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA256 Password Storage Scheme

Password Storage Schemes of type salted-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA384 Password Storage Scheme

Password Storage Schemes of type salted-sha384-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA384 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA384PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA512 Password Storage Scheme

Password Storage Schemes of type salted-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

SHA1 Password Storage Scheme

Password Storage Schemes of type sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Triple DES Password Storage Scheme

Password Storage Schemes of type triple-des-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Triple DES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.TripleDESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-password-validator(1)

Name

dsconfig create-password-validator - Creates Password Validators

Synopsis

`dsconfig create-password-validator` {options}

Description

Creates Password Validators.

Options

The `dsconfig create-password-validator` command takes the following options:

`--validator-name {name}`

The name of the new Password Validator.

Password Validator properties depend on the Password Validator type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

`attribute-value-password-validator`

Default {name}: Attribute Value Password Validator

Enabled by default: true

See Attribute Value Password Validator for the properties of this Password Validator type.

`character-set-password-validator`

Default {name}: Character Set Password Validator

Enabled by default: true

See Character Set Password Validator for the properties of this Password Validator type.

`dictionary-password-validator`

Default {name}: Dictionary Password Validator

Enabled by default: true

See Dictionary Password Validator for the properties of this Password Validator type.

`length-based-password-validator`

Default {name}: Length Based Password Validator

Enabled by default: true

See Length Based Password Validator for the properties of this Password Validator type.

`repeated-characters-password-validator`

Default {name}: Repeated Characters Password Validator

Enabled by default: true

See Repeated Characters Password Validator for the properties of this Password Validator type.

`similarity-based-password-validator`

Default {name}: Similarity Based Password Validator

Enabled by default: true

See Similarity Based Password Validator for the properties of this Password Validator type.

`unique-characters-password-validator`

Default {name}: Unique Characters Password Validator

Enabled by default: true

See Unique Characters Password Validator for the properties of this Password Validator type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Password Validator properties depend on the Password Validator type, which depends on the `--validator-name {name}` option.

`-t | --type {type}`

The type of Password Validator which should be created. The value for TYPE can be one of: attribute-value | character-set | custom | dictionary | length-based | repeated-characters | similarity-based | unique-characters.

Password Validator properties depend on the Password Validator type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

`attribute-value-password-validator`

Default {type}: Attribute Value Password Validator

Enabled by default: true

See Attribute Value Password Validator for the properties of this Password Validator type.

`character-set-password-validator`

Default {type}: Character Set Password Validator

Enabled by default: true

See Character Set Password Validator for the properties of this Password Validator type.

`dictionary-password-validator`

Default {type}: Dictionary Password Validator

Enabled by default: true

See Dictionary Password Validator for the properties of this Password Validator type.

`length-based-password-validator`

Default {type}: Length Based Password Validator

Enabled by default: true

See Length Based Password Validator for the properties of this Password Validator type.

`repeated-characters-password-validator`

Default {type}: Repeated Characters Password Validator

Enabled by default: true

See Repeated Characters Password Validator for the properties of this Password Validator type.

`similarity-based-password-validator`

Default {type}: Similarity Based Password Validator

Enabled by default: true

See Similarity Based Password Validator for the properties of this Password Validator type.

`unique-characters-password-validator`

Default {type}: Unique Characters Password Validator

Enabled by default: true

See Unique Characters Password Validator for the properties of this Password Validator type.

Attribute Value Password Validator

Password Validators of type attribute-value-password-validator have the following properties:

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against attribute values. If "false" then only match the entire password against attribute values otherwise ("true") check whether the password contains attribute values.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.AttributeValuePasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name(s) of the attribute(s) whose values should be checked to determine whether they match the provided password. If no values are provided, then the server checks if the proposed password matches the value of any attribute in the user's entry.

Default Value

All attributes in the user entry will be checked.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator should test the reversed value of the provided password as well as the order in which it was given.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Character Set Password Validator

Password Validators of type character-set-password-validator have the following properties:

allow-unclassified-characters

Description

Indicates whether this password validator allows passwords to contain characters outside of any of the user-defined character sets and ranges. If this is "false", then only those characters in the user-defined character sets and ranges may be used in passwords. Any password containing a character not included in any character set or range will be rejected.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set

Description

Specifies a character set containing characters that a password may contain and a value indicating the minimum number of characters required from that set. Each value must be an integer (indicating the minimum required characters from the set which may be zero, indicating that the character set is optional) followed by a colon and the characters to include in that set (for example, "3:abcdefghijklmnopqrstuvwxyz" indicates that a user password must contain at least three characters from the set of lowercase ASCII letters). Multiple character sets can be defined in separate values, although no character can appear in more than one character set.

Default Value

If no sets are specified, the validator only uses the defined character ranges.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set-ranges

Description

Specifies a character range containing characters that a password may contain and a value indicating the minimum number of characters required from that range. Each value must be an integer (indicating the minimum required characters from the range which may be zero, indicating that the character range is optional) followed by a colon and one or more range specifications. A range specification is 3 characters: the first character allowed, a minus, and the last character allowed. For example, "3:A-Za-z0-9". The ranges in each value should not overlap, and the characters in each range specification should be ordered.

Default Value

If no ranges are specified, the validator only uses the defined character sets.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.CharacterSetPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-character-sets

Description

Specifies the minimum number of character sets and ranges that a password must contain. This property should only be used in conjunction with optional character sets and ranges (those requiring zero characters). Its value must include any mandatory character sets and ranges (those requiring greater than zero characters). This is useful in situations where a password must contain characters from mandatory character sets and ranges, and characters from at least N optional character sets and ranges. For example, it is quite common to require that a password contains at least one non-alphanumeric character as well as characters from two alphanumeric character sets (lower-case, upper-case, digits). In this case, this property should be set to 3.

Default Value

The password must contain characters from each of the mandatory character sets and ranges and, if there are optional character sets and ranges, at least one character from one of the optional character sets and ranges.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Dictionary Password Validator

Password Validators of type dictionary-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator is to treat password characters in a case-sensitive manner. If it is set to true, then the validator rejects a password only if it appears in the dictionary with exactly the same capitalization as provided by the user.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against dictionary words. If "false" then only match the entire password against words otherwise ("true") check whether the password contains words.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dictionary-file

Description

Specifies the path to the file containing a list of words that cannot be used as passwords. It should be formatted with one word per line. The value can be an absolute path or a path that is relative to the OpenDJ instance root.

Default Value

For Unix and Linux systems: config/wordlist.txt. For Windows systems: config\wordlist.txt

Allowed Values

The path to any text file contained on the system that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.DictionaryPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator is to test the reversed value of the provided password as well as the order in which it was given. For example, if the user provides a new password of "password" and this configuration attribute is set to true, then the value "drowssap" is also tested against attribute values in the user's entry.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Length Based Password Validator

Password Validators of type length-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.LengthBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-password-length

Description

Specifies the maximum number of characters that can be included in a proposed password. A value of zero indicates that there will be no upper bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-length

Description

Specifies the minimum number of characters that must be included in a proposed password. A value of zero indicates that there will be no lower bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

6

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Repeated Characters Password Validator

Password Validators of type repeated-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. If the value of this property is false, the validator ignores any differences in capitalization when looking for consecutive characters in the password. If the value is true, the validator considers a character to be repeating only if all consecutive occurrences use the same capitalization.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.RepeatedCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-consecutive-length

Description

Specifies the maximum number of times that any character can appear consecutively in a password value. A value of zero indicates that no maximum limit is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Similarity Based Password Validator

Password Validators of type similarity-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.SimilarityBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-password-difference

Description

Specifies the minimum difference of new and old password. A value of zero indicates that no difference between passwords is acceptable.

Default Value

None

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Unique Characters Password Validator

Password Validators of type unique-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. A value of true indicates that the validator does not consider a capital letter to be the

same as its lower-case counterpart. A value of false indicates that the validator ignores differences in capitalization when looking at the number of unique characters in the password.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.UniqueCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-unique-characters

Description

Specifies the minimum number of unique characters that a password will be allowed to contain. A value of zero indicates that no minimum value is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-plugin(1)

Name

dsconfig create-plugin - Creates Plugins

Synopsis

`dsconfig create-plugin` {options}

Description

Creates Plugins.

Options

The `dsconfig create-plugin` command takes the following options:

`--plugin-name {name}`
: The name of the new Plugin.

  Plugin properties depend on the Plugin type, which depends on the {name} you provide.

  By default, OpenDJ directory server supports the following Plugin types:

  `attribute-cleanup-plugin`
  : Default {name}: Attribute Cleanup Plugin

    Enabled by default: true

    See Attribute Cleanup Plugin for the properties of this Plugin type.

  `change-number-control-plugin`
  : Default {name}: Change Number Control Plugin

    Enabled by default: true

    See Change Number Control Plugin for the properties of this Plugin type.

  `entry-uuid-plugin`
  : Default {name}: Entry UUID Plugin

    Enabled by default: true

    See Entry UUID Plugin for the properties of this Plugin type.

  `fractional-ldif-import-plugin`
  : Default {name}: Fractional LDIF Import Plugin

Enabled by default: true

See Fractional LDIF Import Plugin for the properties of this Plugin type.

`last-mod-plugin`

Default {name}: Last Mod Plugin

Enabled by default: true

See Last Mod Plugin for the properties of this Plugin type.

`ldap-attribute-description-list-plugin`

Default {name}: LDAP Attribute Description List Plugin

Enabled by default: true

See LDAP Attribute Description List Plugin for the properties of this Plugin type.

`password-policy-import-plugin`

Default {name}: Password Policy Import Plugin

Enabled by default: true

See Password Policy Import Plugin for the properties of this Plugin type.

`profiler-plugin`

Default {name}: Profiler Plugin

Enabled by default: true

See Profiler Plugin for the properties of this Plugin type.

`referential-integrity-plugin`

Default {name}: Referential Integrity Plugin

Enabled by default: true

See Referential Integrity Plugin for the properties of this Plugin type.

`samba-password-plugin`

Default {name}: Samba Password Plugin

Enabled by default: true

See Samba Password Plugin for the properties of this Plugin type.

`seven-bit-clean-plugin`

Default {name}: Seven Bit Clean Plugin

Enabled by default: true

See Seven Bit Clean Plugin for the properties of this Plugin type.

`unique-attribute-plugin`

Default {name}: Unique Attribute Plugin

Enabled by default: true

See Unique Attribute Plugin for the properties of this Plugin type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Plugin properties depend on the Plugin type, which depends on the `--plugin-name {name}` option.

`-t | --type {type}`

The type of Plugin which should be created. The value for TYPE can be one of: attribute-cleanup | change-number-control | custom | entry-uuid | fractional-ldif-import | last-mod | ldap-attribute-description-list | password-policy-import | profiler | referential-integrity | samba-password | seven-bit-clean | unique-attribute.

Plugin properties depend on the Plugin type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Plugin types:

`attribute-cleanup-plugin`

Default {type}: Attribute Cleanup Plugin

Enabled by default: true

See Attribute Cleanup Plugin for the properties of this Plugin type.

`change-number-control-plugin`

Default {type}: Change Number Control Plugin

Enabled by default: true

See Change Number Control Plugin for the properties of this Plugin type.

`entry-uuid-plugin`

Default {type}: Entry UUID Plugin

Enabled by default: true

See Entry UUID Plugin for the properties of this Plugin type.

`fractional-ldif-import-plugin`

Default {type}: Fractional LDIF Import Plugin

Enabled by default: true

See Fractional LDIF Import Plugin for the properties of this Plugin type.

`last-mod-plugin`

Default {type}: Last Mod Plugin

Enabled by default: true

See Last Mod Plugin for the properties of this Plugin type.

`ldap-attribute-description-list-plugin`

Default {type}: LDAP Attribute Description List Plugin

Enabled by default: true

See LDAP Attribute Description List Plugin for the properties of this Plugin type.

`password-policy-import-plugin`

Default {type}: Password Policy Import Plugin

Enabled by default: true

See Password Policy Import Plugin for the properties of this Plugin type.

`profiler-plugin`

Default {type}: Profiler Plugin

Enabled by default: true

See Profiler Plugin for the properties of this Plugin type.

`referential-integrity-plugin`

Default {type}: Referential Integrity Plugin

Enabled by default: true

See Referential Integrity Plugin for the properties of this Plugin type.

`samba-password-plugin`

Default {type}: Samba Password Plugin

Enabled by default: true

See Samba Password Plugin for the properties of this Plugin type.

`seven-bit-clean-plugin`

Default {type}: Seven Bit Clean Plugin

Enabled by default: true

See Seven Bit Clean Plugin for the properties of this Plugin type.

`unique-attribute-plugin`

Default {type}: Unique Attribute Plugin

Enabled by default: true

See Unique Attribute Plugin for the properties of this Plugin type.

Attribute Cleanup Plugin

Plugins of type attribute-cleanup-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.AttributeCleanupPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparseadd preparsemodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

remove-inbound-attributes

Description

A list of attributes which should be removed from incoming add or modify requests.

Default Value

No attributes will be removed

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rename-inbound-attributes

Description

A list of attributes which should be renamed in incoming add or modify requests.

Default Value

No attributes will be renamed

Allowed Values

An attribute name mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Change Number Control Plugin

Plugins of type change-number-control-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ChangeNumberControlPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postOperationAdd postOperationDelete postOperationModify postOperationModifyDN

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Entry UUID Plugin

Plugins of type entry-uuid-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.EntryUUIDPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport preoperationadd

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Fractional LDIF Import Plugin

Plugins of type fractional-ldif-import-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

None

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

None

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the

client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

Last Mod Plugin

Plugins of type last-mod-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LastModPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd preoperationmodify preoperationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

LDAP Attribute Description List Plugin

Plugins of type ldap-attribute-description-list-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LDAPADListPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparsesearch

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Policy Import Plugin

Plugins of type password-policy-import-plugin have the following properties:

default-auth-password-storage-scheme

Description

Specifies the names of password storage schemes that to be used for encoding passwords contained in attributes with the auth password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy should be used to govern them.

Default Value

If the default password policy uses an attribute with the auth password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes auth password values using the "SHA1" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import plug-in is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-user-password-storage-scheme

Description

Specifies the names of the password storage schemes to be used for encoding passwords contained in attributes with the user password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy is to be used to govern them.

Default Value

If the default password policy uses the attribute with the user password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes user password values using the "SSHA" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import Plugin is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.PasswordPolicyImportPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Profiler Plugin

Plugins of type profiler-plugin have the following properties:

enable-profiling-on-startup

Description

Indicates whether the profiler plug-in is to start collecting data automatically when the directory server is started. This property is read only when the server is started, and any changes take effect on the next restart. This property is typically set to "false" unless startup profiling is required, because otherwise the volume of data that can be collected can cause the server to run out of memory if it is not turned off in a timely manner.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.profiler.ProfilerPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

startup

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the

client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

profile-action

Description

Specifies the action that should be taken by the profiler. A value of "start" causes the profiler thread to start collecting data if it is not already active. A value of "stop" causes the profiler thread to stop collecting data and write it to disk, and a value of "cancel" causes the profiler thread to stop collecting data and discard anything that has been captured. These operations occur immediately.

Default Value

none

Allowed Values

cancel

Stop collecting profile data and discard what has been captured.

none

Do not take any action.

start

Start collecting profile data.

stop

Stop collecting profile data and write what has been captured to a file in the profile directory.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-directory

Description

Specifies the path to the directory where profile information is to be written. This path may be either an absolute path or a path that is relative to the root of the OpenDJ directory server instance. The directory must exist and the directory server must have permission to create new files in it.

Default Value

None

Allowed Values

The path to any directory that exists on the filesystem and that can be read and written by the server user.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-sample-interval

Description

Specifies the sample interval in milliseconds to be used when capturing profiling information in the server. When capturing data, the profiler thread sleeps for this length of time between calls to obtain traces for all threads running in the JVM.

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

NoneChanges to this configuration attribute take effect the next time the profiler is started.

Advanced Property

No

Read-only

No

Referential Integrity Plugin

Plugins of type referential-integrity-plugin have the following properties:

attribute-type

Description

Specifies the attribute types for which referential integrity is to be maintained. At least one attribute type must be specified, and the syntax of any attributes must be either a distinguished name (1.3.6.1.4.1.1466.115.121.1.12) or name and optional UID (1.3.6.1.4.1.1466.115.121.1.34).

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN that limits the scope within which referential integrity is maintained.

Default Value

Referential integrity is maintained in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references

Description

Specifies whether reference attributes must refer to existing entries. When this property is set to true, this plugin will ensure that any new references added as part of an add or modify operation point to existing entries, and that the referenced entries match the filter criteria for the referencing attribute, if specified.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-filter-criteria

Description

Specifies additional filter criteria which will be enforced when checking references. If a reference attribute has filter criteria defined then this plugin will ensure that any new references added as part of an add or modify operation refer to an existing entry which matches the specified filter.

Default Value

None

Allowed Values

An attribute-filter mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-scope-criteria

Description

Specifies whether referenced entries must reside within the same naming context as the entry containing the reference. The reference scope will only be enforced when reference checking is enabled.

Default Value

global

Allowed Values

global

References may refer to existing entries located anywhere in the Directory.

naming-context

References must refer to existing entries located within the same naming context.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ReferentialIntegrityPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

Specifies the log file location where the update records are written when the plug-in is in background-mode processing. The default location is the logs directory of the server instance, using the file name "referint".

Default Value

logs/referint

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postoperationdelete postoperationmodifydn subordinatemodifydn subordinatedelete preoperationadd preoperationmodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

update-interval

Description

Specifies the interval in seconds when referential integrity updates are made. If this value is 0, then the updates are made synchronously in the foreground.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Samba Password Plugin

Plugins of type samba-password-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SambaPasswordPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationmodify postoperationextended

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pwd-sync-policy

Description

Specifies which Samba passwords should be kept synchronized.

Default Value

sync-nt-password

Allowed Values

sync-lm-password

Synchronize the LanMan password attribute "sambaLMPassword"

sync-nt-password

Synchronize the NT password attribute "sambaNTPassword"

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

samba-administrator-dn

Description

Specifies the distinguished name of the user which Samba uses to perform Password Modify extended operations against this directory server in order to synchronize the userPassword attribute after the LanMan or NT passwords have been updated. The user must have the 'password-reset' privilege and should not be a root user. This user name can be used in order to identify Samba connections and avoid double re-synchronization of the same password. If this property is left undefined, then no password updates will be skipped.

Default Value

Synchronize all updates to user passwords

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Seven Bit Clean Plugin

Plugins of type seven-bit-clean-plugin have the following properties:

attribute-type

Description

Specifies the name or OID of an attribute type for which values should be checked to ensure that

they are 7-bit clean.

Default Value

uid mail userPassword

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN below which the checking is performed. Any attempt to update a value for one of the configured attributes below this base DN must be 7-bit clean for the operation to be allowed.

Default Value

All entries below all public naming contexts will be checked.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SevenBitCleanPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport preparseadd preparsemodify preparsemodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Unique Attribute Plugin

Plugins of type unique-attribute-plugin have the following properties:

base-dn

Description

Specifies a base DN within which the attribute must be unique.

Default Value

The plug-in uses the server's public naming contexts in the searches.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.UniqueAttributePlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd preoperationmodify preoperationmodifydn postoperationadd postoperationmodify postoperationmodifydn postsynchronizationadd postsynchronizationmodify postsynchronizationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the

client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

type

Description

Specifies the type of attributes to check for value uniqueness.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-replication-domain(1)

Name

dsconfig create-replication-domain - Creates Replication Domains

Synopsis

`dsconfig create-replication-domain` {options}

Description

Creates Replication Domains.

Options

The `dsconfig create-replication-domain` command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default {name}: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

`--domain-name {name}`

The name of the new Replication Domain.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default {name}: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Replication Domain properties depend on the Replication Domain type, which depends on the `--domain-name {name}` option.

Replication Domain

Replication Domains of type replication-domain have the following properties:

assured-sd-level

Description

The level of acknowledgment for Safe Data assured sub mode. When assured replication is configured in Safe Data mode, this value defines the number of replication servers (with the same group ID of the local server) that should acknowledge the sent update before the LDAP client call can return.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-timeout

Description

The timeout value when waiting for assured replication acknowledgments. Defines the amount of milliseconds the server will wait for assured acknowledgments (in either Safe Data or Safe Read assured replication modes) before returning anyway the LDAP client call.

Default Value

2000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-type

Description

Defines the assured replication mode of the replicated domain. The assured replication can be disabled or enabled. When enabled, two modes are available: Safe Data or Safe Read modes.

Default Value

not-assured

Allowed Values

not-assured

Assured replication is not enabled. Updates sent for replication (for being replayed on other LDAP servers in the topology) are sent without waiting for any acknowledgment and the LDAP client call returns immediately.

safe-data

Assured replication is enabled in Safe Data mode: updates sent for replication are subject to acknowledgment from the replication servers that have the same group ID as the local server (defined with the group-id property). The number of acknowledgments to expect is defined by the assured-sd-level property. After acknowledgments are received, LDAP client call returns.

safe-read

Assured replication is enabled in Safe Read mode: updates sent for replication are subject to acknowledgments from the LDAP servers in the topology that have the same group ID as the local server (defined with the group-id property). After acknowledgments are received, LDAP client call returns.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN of the replicated data.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

changetime-heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when sending its local change time to the Replication Server. The directory server sends a regular heart-beat to the Replication within the specified interval. The heart-beat indicates the change time of the directory server to the Replication Server.

Default Value

1000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

conflicts-historical-purge-delay

Description

This delay indicates the time (in minutes) the domain keeps the historical information necessary to solve conflicts.When a change stored in the historical part of the user entry has a date (from its replication ChangeNumber) older than this delay, it is candidate to be purged. The purge is applied on 2 events: modify of the entry, dedicated purge task.

Default Value

1440m

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 minutes.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-exclude

Description

Allows to exclude some attributes to replicate to this server. If fractional-exclude configuration attribute is used, attributes specified in this attribute will be ignored (not added/modified/deleted) when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-include attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be excluded. The object class may be "*" indicating that the attribute type(s) should be excluded regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-include

Description

Allows to include some attributes to replicate to this server. If fractional-include configuration attribute is used, only attributes specified in this attribute will be added/modified/deleted when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-exclude attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be included. The object class may be "*" indicating that the attribute type(s) should be included regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group ID associated with this replicated domain. This value defines the group ID of the replicated domain. The replication system will preferably connect and send updates to replicate to a replication server with the same group ID as its own one (the local server group ID).

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when communicating with Replication Servers. The directory server expects a regular heart-beat coming from the Replication Server within the specified interval. If a heartbeat is not received within the interval, the Directory Server closes its connection and connects to another Replication Server.

Default Value

10000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 100 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

initialization-window-size

Description

Specifies the window size that this directory server may use when communicating with remote Directory Servers for initialization.

Default Value

100

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

isolation-policy

Description

Specifies the behavior of the directory server if a write operation is attempted on the data within the Replication Domain when none of the configured Replication Servers are available.

Default Value

reject-all-updates

Allowed Values

accept-all-updates

Indicates that updates should be accepted even though it is not possible to send them to any Replication Server. Best effort is made to re-send those updates to a Replication Servers when one of them is available, however those changes are at risk because they are only available from the historical information. This mode can also introduce high replication latency.

reject-all-updates

Indicates that all updates attempted on this Replication Domain are rejected when no Replication Server is available.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-changenumber

Description

Indicates if this server logs the ChangeNumber in access log. This boolean indicates if the

domain should log the ChangeNumber of replicated operations in the access log.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

referrals-url

Description

The URLs other LDAP servers should use to refer to the local server. URLs used by peer servers in the topology to refer to the local server through LDAP referrals. If this attribute is not defined, every URLs available to access this server will be used. If defined, only URLs specified here will be used.

Default Value

None

Allowed Values

A LDAP URL compliant with RFC 2255.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of the Replication Servers within the Replication Domain to which the directory server should try to connect at startup time. Addresses must be specified using the syntax: hostname:port

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

server-id

Description

Specifies a unique identifier for the directory server within the Replication Domain. Each directory server within the same Replication Domain must have a different server ID. A directory server which is a member of multiple Replication Domains may use the same server ID for each of its Replication Domain configurations.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

solve-conflicts

Description

Indicates if this server solves conflict. This boolean indicates if this domain keeps the historical information necessary to solve conflicts. When set to false the server will not maintain historical information and will therefore not be able to solve conflict. This should therefore be done only if the replication is used in a single master type of deployment.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the directory server will use when communicating with Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-replication-server(1)

Name

dsconfig create-replication-server - Creates Replication Servers

Synopsis

`dsconfig create-replication-server` {options}

Description

Creates Replication Servers.

Options

The `dsconfig create-replication-server` command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Server properties depend on the Replication Server type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

`replication-server`

Default {name}: Replication Server

Enabled by default: false

See Replication Server for the properties of this Replication Server type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Replication Server properties depend on the Replication Server type, which depends on the `--provider-name {name}` option.

Replication Server

Replication Servers of type replication-server have the following properties:

assured-timeout

Description

The timeout value when waiting for assured mode acknowledgments. Defines the number of milliseconds that the replication server will wait for assured acknowledgments (in either Safe Data or Safe Read assured sub modes) before forgetting them and answer to the entity that sent an update and is waiting for acknowledgment.

Default Value

1000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compute-change-number

Description

Whether the replication server will compute change numbers. This boolean tells the replication server to compute change numbers for each replicated change by maintaining a change number index database. Changenumbers are computed according to http://tools.ietf.org/html/draft-good-ldap-changelog-04. Note this functionality has an impact on CPU, disk accesses and storage. If changenumbers are not required, it is advisable to set this value to false.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the replication change-log should make records readable only by Directory Server. Throughput and disk space are affected by the more expensive operations taking place. Confidentiality is achieved by encrypting records on all domains managed by this replication server. Encrypting the records prevents unauthorized parties from accessing contents of LDAP operations. For complete protection, consider enabling secure communications between servers. Change number indexing is not affected by the setting.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect operations performed after the change.

Advanced Property

No

Read-only

No

degraded-status-threshold

Description

The number of pending changes as threshold value for putting a directory server in degraded status. This value represents a number of pending changes a replication server has in queue for sending to a directory server. Once this value is crossed, the matching directory server goes in degraded status. When number of pending changes goes back under this value, the directory server is put back in normal status. 0 means status analyzer is disabled and directory servers are never put in degraded status.

Default Value

5000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group id for the replication server. This value defines the group id of the replication server. The replication system of a LDAP server uses the group id of the replicated domain and tries to connect, if possible, to a replication with the same group id.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

monitoring-period

Description

The period between sending of monitoring messages. Defines the duration that the replication server will wait before sending new monitoring messages to its peers (replication servers and directory servers). Larger values increase the length of time it takes for a directory server to detect and switch to a more suitable replication server, whereas smaller values increase the amount of background network traffic.

Default Value

60s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

Specifies the number of changes that are kept in memory for each directory server in the Replication Domain.

Default Value

10000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

replication-db-directory

Description

The path where the Replication Server stores all persistent information.

Default Value

changelogDb

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

replication-port

Description

The port on which this Replication Server waits for connections from other Replication Servers or Directory Servers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-purge-delay

Description

The time (in seconds) after which the Replication Server erases all persistent information.

Default Value

3 days

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of other Replication Servers to which this Replication Server tries to connect at startup time. Addresses must be specified using the syntax: "hostname:port". If IPv6 addresses are used as the hostname, they must be specified using the syntax "[IPv6Address]:port".

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server-id

Description

Specifies a unique identifier for the Replication Server. Each Replication Server must have a different server ID.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

weight

Description

The weight of the replication server. The weight affected to the replication server. Each replication server of the topology has a weight. When combined together, the weights of the replication servers of a same group can be translated to a percentage that determines the quantity of directory servers of the topology that should be connected to a replication server. For instance imagine a topology with 3 replication servers (with the same group id) with the following weights: RS1=1, RS2=1, RS3=2. This means that RS1 should have 25% of the directory servers connected in the topology, RS2 25%, and RS3 50%. This may be useful if the replication servers of the topology have a different power and one wants to spread the load between the replication servers according to their power.

Default Value

1

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the Replication Server uses when communicating with other Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-sasl-mechanism-handler(1)

Name

dsconfig create-sasl-mechanism-handler - Creates SASL Mechanism Handlers

Synopsis

`dsconfig create-sasl-mechanism-handler` {options}

Description

Creates SASL Mechanism Handlers.

Options

The `dsconfig create-sasl-mechanism-handler` command takes the following options:

`--handler-name {name}`

The name of the new SASL Mechanism Handler.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

`anonymous-sasl-mechanism-handler`

Default {name}: Anonymous SASL Mechanism Handler

Enabled by default: true

See Anonymous SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`cram-md5-sasl-mechanism-handler`

Default {name}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See Cram MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`digest-md5-sasl-mechanism-handler`

Default {name}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See Digest MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler

type.

`external-sasl-mechanism-handler`

Default {name}: External SASL Mechanism Handler

Enabled by default: true

See External SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`gssapi-sasl-mechanism-handler`

Default {name}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See GSSAPI SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`plain-sasl-mechanism-handler`

Default {name}: Plain SASL Mechanism Handler

Enabled by default: true

See Plain SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the `--handler-name {name}` option.

`-t | --type {type}`

The type of SASL Mechanism Handler which should be created. The value for TYPE can be one of: anonymous | cram-md5 | custom | digest-md5 | external | gssapi | plain.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

`anonymous-sasl-mechanism-handler`

Default {type}: Anonymous SASL Mechanism Handler

Enabled by default: true

See Anonymous SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`cram-md5-sasl-mechanism-handler`

Default {type}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See Cram MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`digest-md5-sasl-mechanism-handler`

Default {type}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See Digest MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`external-sasl-mechanism-handler`

Default {type}: External SASL Mechanism Handler

Enabled by default: true

See External SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`gssapi-sasl-mechanism-handler`

Default {type}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See GSSAPI SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`plain-sasl-mechanism-handler`

Default {type}: Plain SASL Mechanism Handler

Enabled by default: true

See Plain SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

Anonymous SASL Mechanism Handler

SASL Mechanism Handlers of type anonymous-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.AnonymousSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Cram MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type cram-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper used with this SASL mechanism handler to match the authentication ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Cram MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.CRAMMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Digest MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type digest-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Digest MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.DigestMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realms that is to be used by the server for DIGEST-MD5 authentication. If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Default Value

If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Allowed Values

Any realm string that does not contain a comma.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the server that is used when validating the digest-uri parameter during the authentication process. If this configuration attribute is present, then the server expects that clients use a digest-uri equal to "ldap/" followed by the value of this attribute. For example, if the attribute has a value of "directory.example.com", then the server expects clients to use a digest-uri of "ldap/directory.example.com". If no value is provided, then the server does not attempt to validate the digest-uri provided by the client and accepts any value.

Default Value

The server attempts to determine the fully-qualified domain name dynamically.

Allowed Values

The fully-qualified address that is expected for clients to use when connecting to the server and authenticating via DIGEST-MD5.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

External SASL Mechanism Handler

SASL Mechanism Handlers of type external-sasl-mechanism-handler have the following properties:

certificate-attribute

Description

Specifies the name of the attribute to hold user certificates. This property must specify the name of a valid attribute type defined in the server schema.

Default Value

userCertificate

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-mapper

Description

Specifies the name of the certificate mapper that should be used to match client certificates to user entries.

Default Value

None

Allowed Values

The DN of any Certificate Mapper. The referenced certificate mapper must be enabled when the External SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-validation-policy

Description

Indicates whether to attempt to validate the peer certificate against a certificate held in the user's entry.

Default Value

None

Allowed Values

always

Always require the peer certificate to be present in the user's entry.

ifpresent

If the user's entry contains one or more certificates, require that one of them match the peer certificate.

never

Do not look for the peer certificate to be present in the user's entry.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.ExternalSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

GSSAPI SASL Mechanism Handler

SASL Mechanism Handlers of type gssapi-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the Kerberos principal included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the GSSAPI SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.GSSAPISASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

kdc-address

Description

Specifies the address of the KDC that is to be used for Kerberos processing. If provided, this property must be a fully-qualified DNS-resolvable name. If this property is not provided, then the server attempts to determine it from the system-wide Kerberos configuration.

Default Value

The server attempts to determine the KDC address from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

keytab

Description

Specifies the path to the keytab file that should be used for Kerberos processing. If provided, this is either an absolute path or one that is relative to the server instance root.

Default Value

The server attempts to use the system-wide default keytab.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

principal-name

Description

Specifies the principal name. It can either be a simple user name or a service name such as host/example.com. If this property is not provided, then the server attempts to build the principal name by appending the fully qualified domain name to the string "ldap/".

Default Value

The server attempts to determine the principal name from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realm to be used for GSSAPI authentication.

Default Value

The server attempts to determine the realm from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the system.

Default Value

The server attempts to determine the fully-qualified domain name dynamically .

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Plain SASL Mechanism Handler

SASL Mechanism Handlers of type plain-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Plain SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.PlainSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-schema-provider(1)

Name

dsconfig create-schema-provider - Creates Schema Providers

Synopsis

`dsconfig create-schema-provider` {options}

Description

Creates Schema Providers.

Options

The `dsconfig create-schema-provider` command takes the following options:

`--provider-name {name}`

The name of the new Schema Provider.

Schema Provider properties depend on the Schema Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

`core-schema`

Default {name}: Core Schema

Enabled by default: true

See Core Schema for the properties of this Schema Provider type.

`json-schema`

Default {name}: Json Schema

Enabled by default: true

See Json Schema for the properties of this Schema Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Schema Provider properties depend on the Schema Provider type, which depends on the `--provider-name {name}` option.

`-t | --type {type}`

The type of Schema Provider which should be created (Default: generic). The value for TYPE can be one of: core-schema | generic | json-schema.

Schema Provider properties depend on the Schema Provider type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

`core-schema`

Default {type}: Core Schema

Enabled by default: true

See Core Schema for the properties of this Schema Provider type.

`json-schema`

Default {type}: Json Schema

Enabled by default: true

See Json Schema for the properties of this Schema Provider type.

Core Schema

Schema Providers of type core-schema have the following properties:

allow-attribute-types-with-no-sup-or-syntax

Description

Indicates whether the schema should allow attribute type definitions that do not declare a superior attribute type or syntax When set to true, invalid attribute type definitions will use the default syntax.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-zero-length-values-directory-string

Description

Indicates whether zero-length (that is, an empty string) values are allowed for directory string. This is technically not allowed by the revised LDAPv3 specification, but some environments may require it for backward compatibility with servers that do allow it.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disabled-matching-rule

Description

The set of disabled matching rules. Matching rules must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled matching rule.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

disabled-syntax

Description

The set of disabled syntaxes. Syntaxes must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled syntax, or NONE

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Core Schema implementation.

Default Value

org.opends.server.schema.CoreSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

json-validation-policy

Description

Specifies the policy that will be used when validating JSON syntax values.

Default Value

strict

Allowed Values

disabled

JSON syntax values will not be validated and, as a result any sequence of bytes will be acceptable.

lenient

JSON syntax values must comply with RFC 7159 except: 1) comments are allowed, 2) single quotes may be used instead of double quotes, and 3) unquoted control characters are allowed in strings.

strict

JSON syntax values must strictly conform to RFC 7159.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-certificates

Description

Indicates whether X.509 Certificate values are required to strictly comply with the standard definition for this syntax. When set to false, certificates will not be validated and, as a result any sequence of bytes will be acceptable.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-country-string

Description

Indicates whether country code values are required to strictly comply with the standard definition for this syntax. When set to false, country codes will not be validated and, as a result any string containing 2 characters will be acceptable.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-jpeg-photos

Description

Indicates whether to require JPEG values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-telephone-numbers

Description

Indicates whether to require telephone number values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strip-syntax-min-upper-bound-attribute-type-description

Description

Indicates whether the suggested minimum upper bound appended to an attribute's syntax OID in it's schema definition Attribute Type Description is stripped off. When retrieving the server's schema, some APIs (JNDI) fail in their syntax lookup methods, because they do not parse this value correctly. This configuration option allows the server to be configured to provide schema definitions these APIs can parse correctly.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Json Schema

Schema Providers of type json-schema have the following properties:

case-sensitive-strings

Description

Indicates whether JSON string comparisons should be case-sensitive.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ignore-white-space

Description

Indicates whether JSON string comparisons should ignore white-space. When enabled all leading and trailing white space will be removed and intermediate white space will be reduced to a single character.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

indexed-field

Description

Specifies which JSON fields should be indexed. A field will be indexed if it matches any of the configured field patterns.

Default Value

All JSON fields will be indexed.

Allowed Values

A JSON pointer which may include wild-cards. A single '**' wild-card matches at most a single path element, whereas a double '**' matches zero or more path elements.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Json Schema implementation.

Default Value

org.opends.server.schema.JsonSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

matching-rule-name

Description

The name of the custom JSON matching rule.

Default Value

The matching rule will not have a name.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

matching-rule-oid

Description

The numeric OID of the custom JSON matching rule.

Default Value

None

Allowed Values

The OID of the matching rule.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-service-discovery-mechanism(1)

Name

dsconfig create-service-discovery-mechanism - Creates Service Discovery Mechanisms

Synopsis

`dsconfig create-service-discovery-mechanism` {options}

Description

Creates Service Discovery Mechanisms.

Options

The `dsconfig create-service-discovery-mechanism` command takes the following options:

`--mechanism-name {name}`

The name of the new Service Discovery Mechanism.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

`replication-service-discovery-mechanism`

Default {name}: Replication Service Discovery Mechanism

Enabled by default: false

See Replication Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`static-service-discovery-mechanism`

Default {name}: Static Service Discovery Mechanism

Enabled by default: false

See Static Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one

value to it.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the `--mechanism-name {name}` option.

`-t | --type {type}`

The type of Service Discovery Mechanism which should be created (Default: generic). The value for TYPE can be one of: generic | replication | static.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

`replication-service-discovery-mechanism`

Default {type}: Replication Service Discovery Mechanism

Enabled by default: false

See Replication Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`static-service-discovery-mechanism`

Default {type}: Static Service Discovery Mechanism

Enabled by default: false

See Static Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

Replication Service Discovery Mechanism

Service Discovery Mechanisms of type replication-service-discovery-mechanism have the following properties:

bind-dn

Description

The bind DN for periodically reading replication server configurations The bind DN must be present on all replication servers and directory servers, it must be able to read the server configuration.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

bind-password

Description

The bind password for periodically reading replication server configurations The bind password must be the same on all replication and directory servers

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

discovery-interval

Description

Interval between two replication server configuration discovery queries. Specifies how frequently to query a replication server configuration in order to discover information about available directory server replicas.

Default Value

60s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.ReplicationServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-group-id

Description

Replication domain group ID of preferred directory server replicas. Directory server replicas with this replication domain group ID will be preferred over other directory server replicas. Secondary server replicas will only be used when all primary server replicas become unavailable.

Default Value

All the server replicas will be treated the same.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the list of replication servers to contact periodically when discovering server replicas.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service

Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

Static Service Discovery Mechanism

Service Discovery Mechanisms of type static-service-discovery-mechanism have the following properties:

discovery-interval

Description

Interval between two server configuration discovery executions. Specifies how frequently to read the configuration of the servers in order to discover their new information.

Default Value

60s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.StaticServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to

access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-server

Description

Specifies a list of servers that will be used in preference to secondary servers when available.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-server

Description

Specifies a list of servers that will be used in place of primary servers when all primary servers are unavailable.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig create-synchronization-provider(1)

Name

dsconfig create-synchronization-provider - Creates Synchronization Providers

Synopsis

`dsconfig create-synchronization-provider` {options}

Description

Creates Synchronization Providers.

Options

The `dsconfig create-synchronization-provider` command takes the following options:

`--provider-name {name}`

The name of the new Synchronization Provider.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

`replication-synchronization-provider`

Default {name}: Replication Synchronization Provider

Enabled by default: true

See Replication Synchronization Provider for the properties of this Synchronization Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the `--provider-name {name}` option.

`-t | --type {type}`

The type of Synchronization Provider which should be created. The value for TYPE can be one of: custom | replication.

Synchronization Provider properties depend on the Synchronization Provider type, which

depends on the {type} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

`replication-synchronization-provider`

Default {type}: Replication Synchronization Provider

Enabled by default: true

See Replication Synchronization Provider for the properties of this Synchronization Provider type.

Replication Synchronization Provider

Synchronization Providers of type replication-synchronization-provider have the following properties:

connection-timeout

Description

Specifies the timeout used when connecting to peers and when performing SSL negotiation.

Default Value

5 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Synchronization Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Synchronization Provider implementation.

Default Value

org.opends.server.replication.plugin.MultimasterReplication

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SynchronizationProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-update-replay-threads

Description

Specifies the number of update replay threads. This value is the number of threads created for replaying every updates received for all the replication domains.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-trust-manager-provider(1)

Name

dsconfig create-trust-manager-provider - Creates Trust Manager Providers

Synopsis

`dsconfig create-trust-manager-provider` {options}

Description

Creates Trust Manager Providers.

Options

The `dsconfig create-trust-manager-provider` command takes the following options:

`--provider-name {name}`

The name of the new Trust Manager Provider.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

`blind-trust-manager-provider`

Default {name}: Blind Trust Manager Provider

Enabled by default: true

See Blind Trust Manager Provider for the properties of this Trust Manager Provider type.

`file-based-trust-manager-provider`

Default {name}: File Based Trust Manager Provider

Enabled by default: true

See File Based Trust Manager Provider for the properties of this Trust Manager Provider type.

`ldap-trust-manager-provider`

Default {name}: LDAP Trust Manager Provider

Enabled by default: true

See LDAP Trust Manager Provider for the properties of this Trust Manager Provider type.

`pkcs11-trust-manager-provider`

Default {name}: PKCS11 Trust Manager Provider

Enabled by default: true

See PKCS11 Trust Manager Provider for the properties of this Trust Manager Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the `--provider-name {name}` option.

`-t | --type {type}`

The type of Trust Manager Provider which should be created. The value for TYPE can be one of: blind | custom | file-based | ldap | pkcs11.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

`blind-trust-manager-provider`

Default {type}: Blind Trust Manager Provider

Enabled by default: true

See Blind Trust Manager Provider for the properties of this Trust Manager Provider type.

`file-based-trust-manager-provider`

Default {type}: File Based Trust Manager Provider

Enabled by default: true

See File Based Trust Manager Provider for the properties of this Trust Manager Provider type.

`ldap-trust-manager-provider`

Default {type}: LDAP Trust Manager Provider

Enabled by default: true

See LDAP Trust Manager Provider for the properties of this Trust Manager Provider type.

`pkcs11-trust-manager-provider`

Default {type}: PKCS11 Trust Manager Provider

Enabled by default: true

See PKCS11 Trust Manager Provider for the properties of this Trust Manager Provider type.

Blind Trust Manager Provider

Trust Manager Providers of type blind-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Blind Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.BlindTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Trust Manager Provider

Trust Manager Providers of type file-based-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file containing the trust information. It can be an absolute path or a path that is relative to the OpenDJ instance root. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

An absolute path or a path that is relative to the OpenDJ directory server instance root.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the trust store file. Valid values always include 'JKS' and 'PKCS12', but different implementations can allow other values as well. If no value is provided, then the JVM default value is used. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment. The "JKS" and "PKCS12" formats are typically available in Java environments.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

LDAP Trust Manager Provider

Trust Manager Providers of type ldap-trust-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

PKCS11 Trust Manager Provider

Trust Manager Providers of type pkcs11-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11TrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the

PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig create-virtual-attribute(1)

Name

dsconfig create-virtual-attribute - Creates Virtual Attributes

Synopsis

`dsconfig create-virtual-attribute` {options}

Description

Creates Virtual Attributes.

Options

The `dsconfig create-virtual-attribute` command takes the following options:

`--name {name}`

The name of the new Virtual Attribute.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

`collective-attribute-subentries-virtual-attribute`

Default {name}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See Collective Attribute Subentries Virtual Attribute for the properties of this Virtual Attribute type.

`entity-tag-virtual-attribute`

Default {name}: Entity Tag Virtual Attribute

Enabled by default: true

See Entity Tag Virtual Attribute for the properties of this Virtual Attribute type.

`entry-dn-virtual-attribute`

Default {name}: Entry DN Virtual Attribute

Enabled by default: true

See Entry DN Virtual Attribute for the properties of this Virtual Attribute type.

`entry-uuid-virtual-attribute`

Default {name}: Entry UUID Virtual Attribute

Enabled by default: true

See Entry UUID Virtual Attribute for the properties of this Virtual Attribute type.

`governing-structure-rule-virtual-attribute`

Default {name}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See Governing Structure Rule Virtual Attribute for the properties of this Virtual Attribute type.

`has-subordinates-virtual-attribute`

Default {name}: Has Subordinates Virtual Attribute

Enabled by default: true

See Has Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`is-member-of-virtual-attribute`

Default {name}: Is Member Of Virtual Attribute

Enabled by default: true

See Is Member Of Virtual Attribute for the properties of this Virtual Attribute type.

`member-virtual-attribute`

Default {name}: Member Virtual Attribute

Enabled by default: true

See Member Virtual Attribute for the properties of this Virtual Attribute type.

`num-subordinates-virtual-attribute`

Default {name}: Num Subordinates Virtual Attribute

Enabled by default: true

See Num Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`password-expiration-time-virtual-attribute`

Default {name}: Password Expiration Time Virtual Attribute

Enabled by default: true

See Password Expiration Time Virtual Attribute for the properties of this Virtual Attribute type.

`password-policy-subentry-virtual-attribute`

Default {name}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See Password Policy Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`structural-object-class-virtual-attribute`

Default {name}: Structural Object Class Virtual Attribute

Enabled by default: true

See Structural Object Class Virtual Attribute for the properties of this Virtual Attribute type.

`subschema-subentry-virtual-attribute`

Default {name}: Subschema Subentry Virtual Attribute

Enabled by default: true

See Subschema Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`user-defined-virtual-attribute`

Default {name}: User Defined Virtual Attribute

Enabled by default: true

See User Defined Virtual Attribute for the properties of this Virtual Attribute type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the `--name {name}` option.

`-t | --type {type}`

The type of Virtual Attribute which should be created. The value for TYPE can be one of: collective-attribute-subentries | custom | entity-tag | entry-dn | entry-uuid | governing-structure-rule | has-subordinates | is-member-of | member | num-subordinates | password-expiration-time | password-policy-subentry | structural-object-class | subschema-subentry | user-defined.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

`collective-attribute-subentries-virtual-attribute`

Default {type}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See Collective Attribute Subentries Virtual Attribute for the properties of this Virtual Attribute type.

`entity-tag-virtual-attribute`

Default {type}: Entity Tag Virtual Attribute

Enabled by default: true

See Entity Tag Virtual Attribute for the properties of this Virtual Attribute type.

`entry-dn-virtual-attribute`

Default {type}: Entry DN Virtual Attribute

Enabled by default: true

See Entry DN Virtual Attribute for the properties of this Virtual Attribute type.

`entry-uuid-virtual-attribute`

Default {type}: Entry UUID Virtual Attribute

Enabled by default: true

See Entry UUID Virtual Attribute for the properties of this Virtual Attribute type.

`governing-structure-rule-virtual-attribute`

Default {type}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See Governing Structure Rule Virtual Attribute for the properties of this Virtual Attribute type.

`has-subordinates-virtual-attribute`

Default {type}: Has Subordinates Virtual Attribute

Enabled by default: true

See Has Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`is-member-of-virtual-attribute`

Default {type}: Is Member Of Virtual Attribute

Enabled by default: true

See Is Member Of Virtual Attribute for the properties of this Virtual Attribute type.

`member-virtual-attribute`

Default {type}: Member Virtual Attribute

Enabled by default: true

See Member Virtual Attribute for the properties of this Virtual Attribute type.

`num-subordinates-virtual-attribute`

Default {type}: Num Subordinates Virtual Attribute

Enabled by default: true

See Num Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`password-expiration-time-virtual-attribute`

Default {type}: Password Expiration Time Virtual Attribute

Enabled by default: true

See Password Expiration Time Virtual Attribute for the properties of this Virtual Attribute type.

`password-policy-subentry-virtual-attribute`

Default {type}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See Password Policy Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`structural-object-class-virtual-attribute`

Default {type}: Structural Object Class Virtual Attribute

Enabled by default: true

See Structural Object Class Virtual Attribute for the properties of this Virtual Attribute type.

`subschema-subentry-virtual-attribute`

Default {type}: Subschema Subentry Virtual Attribute

Enabled by default: true

See Subschema Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`user-defined-virtual-attribute`

Default {type}: User Defined Virtual Attribute

Enabled by default: true

See User Defined Virtual Attribute for the properties of this Virtual Attribute type.

Collective Attribute Subentries Virtual Attribute

Virtual Attributes of type collective-attribute-subentries-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

collectiveAttributeSubentries

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.CollectiveAttributeSubentriesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Entity Tag Virtual Attribute

Virtual Attributes of type entity-tag-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

etag

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

checksum-algorithm

Description

The algorithm which should be used for calculating the entity tag checksum value.

Default Value

adler-32

Allowed Values

adler-32

The Adler-32 checksum algorithm which is almost as reliable as a CRC-32 but can be computed much faster.

crc-32

The CRC-32 checksum algorithm.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

excluded-attribute

Description

The list of attributes which should be ignored when calculating the entity tag checksum value. Certain attributes like "ds-sync-hist" may vary between replicas due to different purging schedules and should not be included in the checksum.

Default Value

ds-sync-hist

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntityTagVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Entry DN Virtual Attribute

Virtual Attributes of type entry-dn-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryDN

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to

use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryDNVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Entry UUID Virtual Attribute

Virtual Attributes of type entry-uuid-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryUUID

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no

values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryUUIDVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Governing Structure Rule Virtual Attribute

Virtual Attributes of type governing-structure-rule-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

governingStructureRule

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.GoverningSturctureRuleVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Has Subordinates Virtual Attribute

Virtual Attributes of type has-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

hasSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.HasSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Is Member Of Virtual Attribute

Virtual Attributes of type is-member-of-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

isMemberOf

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry

and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those

filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.IsMemberOfVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Member Virtual Attribute

Virtual Attributes of type member-virtual-attribute have the following properties:

allow-retrieving-membership

Description

Indicates whether to handle requests that request all values for the virtual attribute. This operation can be very expensive in some cases and is not consistent with the primary function of virtual static groups, which is to make it possible to use static group idioms to determine whether a given user is a member. If this attribute is set to false, attempts to retrieve the entire set of values receive an empty set, and only attempts to determine whether the attribute has a specific value or set of values (which is the primary anticipated use for virtual static groups) are handled properly.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an

entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.MemberVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Num Subordinates Virtual Attribute

Virtual Attributes of type num-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

numSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry

and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those

filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.NumSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Password Expiration Time Virtual Attribute

Virtual Attributes of type password-expiration-time-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

ds-pwp-password-expiration-time

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordExpirationTimeVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Password Policy Subentry Virtual Attribute

Virtual Attributes of type password-policy-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

pwdPolicySubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no

values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordPolicySubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Structural Object Class Virtual Attribute

Virtual Attributes of type structural-object-class-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

structuralObjectClass

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.StructuralObjectClassVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subschema Subentry Virtual Attribute

Virtual Attributes of type subschema-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

subschemaSubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.SubschemaSubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

User Defined Virtual Attribute

Virtual Attributes of type user-defined-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry

and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those

filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.UserDefinedVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

value

Description

Specifies the values to be included in the virtual attribute.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-access-log-filtering-criteria(1)

Name

dsconfig delete-access-log-filtering-criteria - Deletes Access Log Filtering Criteria

Synopsis

`dsconfig delete-access-log-filtering-criteria` {options}

Description

Deletes Access Log Filtering Criteria.

Options

The `dsconfig delete-access-log-filtering-criteria` command takes the following options:

`--publisher-name {name}`

The name of the Access Log Publisher.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

`--criteria-name {name}`

The name of the Access Log Filtering Criteria.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

`-f | --force`

Ignore non-existent Access Log Filtering Criteria.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default null: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

Access Log Filtering Criteria

Access Log Filtering Criteria of type access-log-filtering-criteria have the following properties:

connection-client-address-equal-to

Description

Filters log records associated with connections which match at least one of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-client-address-not-equal-to

Description

Filters log records associated with connections which do not match any of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-port-equal-to

Description

Filters log records associated with connections to any of the specified listener port numbers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-protocol-equal-to

Description

Filters log records associated with connections which match any of the specified protocols. Typical values include "ldap", "ldaps", or "jmx".

Default Value

None

Allowed Values

The protocol name as reported in the access log.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-type

Description

Filters log records based on their type.

Default Value

None

Allowed Values

abandon

Abandon operations

add

Add operations

bind

Bind operations

compare

Compare operations

connect

Client connections

delete

Delete operations

disconnect

Client disconnections

extended

Extended operations

modify

Modify operations

rename

Rename operations

search

Search operations

unbind

Unbind operations

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-equal-to

Description

Filters operation log records associated with operations which target entries matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,,**dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-not-equal-to

Description

Filters operation log records associated with operations which target entries matching none of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,,**dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-greater-than

Description

Filters operation response log records associated with operations which took longer than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-less-than

Description

Filters operation response log records associated with operations which took less than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-equal-to

Description

Filters operation response log records associated with operations which include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-not-equal-to

Description

Filters operation response log records associated with operations which do not include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-is-indexed

Description

Filters search operation response log records associated with searches which were either indexed or unindexed. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-greater-than

Description

Filters search operation response log records associated with searches which returned more than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-less-than

Description

Filters search operation response log records associated with searches which returned less than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-equal-to

Description

Filters log records associated with users matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-not-equal-to

Description

Filters log records associated with users which do not match any of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-member-of

Description

Filters log records associated with users which are members of at least one of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-not-member-of

Description

Filters log records associated with users which are not members of any of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-account-status-notification-handler(1)

Name

dsconfig delete-account-status-notification-handler - Deletes Account Status Notification Handlers

Synopsis

`dsconfig delete-account-status-notification-handler` {options}

Description

Deletes Account Status Notification Handlers.

Options

The `dsconfig delete-account-status-notification-handler` command takes the following options:

`--handler-name {name}`

The name of the Account Status Notification Handler.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

`error-log-account-status-notification-handler`

Default {name}: Error Log Account Status Notification Handler

Enabled by default: true

See Error Log Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`smtp-account-status-notification-handler`

Default {name}: SMTP Account Status Notification Handler

Enabled by default: true

See SMTP Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`-f | --force`

Ignore non-existent Account Status Notification Handlers.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

`error-log-account-status-notification-handler`

Default null: Error Log Account Status Notification Handler

Enabled by default: true

See Error Log Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`smtp-account-status-notification-handler`

Default null: SMTP Account Status Notification Handler

Enabled by default: true

See SMTP Account Status Notification Handler for the properties of this Account Status Notification Handler type.

Error Log Account Status Notification Handler

Account Status Notification Handlers of type error-log-account-status-notification-handler have the following properties:

account-status-notification-type

Description

Indicates which types of event can trigger an account status notification.

Default Value

None

Allowed Values

account-disabled

Generate a notification whenever a user account has been disabled by an administrator.

account-enabled

Generate a notification whenever a user account has been enabled by an administrator.

account-expired

Generate a notification whenever a user authentication has failed because the account has expired.

account-idle-locked

Generate a notification whenever a user account has been locked because it was idle for too long.

account-permanently-locked

Generate a notification whenever a user account has been permanently locked after too many failed attempts.

account-reset-locked

Generate a notification whenever a user account has been locked, because the password had been reset by an administrator but not changed by the user within the required interval.

account-temporarily-locked

Generate a notification whenever a user account has been temporarily locked after too many failed attempts.

account-unlocked

Generate a notification whenever a user account has been unlocked by an administrator.

password-changed

Generate a notification whenever a user changes his/her own password.

password-expired

Generate a notification whenever a user authentication has failed because the password has expired.

password-expiring

Generate a notification whenever a password expiration warning is encountered for a user password for the first time.

password-reset

Generate a notification whenever a user's password is reset by an administrator.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are

invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Error Log Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.ErrorLogAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

SMTP Account Status Notification Handler

Account Status Notification Handlers of type smtp-account-status-notification-handler have the following properties:

email-address-attribute-type

Description

Specifies which attribute in the user's entries may be used to obtain the email address when notifying the end user. You can specify more than one email address as separate values. In this case, the OpenDJ server sends a notification to all email addresses identified.

Default Value

If no email address attribute types are specified, then no attempt is made to send email notification messages to end users. Only those users specified in the set of additional recipient addresses are sent the notification messages.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.SMTPAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this account status notification handler. The values for this property should begin with the name of an account status notification type followed by a colon and the subject that should be used for the associated notification message. If an email message is generated for an account status notification type for which no subject is defined, then that message is given a generic subject.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-template-file

Description

Specifies the path to the file containing the message template to generate the email notification messages. The values for this property should begin with the name of an account status notification type followed by a colon and the path to the template file that should be used for that notification type. If an account status notification has a notification type that is not associated with a message template file, then no email message is generated for that notification.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which notification messages are sent, either instead of or in addition to the end user for whom the notification has been generated. This may be used to ensure that server administrators also receive a copy of any notification messages that are generated.

Default Value

If no additional recipient addresses are specified, then only the end users that are the subjects of the account status notifications receive the notification messages.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

send-email-as-html

Description

Indicates whether an email notification message should be sent as HTML. If this value is true, email notification messages are marked as text/html. Otherwise outgoing email messages are assumed to be plaintext and marked as text/plain.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-message-without-end-user-address

Description

Indicates whether an email notification message should be generated and sent to the set of notification recipients even if the user entry does not contain any values for any of the email address attributes (that is, in cases when it is not be possible to notify the end user). This is only applicable if both one or more email address attribute types and one or more additional recipient addresses are specified.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

sender-address

Description

Specifies the email address from which the message is sent. Note that this does not necessarily have to be a legitimate email address.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-alert-handler(1)

Name

dsconfig delete-alert-handler - Deletes Alert Handlers

Synopsis

`dsconfig delete-alert-handler` {options}

Description

Deletes Alert Handlers.

Options

The `dsconfig delete-alert-handler` command takes the following options:

`--handler-name {name}`

The name of the Alert Handler.

Alert Handler properties depend on the Alert Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

`jmx-alert-handler`

Default {name}: JMX Alert Handler

Enabled by default: true

See JMX Alert Handler for the properties of this Alert Handler type.

`smtp-alert-handler`

Default {name}: SMTP Alert Handler

Enabled by default: true

See SMTP Alert Handler for the properties of this Alert Handler type.

`-f | --force`

Ignore non-existent Alert Handlers.

Alert Handler properties depend on the Alert Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

`jmx-alert-handler`

Default null: JMX Alert Handler

Enabled by default: true

See JMX Alert Handler for the properties of this Alert Handler type.

`smtp-alert-handler`

Default null: SMTP Alert Handler

Enabled by default: true

See SMTP Alert Handler for the properties of this Alert Handler type.

JMX Alert Handler

Alert Handlers of type jmx-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Alert Handler implementation.

Default Value

org.opends.server.extensions.JMXAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

SMTP Alert Handler

Alert Handlers of type smtp-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed.

Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Alert Handler implementation.

Default Value

org.opends.server.extensions.SMTPAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-body

Description

Specifies the body that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which the messages should be sent. Multiple values may be provided if there should be more than one recipient.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

sender-address

Description

Specifies the email address to use as the sender for messages generated by this alert handler.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-backend(1)

Name

dsconfig delete-backend - Deletes Backends

Synopsis

`dsconfig delete-backend` {options}

Description

Deletes Backends.

Options

The `dsconfig delete-backend` command takes the following options:

`--backend-name {name}`
: The name of the Backend.

  Backend properties depend on the Backend type, which depends on the {name} you provide.

  By default, OpenDJ directory server supports the following Backend types:

  `backup-backend`
  : Default {name}: Backup Backend

    Enabled by default: true

    See Backup Backend for the properties of this Backend type.

  `cas-backend`
  : Default {name}: CAS Backend

    Enabled by default: true

    See CAS Backend for the properties of this Backend type.

  `jdbc-backend`
  : Default {name}: JDBC Backend

    Enabled by default: true

    See JDBC Backend for the properties of this Backend type.

  `je-backend`
  : Default {name}: JE Backend

Enabled by default: true

See JE Backend for the properties of this Backend type.

`ldif-backend`

Default {name}: LDIF Backend

Enabled by default: true

See LDIF Backend for the properties of this Backend type.

`memory-backend`

Default {name}: Memory Backend

Enabled by default: true

See Memory Backend for the properties of this Backend type.

`monitor-backend`

Default {name}: Monitor Backend

Enabled by default: true

See Monitor Backend for the properties of this Backend type.

`null-backend`

Default {name}: Null Backend

Enabled by default: true

See Null Backend for the properties of this Backend type.

`pdb-backend`

Default {name}: PDB Backend

Enabled by default: true

See PDB Backend for the properties of this Backend type.

`schema-backend`

Default {name}: Schema Backend

Enabled by default: true

See Schema Backend for the properties of this Backend type.

`task-backend`

Default {name}: Task Backend

Enabled by default: true

See Task Backend for the properties of this Backend type.

`trust-store-backend`

Default {name}: Trust Store Backend

Enabled by default: true

See Trust Store Backend for the properties of this Backend type.

`-f | --force`

Ignore non-existent Backends.

Backend properties depend on the Backend type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Backend types:

`backup-backend`

Default null: Backup Backend

Enabled by default: true

See Backup Backend for the properties of this Backend type.

`cas-backend`

Default null: CAS Backend

Enabled by default: true

See CAS Backend for the properties of this Backend type.

`jdbc-backend`

Default null: JDBC Backend

Enabled by default: true

See JDBC Backend for the properties of this Backend type.

`je-backend`

Default null: JE Backend

Enabled by default: true

See JE Backend for the properties of this Backend type.

`ldif-backend`

Default null: LDIF Backend

Enabled by default: true

See LDIF Backend for the properties of this Backend type.

`memory-backend`

Default null: Memory Backend

Enabled by default: true

See Memory Backend for the properties of this Backend type.

`monitor-backend`

Default null: Monitor Backend

Enabled by default: true

See Monitor Backend for the properties of this Backend type.

`null-backend`

Default null: Null Backend

Enabled by default: true

See Null Backend for the properties of this Backend type.

`pdb-backend`

Default null: PDB Backend

Enabled by default: true

See PDB Backend for the properties of this Backend type.

`schema-backend`

Default null: Schema Backend

Enabled by default: true

See Schema Backend for the properties of this Backend type.

`task-backend`

Default null: Task Backend

Enabled by default: true

See Task Backend for the properties of this Backend type.

`trust-store-backend`

Default null: Trust Store Backend

Enabled by default: true

See Trust Store Backend for the properties of this Backend type.

Backup Backend

Backends of type backup-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

backup-directory

Description

Specifies the path to a backup directory containing one or more backups for a particular backend. This is a multivalued property. Each value may specify a different backup directory if desired (one for each backend for which backups are taken). Values may be either absolute paths or paths that are relative to the base of the OpenDJ directory server installation.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.BackupBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

CAS Backend

Backends of type cas-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-directory

Description

Specifies the keyspace name The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

ldap_opendj

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.cassandra.Backend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

JDBC Backend

Backends of type jdbc-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-directory

Description

Specifies the connection string jdbc:postgresql://localhost/test

Default Value

jdbc:postgresql://localhost/test

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.jdbc.Backend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation,

and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

JE Backend

Backends of type je-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-bytes-interval

Description

Specifies the maximum number of bytes that may be written to the database before it is forced to perform a checkpoint. This can be used to bound the recovery time that may be required if the database environment is opened without having been properly closed. If this property is set to a non-zero value, the checkpointer wakeup interval is not used. To use time-based checkpointing, set this property to zero.

Default Value

500mb

Allowed Values

Upper value is 9223372036854775807.

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. Note that this is only used if the value of the checkpointer bytes interval is zero.

Default Value

30s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.Upper limit is 4294 seconds.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-cleaner-min-utilization

Description

Specifies the occupancy percentage for "live" data in this backend's database. When the amount of "live" data in the database drops below this value, cleaners will act to increase the occupancy percentage by compacting the database.

Default Value

50

Allowed Values

An integer value. Lower value is 0. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Berkeley DB Java Edition database files containing the data for this backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-core-threads

Description

Specifies the core number of threads in the eviction thread pool. Specifies the core number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

1

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-keep-alive

Description

The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

600s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.Upper limit is 86400 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-lru-only

Description

Indicates whether the database should evict existing data from the cache based on an LRU policy (where the least recently used information will be evicted first). If set to "false", then the eviction keeps internal nodes of the underlying Btree in the cache over leaf nodes, even if the leaf nodes have been accessed more recently. This may be a better configuration for databases in which only a very small portion of the data is cached.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-max-threads

Description

Specifies the maximum number of threads in the eviction thread pool. Specifies the maximum number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-nodes-per-scan

Description

Specifies the number of Btree nodes that should be evicted from the cache in a single pass if it is determined that it is necessary to free existing data in order to make room for new information. Changes to this property do not take effect until the backend is restarted. It is recommended that you also change this property when you set db-evictor-lru-only to false. This setting controls the number of Btree nodes that are considered, or sampled, each time a node is evicted. A setting of 10 often produces good results, but this may vary from application to application. The larger the nodes per scan, the more accurate the algorithm. However, don't set it too high. When considering larger numbers of nodes for each eviction, the evictor may delay the completion of a given database operation, which impacts the response time of the application thread. In JE 4.1 and later, setting this value too high in an application that is largely CPU bound can reduce the effectiveness of cache eviction. It's best to start with the default value, and increase it gradually to see if it is beneficial for your application.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 1000.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-file-max

Description

Specifies the maximum size for a database log file.

Default Value

100mb

Allowed Values

Lower value is 1000000.Upper value is 4294967296.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-filecache-size

Description

Specifies the size of the file handle cache. The file handle cache is used to keep as much opened log files as possible. When the cache is smaller than the number of logs, the database needs to close some handles and open log files it needs, resulting in less optimal performances. Ideally, the size of the cache should be higher than the number of files contained in the database. Make sure the OS number of open files per process is also tuned appropriately.

Default Value

100

Allowed Values

An integer value. Lower value is 3. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-file-handler-on

Description

Indicates whether the database should maintain a je.info file in the same directory as the database log directory. This file contains information about the internal processing performed by the underlying database.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-level

Description

Specifies the log level that should be used by the database when it is writing information into the je.info file. The database trace logging level is (in increasing order of verbosity) chosen from: OFF, SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST, ALL.

Default Value

CONFIG

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-cleaner-threads

Description

Specifies the number of threads that the backend should maintain to keep the database log files at or near the desired utilization. In environments with high write throughput, multiple cleaner threads may be required to maintain the desired utilization.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-lock-tables

Description

Specifies the number of lock tables that are used by the underlying database. This can be particularly important to help improve scalability by avoiding contention on systems with large numbers of CPUs. The value of this configuration property should be set to a prime number that is less than or equal to the number of worker threads configured for use in the server.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 32767.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-run-cleaner

Description

Indicates whether the cleaner threads should be enabled to compact the database. The cleaner threads are used to periodically compact the database when it reaches a percentage of occupancy lower than the amount specified by the db-cleaner-min-utilization property. They identify database files with a low percentage of live data, and relocate their remaining live data to the end of the log.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-write-no-sync

Description

Indicates whether the database should synchronously flush data as it is written to disk. If this value is set to "false", then all data written to disk is synchronously flushed to persistent storage and thereby providing full durability. If it is set to "true", then data may be cached for a period of time by the underlying operating system before actually being written to disk. This may improve performance, but could cause the most recent changes to be lost in the event of an underlying OS or hardware failure (but not in the case that the OpenDJ directory server or the JVM exits abnormally).

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.jeb.JEBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

je-property

Description

Specifies the database and environment properties for the Berkeley DB Java Edition database serving the data for this backend. Any Berkeley DB Java Edition property can be specified using the following form: property-name=property-value. Refer to OpenDJ documentation for further information on related properties, their implications, and range values. The definitive identification of all the property parameters is available in the example.properties file of Berkeley DB Java Edition distribution.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation,

and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

LDIF Backend

Backends of type ldif-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

is-private-backend

Description

Indicates whether the backend should be considered a private backend, which indicates that it is used for storing operational data rather than user-defined information.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.LDIFBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-file

Description

Specifies the path to the LDIF file containing the data for this backend.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Memory Backend

Backends of type memory-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MemoryBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Monitor Backend

Backends of type monitor-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MonitorBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Null Backend

Backends of type null-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.NullBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

PDB Backend

Backends of type pdb-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be

responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. This setting controls the elapsed time between attempts to write a checkpoint to the journal. A longer interval allows more updates to accumulate in buffers before they are required to be written to disk, but also potentially causes recovery from an abrupt termination (crash) to take more time.

Default Value

15s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 10 seconds.Upper limit is 3600 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Persistit database files containing the data for this backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.pdb.PDBBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be

more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Schema Backend

Backends of type schema-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be

responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.SchemaBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

schema-entry-dn

Description

Defines the base DNs of the subtrees in which the schema information is published in addition to the value included in the base-dn property. The value provided in the base-dn property is the only one that appears in the subschemaSubentry operational attribute of the server's root DSE (which is necessary because that is a single-valued attribute) and as a virtual attribute in other entries. The schema-entry-dn attribute may be used to make the schema information available in other locations to accommodate certain client applications that have been hard-coded to expect the schema to reside in a specific location.

Default Value

cn=schema

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

show-all-attributes

Description

Indicates whether to treat all attributes in the schema entry as if they were user attributes regardless of their configuration. This may provide compatibility with some applications that expect schema attributes like attributeTypes and objectClasses to be included by default even if they are not requested. Note that the ldapSyntaxes attribute is always treated as operational in order to avoid problems with attempts to modify the schema over protocol.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Task Backend

Backends of type task-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.task.TaskBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

notification-sender-address

Description

Specifies the email address to use as the sender (that is, the "From:" address) address for notification mail messages generated when a task completes execution.

Default Value

The default sender address used is "opendj-task-notification@" followed by the canonical address of the system on which the server is running.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

task-backing-file

Description

Specifies the path to the backing file for storing information about the tasks configured in the server. It may be either an absolute path or a relative path to the base of the OpenDJ directory server instance.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

task-retention-time

Description

Specifies the length of time that task entries should be retained after processing on the associated task has been completed.

Default Value

24 hours

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Trust Store Backend

Backends of type trust-store-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.TrustStoreBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file that stores the trust information. It may be an absolute path, or a path that is relative to the OpenDJ instance root.

Default Value

config/ads-truststore

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the

clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well.

Default Value

The JVM default value is used.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect the next time that the key manager is accessed.

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-backend-index(1)

Name

dsconfig delete-backend-index - Deletes Backend Indexes

Synopsis

`dsconfig delete-backend-index` {options}

Description

Deletes Backend Indexes.

Options

The `dsconfig delete-backend-index` command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend Index properties depend on the Backend Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default {name}: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

`--index-name {name}`

The name of the Backend Index.

Backend Index properties depend on the Backend Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default {name}: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

`-f | --force`

Ignore non-existent Backend Indexes.

Backend Index properties depend on the Backend Index type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default null: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

Backend Index

Backend Indexes of type backend-index have the following properties:

attribute

Description

Specifies the name of the attribute for which the index is to be maintained.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

confidentiality-enabled

Description

Specifies whether contents of the index should be confidential. Setting the flag to true will hash

keys for equality type indexes using SHA-1 and encrypt the list of entries matching a substring key for substring indexes.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

If the index for the attribute must be protected for security purposes and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate. The property cannot be set on a backend for which confidentiality is not enabled.

Advanced Property

No

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that are allowed to match a given index key before that particular index key is no longer maintained. This is analogous to the ALL IDs threshold in the Sun Java System Directory Server. If this is specified, its value overrides the JE backend-wide configuration. For no limit, use 0 for the value.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

If any index keys have already reached this limit, indexes must be rebuilt before they will be

allowed to use the new limit.

Advanced Property

No

Read-only

No

index-extensible-matching-rule

Description

The extensible matching rule in an extensible index. An extensible matching rule must be specified using either LOCALE or OID of the matching rule.

Default Value

No extensible matching rules will be indexed.

Allowed Values

A Locale or an OID.

Multi-valued

Yes

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

No

Read-only

No

index-type

Description

Specifies the type(s) of indexing that should be performed for the associated attribute. For equality, presence, and substring index types, the associated attribute type must have a corresponding matching rule.

Default Value

None

Allowed Values

approximate

This index type is used to improve the efficiency of searches using approximate matching search

filters.

equality

This index type is used to improve the efficiency of searches using equality search filters.

extensible

This index type is used to improve the efficiency of searches using extensible matching search filters.

ordering

This index type is used to improve the efficiency of searches using "greater than or equal to" or "less then or equal to" search filters.

presence

This index type is used to improve the efficiency of searches using the presence search filters.

substring

This index type is used to improve the efficiency of searches using substring search filters.

Multi-valued

Yes

Required

Yes

Admin Action Required

If any new index types are added for an attribute, and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate.

Advanced Property

No

Read-only

No

substring-length

Description

The length of substrings in a substring index.

Default Value

6

Allowed Values

An integer value. Lower value is 3.

Multi-valued

No

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-backend-vlv-index(1)

Name

dsconfig delete-backend-vlv-index - Deletes Backend VLV Indexes

Synopsis

`dsconfig delete-backend-vlv-index` {options}

Description

Deletes Backend VLV Indexes.

Options

The `dsconfig delete-backend-vlv-index` command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default {name}: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

`--index-name {name}`

The name of the Backend VLV Index.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default {name}: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

`-f | --force`

Ignore non-existent Backend VLV Indexes.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default null: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

Backend VLV Index

Backend VLV Indexes of type backend-vlv-index have the following properties:

base-dn

Description

Specifies the base DN used in the search query that is being indexed.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

filter

Description

Specifies the LDAP filter used in the query that is being indexed.

Default Value

None

Allowed Values

A valid LDAP search filter.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

name

Description

Specifies a unique name for this VLV index.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

NoneThe VLV index name cannot be altered after the index is created.

Advanced Property

No

Read-only

Yes

scope

Description

Specifies the LDAP scope of the query that is being indexed.

Default Value

None

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

sort-order

Description

Specifies the names of the attributes that are used to sort the entries for the query being indexed. Multiple attributes can be used to determine the sort order by listing the attribute names from highest to lowest precedence. Optionally, + or - can be prefixed to the attribute name to sort the attribute in ascending order or descending order respectively.

Default Value

None

Allowed Values

Valid attribute types defined in the schema, separated by a space and optionally prefixed by + or

-.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

dsconfig delete-certificate-mapper(1)

Name

dsconfig delete-certificate-mapper - Deletes Certificate Mappers

Synopsis

`dsconfig delete-certificate-mapper` {options}

Description

Deletes Certificate Mappers.

Options

The `dsconfig delete-certificate-mapper` command takes the following options:

`--mapper-name {name}`

The name of the Certificate Mapper.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

`fingerprint-certificate-mapper`

Default {name}: Fingerprint Certificate Mapper

Enabled by default: true

See Fingerprint Certificate Mapper for the properties of this Certificate Mapper type.

`subject-attribute-to-user-attribute-certificate-mapper`

Default {name}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See Subject Attribute To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-dn-to-user-attribute-certificate-mapper`

Default {name}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See Subject DN To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-equals-dn-certificate-mapper`

Default {name}: Subject Equals DN Certificate Mapper

Enabled by default: true

See Subject Equals DN Certificate Mapper for the properties of this Certificate Mapper type.

`-f | --force`

Ignore non-existent Certificate Mappers.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

`fingerprint-certificate-mapper`

Default null: Fingerprint Certificate Mapper

Enabled by default: true

See Fingerprint Certificate Mapper for the properties of this Certificate Mapper type.

`subject-attribute-to-user-attribute-certificate-mapper`

Default null: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See Subject Attribute To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-dn-to-user-attribute-certificate-mapper`

Default null: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See Subject DN To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-equals-dn-certificate-mapper`

Default null: Subject Equals DN Certificate Mapper

Enabled by default: true

See Subject Equals DN Certificate Mapper for the properties of this Certificate Mapper type.

Fingerprint Certificate Mapper

Certificate Mappers of type fingerprint-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-algorithm

Description

Specifies the name of the digest algorithm to compute the fingerprint of client certificates.

Default Value

None

Allowed Values

md5

Use the MD5 digest algorithm to compute certificate fingerprints.

sha1

Use the SHA-1 digest algorithm to compute certificate fingerprints.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-attribute

Description

Specifies the attribute in which to look for the fingerprint. Values of the fingerprint attribute should exactly match the MD5 or SHA1 representation of the certificate fingerprint.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fingerprint Certificate Mapper implementation.

Default Value

org.opends.server.extensions.FingerprintCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs are used when performing searches to map the client certificates to a user entry.

Default Value

The server performs the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subject Attribute To User Attribute Certificate Mapper

Certificate Mappers of type subject-attribute-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Attribute To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectAttributeToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute-mapping

Description

Specifies a mapping between certificate attributes and user attributes. Each value should be in the form "certattr:userattr" where certattr is the name of the attribute in the certificate subject and userattr is the name of the corresponding attribute in user entries. There may be multiple mappings defined, and when performing the mapping values for all attributes present in the certificate subject that have mappings defined must be present in the corresponding user entries.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subject DN To User Attribute Certificate Mapper

Certificate Mappers of type subject-dn-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject DN To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectDNToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute

Description

Specifies the name or OID of the attribute whose value should exactly match the certificate subject DN.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subject Equals DN Certificate Mapper

Certificate Mappers of type subject-equals-dn-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Equals DN Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectEqualsDNCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-connection-handler(1)

Name

dsconfig delete-connection-handler - Deletes Connection Handlers

Synopsis

`dsconfig delete-connection-handler` {options}

Description

Deletes Connection Handlers.

Options

The `dsconfig delete-connection-handler` command takes the following options:

`--handler-name {name}`

The name of the Connection Handler.

Connection Handler properties depend on the Connection Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

`http-connection-handler`

Default {name}: HTTP Connection Handler

Enabled by default: true

See HTTP Connection Handler for the properties of this Connection Handler type.

`jmx-connection-handler`

Default {name}: JMX Connection Handler

Enabled by default: true

See JMX Connection Handler for the properties of this Connection Handler type.

`ldap-connection-handler`

Default {name}: LDAP Connection Handler

Enabled by default: true

See LDAP Connection Handler for the properties of this Connection Handler type.

`ldif-connection-handler`

Default {name}: LDIF Connection Handler

Enabled by default: true

See LDIF Connection Handler for the properties of this Connection Handler type.

`snmp-connection-handler`

Default {name}: SNMP Connection Handler

Enabled by default: true

See SNMP Connection Handler for the properties of this Connection Handler type.

`-f | --force`

Ignore non-existent Connection Handlers.

Connection Handler properties depend on the Connection Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

`http-connection-handler`

Default null: HTTP Connection Handler

Enabled by default: true

See HTTP Connection Handler for the properties of this Connection Handler type.

`jmx-connection-handler`

Default null: JMX Connection Handler

Enabled by default: true

See JMX Connection Handler for the properties of this Connection Handler type.

`ldap-connection-handler`

Default null: LDAP Connection Handler

Enabled by default: true

See LDAP Connection Handler for the properties of this Connection Handler type.

`ldif-connection-handler`

Default null: LDIF Connection Handler

Enabled by default: true

See LDIF Connection Handler for the properties of this Connection Handler type.

`snmp-connection-handler`

Default null: SNMP Connection Handler

Enabled by default: true

See SNMP Connection Handler for the properties of this Connection Handler type.

HTTP Connection Handler

Connection Handlers of type http-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the HTTP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of

socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that

may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the HTTP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer HTTP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Connection Handler implementation.

Default Value

org.opends.server.protocols.http.HTTPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the HTTP Connection Handler should keep statistics. If enabled, the HTTP Connection Handler maintains statistics about the number and types of operations requested over HTTP and the amount of data sent and received.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this HTTP Connection Handler should listen for connections from HTTP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the HTTP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the HTTP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to HTTP clients should be

allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-concurrent-ops-per-connection

Description

Specifies the maximum number of internal operations that each HTTP client connection can execute concurrently. This property allow to limit the impact that each HTTP request can have on the whole server by limiting the number of internal operations that each HTTP request can execute concurrently. A value of 0 means that no limit is enforced.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest HTTP request message that will be allowed by the HTTP Connection Handler. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The HTTP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the HTTP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the HTTP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the HTTP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the HTTP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the HTTP Connection Handler should use SSL. If enabled, the HTTP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the HTTP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the HTTP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides

better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

JMX Connection Handler

Connection Handlers of type jmx-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Connection Handler implementation.

Default Value

org.opends.server.protocols.jmx.JmxConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this JMX Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the JMX Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address on which this JMX Connection Handler should listen for connections from JMX clients. If no value is provided, then the JMX Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the JMX Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

rmi-port

Description

Specifies the port number on which the JMX RMI service will listen for connections from clients. A value of 0 indicates the service to choose a port of its own. If the value provided is different than 0, the value will be used as the RMI port. Otherwise, the RMI service will choose a port of its own.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the JMX Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the JMX Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the JMX Connection Handler should use SSL. If enabled, the JMX Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

LDAP Connection Handler

Connection Handlers of type ldap-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-ldap-v2

Description

Indicates whether connections from LDAPv2 clients are allowed. If LDAPv2 clients are allowed, then only a minimal degree of special support are provided for them to ensure that LDAPv3-specific protocol elements (for example, Configuration Guide 25 controls, extended response messages, intermediate response messages, referrals) are not sent to an LDAPv2 client.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-start-tls

Description

Indicates whether clients are allowed to use StartTLS. If enabled, the LDAP Connection Handler allows clients to use the StartTLS extended operation to initiate secure communication over an otherwise insecure channel. Note that this is only allowed if the LDAP Connection Handler is not configured to use SSL, and if the server is configured with a valid key manager provider and a valid trust manager provider.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the LDAP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the LDAP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer LDAP

response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that

may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDAP Connection Handler implementation.

Default Value

org.opends.server.protocols.ldap.LDAPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the LDAP Connection Handler should keep statistics. If enabled, the LDAP Connection Handler maintains statistics about the number and types of operations requested over LDAP and the amount of data sent and received.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this LDAP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this LDAP Connection Handler should listen for connections from LDAP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the LDAP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the LDAP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to LDAP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest LDAP request message that will be allowed by this LDAP Connection handler. This property is analogous to the maxBERSize configuration attribute of the Sun Java System Directory Server. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The LDAP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new

requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-rejection-notice

Description

Indicates whether the LDAP Connection Handler should send a notice of disconnection extended response message to the client if a new connection is rejected for some reason. The extended response message may provide an explanation indicating the reason that the connection was rejected.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the LDAP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the LDAP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the LDAP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the LDAP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled

when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Connection Handler should use SSL. If enabled, the LDAP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the LDAP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the LDAP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

LDIF Connection Handler

Connection Handlers of type ldif-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDIF Connection Handler implementation.

Default Value

org.opends.server.protocols.LDIFConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-directory

Description

Specifies the path to the directory in which the LDIF files should be placed.

Default Value

config/auto-process-ldif

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

poll-interval

Description

Specifies how frequently the LDIF connection handler should check the LDIF directory to determine whether a new LDIF file has been added.

Default Value

5 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

SNMP Connection Handler

Connection Handlers of type snmp-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

allowed-manager

Description

Specifies the hosts of the managers to be granted the access rights. This property is required for SNMP v1 and v2 security configuration. An asterisk (*) opens access to all managers.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take

effect

Advanced Property

No

Read-only

No

allowed-user

Description

Specifies the users to be granted the access rights. This property is required for SNMP v3 security configuration. An asterisk (*) opens access to all users.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

community

Description

Specifies the v1,v2 community or the v3 context name allowed to access the MIB 2605 monitoring information or the USM MIB. The mapping between "community" and "context name" is set.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SNMP Connection Handler implementation.

Default Value

org.opends.server.snmp.SNMPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this SNMP Connection Handler should listen for connections from SNMP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the SNMP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

Yes

listen-port

Description

Specifies the port number on which the SNMP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

opendmk-jarfile

Description

Indicates the OpenDMK runtime jar file location

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

registered-mbean

Description

Indicates whether the SNMP objects have to be registered in the directory server MBeanServer or not allowing to access SNMP Objects with RMI connector if enabled.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-agent-file

Description

Specifies the USM security configuration to receive authenticated only SNMP requests.

Default Value

config/snmp/security/opendj-snmp.security

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-level

Description

Specifies the type of security level : NoAuthNoPriv : No security mechanisms activated, AuthNoPriv : Authentication activated with no privacy, AuthPriv : Authentication with privacy activated. This property is required for SNMP V3 security configuration.

Default Value

authnopriv

Allowed Values

authnopriv

Authentication activated with no privacy.

authpriv

Authentication with privacy activated.

noauthnopriv

No security mechanisms activated.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trap-port

Description

Specifies the port to use to send SNMP Traps.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-community

Description

Specifies the community string that must be included in the traps sent to define managers (trap-destinations). This property is used in the context of SNMP v1, v2 and v3.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-destination

Description

Specifies the hosts to which V1 traps will be sent. V1 Traps are sent to every host listed. If this list

is empty, V1 traps are sent to "localhost". Each host in the list must be identifed by its name or complete IP Addess.

Default Value

If the list is empty, V1 traps are sent to "localhost".

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig delete-debug-target(1)

Name

dsconfig delete-debug-target - Deletes Debug Targets

Synopsis

`dsconfig delete-debug-target` {options}

Description

Deletes Debug Targets.

Options

The `dsconfig delete-debug-target` command takes the following options:

`--publisher-name {name}`

The name of the Debug Log Publisher.

Debug Target properties depend on the Debug Target type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default {name}: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

`--target-name {name}`

The name of the Debug Target.

Debug Target properties depend on the Debug Target type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default {name}: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

`-f | --force`

Ignore non-existent Debug Targets.

Debug Target properties depend on the Debug Target type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default null: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

Debug Target

Debug Targets of type debug-target have the following properties:

debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

debug-scope

Description

Specifies the fully-qualified OpenDJ Java package, class, or method affected by the settings in this

target definition. Use the number character (#) to separate the class name and the method name (that is, org.opends.server.core.DirectoryServer#startUp).

Default Value

None

Allowed Values

The fully-qualified OpenDJ Java package, class, or method name.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the Debug Target is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

include-throwable-cause

Description

Specifies the property to indicate whether to include the cause of exceptions in exception thrown and caught messages.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-entry-arguments

Description

Specifies the property to indicate whether to include method arguments in debug messages.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-return-value

Description

Specifies the property to indicate whether to include the return value in debug messages.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

throwable-stack-frames

Description

Specifies the property to indicate the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

0

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-entry-cache(1)

Name

dsconfig delete-entry-cache - Deletes Entry Caches

Synopsis

`dsconfig delete-entry-cache` {options}

Description

Deletes Entry Caches.

Options

The `dsconfig delete-entry-cache` command takes the following options:

`--cache-name {name}`

The name of the Entry Cache.

Entry Cache properties depend on the Entry Cache type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

`fifo-entry-cache`

Default {name}: FIFO Entry Cache

Enabled by default: true

See FIFO Entry Cache for the properties of this Entry Cache type.

`soft-reference-entry-cache`

Default {name}: Soft Reference Entry Cache

Enabled by default: true

See Soft Reference Entry Cache for the properties of this Entry Cache type.

`-f | --force`

Ignore non-existent Entry Caches.

Entry Cache properties depend on the Entry Cache type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

`fifo-entry-cache`

Default null: FIFO Entry Cache

Enabled by default: true

See FIFO Entry Cache for the properties of this Entry Cache type.

`soft-reference-entry-cache`

Default null: Soft Reference Entry Cache

Enabled by default: true

See Soft Reference Entry Cache for the properties of this Entry Cache type.

FIFO Entry Cache

Entry Caches of type fifo-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the FIFO Entry Cache implementation.

Default Value

org.opends.server.extensions.FIFOEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time to wait while attempting to acquire a read or write lock.

Default Value

2000.0ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-entries

Description

Specifies the maximum number of entries that we will allow in the cache.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-memory-percent

Description

Specifies the maximum percentage of JVM memory used by the server before the entry caches stops caching and begins purging itself. Very low settings such as 10 or 20 (percent) can prevent this entry cache from having enough space to hold any of the entries to cache, making it appear that the server is ignoring or skipping the entry cache entirely.

Default Value

90

Allowed Values

An integer value. Lower value is 1. Upper value is 100.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Soft Reference Entry Cache

Entry Caches of type soft-reference-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Soft Reference Entry Cache implementation.

Default Value

org.opends.server.extensions.SoftReferenceEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time in milliseconds to wait while attempting to acquire a read or write lock.

Default Value

3000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-extended-operation-handler(1)

Name

dsconfig delete-extended-operation-handler - Deletes Extended Operation Handlers

Synopsis

`dsconfig delete-extended-operation-handler` {options}

Description

Deletes Extended Operation Handlers.

Options

The `dsconfig delete-extended-operation-handler` command takes the following options:

`--handler-name {name}`

The name of the Extended Operation Handler.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

`cancel-extended-operation-handler`

Default {name}: Cancel Extended Operation Handler

Enabled by default: true

See Cancel Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-connection-id-extended-operation-handler`

Default {name}: Get Connection Id Extended Operation Handler

Enabled by default: true

See Get Connection Id Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-symmetric-key-extended-operation-handler`

Default {name}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See Get Symmetric Key Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-modify-extended-operation-handler`

Default {name}: Password Modify Extended Operation Handler

Enabled by default: true

See Password Modify Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-policy-state-extended-operation-handler`

Default {name}: Password Policy State Extended Operation Handler

Enabled by default: true

See Password Policy State Extended Operation Handler for the properties of this Extended Operation Handler type.

`start-tls-extended-operation-handler`

Default {name}: Start TLS Extended Operation Handler

Enabled by default: true

See Start TLS Extended Operation Handler for the properties of this Extended Operation Handler type.

`who-am-i-extended-operation-handler`

Default {name}: Who Am I Extended Operation Handler

Enabled by default: true

See Who Am I Extended Operation Handler for the properties of this Extended Operation Handler type.

`-f | --force`

Ignore non-existent Extended Operation Handlers.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

`cancel-extended-operation-handler`

Default null: Cancel Extended Operation Handler

Enabled by default: true

See Cancel Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-connection-id-extended-operation-handler`

Default null: Get Connection Id Extended Operation Handler

Enabled by default: true

See Get Connection Id Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-symmetric-key-extended-operation-handler`

Default null: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See Get Symmetric Key Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-modify-extended-operation-handler`

Default null: Password Modify Extended Operation Handler

Enabled by default: true

See Password Modify Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-policy-state-extended-operation-handler`

Default null: Password Policy State Extended Operation Handler

Enabled by default: true

See Password Policy State Extended Operation Handler for the properties of this Extended Operation Handler type.

`start-tls-extended-operation-handler`

Default null: Start TLS Extended Operation Handler

Enabled by default: true

See Start TLS Extended Operation Handler for the properties of this Extended Operation Handler type.

`who-am-i-extended-operation-handler`

Default null: Who Am I Extended Operation Handler

Enabled by default: true

See Who Am I Extended Operation Handler for the properties of this Extended Operation Handler type.

Cancel Extended Operation Handler

Extended Operation Handlers of type cancel-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Cancel Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.CancelExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Get Connection Id Extended Operation Handler

Extended Operation Handlers of type get-connection-id-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Connection Id Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.GetConnectionIDExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Get Symmetric Key Extended Operation Handler

Extended Operation Handlers of type get-symmetric-key-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Symmetric Key Extended Operation Handler implementation.

Default Value

org.opends.server.crypto.GetSymmetricKeyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Modify Extended Operation Handler

Extended Operation Handlers of type password-modify-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that should be used in conjunction with the password modify extended operation. This property is used to identify a user based on an authorization ID in the 'u:' form. Changes to this property take effect immediately.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Password Modify Extended Operation Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Modify Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordModifyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Policy State Extended Operation Handler

Extended Operation Handlers of type password-policy-state-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Policy State Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordPolicyStateExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Start TLS Extended Operation Handler

Extended Operation Handlers of type start-tls-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Start TLS Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.StartTLSExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Who Am I Extended Operation Handler

Extended Operation Handlers of type who-am-i-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Who Am I Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.WhoAmIExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-group-implementation(1)

Name

dsconfig delete-group-implementation - Deletes Group Implementations

Synopsis

`dsconfig delete-group-implementation` {options}

Description

Deletes Group Implementations.

Options

The `dsconfig delete-group-implementation` command takes the following options:

`--implementation-name {name}`

The name of the Group Implementation.

Group Implementation properties depend on the Group Implementation type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

`dynamic-group-implementation`

Default {name}: Dynamic Group Implementation

Enabled by default: true

See Dynamic Group Implementation for the properties of this Group Implementation type.

`static-group-implementation`

Default {name}: Static Group Implementation

Enabled by default: true

See Static Group Implementation for the properties of this Group Implementation type.

`virtual-static-group-implementation`

Default {name}: Virtual Static Group Implementation

Enabled by default: true

See Virtual Static Group Implementation for the properties of this Group Implementation type.

`-f | --force`

Ignore non-existent Group Implementations.

Group Implementation properties depend on the Group Implementation type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

`dynamic-group-implementation`

Default null: Dynamic Group Implementation

Enabled by default: true

See Dynamic Group Implementation for the properties of this Group Implementation type.

`static-group-implementation`

Default null: Static Group Implementation

Enabled by default: true

See Static Group Implementation for the properties of this Group Implementation type.

`virtual-static-group-implementation`

Default null: Virtual Static Group Implementation

Enabled by default: true

See Virtual Static Group Implementation for the properties of this Group Implementation type.

Dynamic Group Implementation

Group Implementations of type dynamic-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Dynamic Group Implementation implementation.

Default Value

org.opends.server.extensions.DynamicGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Static Group Implementation

Group Implementations of type static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Group Implementation implementation.

Default Value

org.opends.server.extensions.StaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Virtual Static Group Implementation

Group Implementations of type virtual-static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Virtual Static Group Implementation implementation.

Default Value

org.opends.server.extensions.VirtualStaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-http-authorization-mechanism(1)

Name

dsconfig delete-http-authorization-mechanism - Deletes HTTP Authorization Mechanisms

Synopsis

`dsconfig delete-http-authorization-mechanism` {options}

Description

Deletes HTTP Authorization Mechanisms.

Options

The `dsconfig delete-http-authorization-mechanism` command takes the following options:

`--mechanism-name {name}`

The name of the HTTP Authorization Mechanism.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

`http-anonymous-authorization-mechanism`

Default {name}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See HTTP Anonymous Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-basic-authorization-mechanism`

Default {name}: HTTP Basic Authorization Mechanism

Enabled by default: true

See HTTP Basic Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-cts-authorization-mechanism`

Default {name}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Cts Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-file-authorization-mechanism`

Default {name}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 File Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-openam-authorization-mechanism`

Default {name}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Openam Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-token-introspection-authorization-mechanism`

Default {name}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Token Introspection Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`-f | --force`

Ignore non-existent HTTP Authorization Mechanisms.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the null you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

`http-anonymous-authorization-mechanism`

Default null: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See HTTP Anonymous Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-basic-authorization-mechanism`

Default null: HTTP Basic Authorization Mechanism

Enabled by default: true

See HTTP Basic Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-cts-authorization-mechanism`

Default null: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Cts Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-file-authorization-mechanism`

Default null: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 File Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-openam-authorization-mechanism`

Default null: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Openam Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-token-introspection-authorization-mechanism`

Default null: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Token Introspection Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

HTTP Anonymous Authorization Mechanism

HTTP Authorization Mechanisms of type http-anonymous-authorization-mechanism have the following properties:

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Anonymous Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpAnonymousAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-dn

Description

The authorization DN which will be used for performing anonymous operations.

Default Value

By default, operations will be performed using an anonymously bound connection.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

HTTP Basic Authorization Mechanism

HTTP Authorization Mechanisms of type http-basic-authorization-mechanism have the following properties:

alt-authentication-enabled

Description

Specifies whether user credentials may be provided using alternative headers to the standard 'Authorize' header.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-password-header

Description

Alternate HTTP headers to get the user's password from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-username-header

Description

Alternate HTTP headers to get the user's name from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper used to get the user's entry corresponding to the user-id provided in the HTTP authentication header.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Basic Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Basic Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpBasicAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

HTTP Oauth2 Cts Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-cts-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

The base DN of the Core Token Service where access token are stored. (example: ou=famrecords,ou=openam-session,ou=tokens,dc=example,dc=com)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Cts Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2CtsAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

HTTP Oauth2 File Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-file-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-directory

Description

Directory containing token files. File names must be equal to the token strings. The file content must a JSON object with the following attributes: 'scope', 'expireTime' and all the field(s) needed to resolve the authzIdTemplate.

Default Value

oauth2-demo/

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 File Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2FileAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

HTTP Oauth2 Openam Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-openam-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Openam Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2OpenAmAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Openam Authorization Mechanism .

Default Value

By default the system key manager(s) will be used.

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-info-url

Description

Defines the OpenAM endpoint URL where the access-token resolution request should be sent.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

HTTP Oauth2 Token Introspection Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-token-introspection-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-id

Description

Client's ID to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-secret

Description

Client's secret to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Token Introspection Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2TokenIntrospectionAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Token Introspection Authorization Mechanism .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-introspection-url

Description

Defines the token introspection endpoint URL where the access-token resolution request should be sent. (example: http://example.com/introspect)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

dsconfig delete-http-endpoint(1)

Name

dsconfig delete-http-endpoint - Deletes HTTP Endpoints

Synopsis

`dsconfig delete-http-endpoint` {options}

Description

Deletes HTTP Endpoints.

Options

The `dsconfig delete-http-endpoint` command takes the following options:

`--endpoint-name {name}`

The name of the HTTP Endpoint.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

`admin-endpoint`

Default {name}: Admin Endpoint

Enabled by default: true

See Admin Endpoint for the properties of this HTTP Endpoint type.

`rest2ldap-endpoint`

Default {name}: Rest2ldap Endpoint

Enabled by default: true

See Rest2ldap Endpoint for the properties of this HTTP Endpoint type.

`-f | --force`

Ignore non-existent HTTP Endpoints.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the null you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

`admin-endpoint`

Default null: Admin Endpoint

Enabled by default: true

See Admin Endpoint for the properties of this HTTP Endpoint type.

`rest2ldap-endpoint`

Default null: Rest2ldap Endpoint

Enabled by default: true

See Rest2ldap Endpoint for the properties of this HTTP Endpoint type.

Admin Endpoint

HTTP Endpoints of type admin-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP

endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Admin Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.AdminEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Rest2ldap Endpoint

HTTP Endpoints of type rest2ldap-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

config-directory

Description

The directory containing the Rest2Ldap configuration file(s) for this specific endpoint. The directory must be readable by the server and may contain multiple configuration files, one for each supported version of the REST endpoint. If a relative path is used then it will be resolved against the server's instance directory.

Default Value

None

Allowed Values

A directory that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Rest2ldap Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.Rest2LdapEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-identity-mapper(1)

Name

dsconfig delete-identity-mapper - Deletes Identity Mappers

Synopsis

`dsconfig delete-identity-mapper` {options}

Description

Deletes Identity Mappers.

Options

The `dsconfig delete-identity-mapper` command takes the following options:

`--mapper-name {name}`

The name of the Identity Mapper.

Identity Mapper properties depend on the Identity Mapper type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

`exact-match-identity-mapper`

Default {name}: Exact Match Identity Mapper

Enabled by default: true

See Exact Match Identity Mapper for the properties of this Identity Mapper type.

`regular-expression-identity-mapper`

Default {name}: Regular Expression Identity Mapper

Enabled by default: true

See Regular Expression Identity Mapper for the properties of this Identity Mapper type.

`-f | --force`

Ignore non-existent Identity Mappers.

Identity Mapper properties depend on the Identity Mapper type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

`exact-match-identity-mapper`

Default null: Exact Match Identity Mapper

Enabled by default: true

See Exact Match Identity Mapper for the properties of this Identity Mapper type.

`regular-expression-identity-mapper`

Default null: Regular Expression Identity Mapper

Enabled by default: true

See Regular Expression Identity Mapper for the properties of this Identity Mapper type.

Exact Match Identity Mapper

Identity Mappers of type exact-match-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Exact Match Identity Mapper implementation.

Default Value

org.opends.server.extensions.ExactMatchIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the attribute whose value should exactly match the ID string provided to this identity mapper. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry. The internal search performed includes a logical OR across all of these values.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs will be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Regular Expression Identity Mapper

Identity Mappers of type regular-expression-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Regular Expression Identity Mapper implementation.

Default Value

org.opends.server.extensions.RegularExpressionIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name or OID of the attribute whose value should match the provided identifier string after it has been processed by the associated regular expression. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the base DN(s) that should be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all the specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

match-pattern

Description

Specifies the regular expression pattern that is used to identify portions of the ID string that will be replaced. Any portion of the ID string that matches this pattern is replaced in accordance with the provided replace pattern (or is removed if no replace pattern is specified). If multiple substrings within the given ID string match this pattern, all occurrences are replaced. If no part of the given ID string matches this pattern, the ID string is not altered. Exactly one match pattern value must be provided, and it must be a valid regular expression as described in the API documentation for the java.util.regex.Pattern class, including support for capturing groups.

Default Value

None

Allowed Values

Any valid regular expression pattern which is supported by the javax.util.regex.Pattern class (see http://download.oracle.com/docs/cd/E17409_01/javase/6/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 6).

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replace-pattern

Description

Specifies the replacement pattern that should be used for substrings in the ID string that match the provided regular expression pattern. If no replacement pattern is provided, then any matching portions of the ID string will be removed (i.e., replaced with an empty string). The replacement pattern may include a string from a capturing group by using a dollar sign ($) followed by an integer value that indicates which capturing group should be used.

Default Value

The replace pattern will be the empty string.

Allowed Values

Any valid replacement string that is allowed by the javax.util.regex.Matcher class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-key-manager-provider(1)

Name

dsconfig delete-key-manager-provider - Deletes Key Manager Providers

Synopsis

`dsconfig delete-key-manager-provider` {options}

Description

Deletes Key Manager Providers.

Options

The `dsconfig delete-key-manager-provider` command takes the following options:

`--provider-name {name}`

The name of the Key Manager Provider.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

`file-based-key-manager-provider`

Default {name}: File Based Key Manager Provider

Enabled by default: true

See File Based Key Manager Provider for the properties of this Key Manager Provider type.

`ldap-key-manager-provider`

Default {name}: LDAP Key Manager Provider

Enabled by default: true

See LDAP Key Manager Provider for the properties of this Key Manager Provider type.

`pkcs11-key-manager-provider`

Default {name}: PKCS11 Key Manager Provider

Enabled by default: true

See PKCS11 Key Manager Provider for the properties of this Key Manager Provider type.

`-f | --force`

Ignore non-existent Key Manager Providers.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

`file-based-key-manager-provider`

Default null: File Based Key Manager Provider

Enabled by default: true

See File Based Key Manager Provider for the properties of this Key Manager Provider type.

`ldap-key-manager-provider`

Default null: LDAP Key Manager Provider

Enabled by default: true

See LDAP Key Manager Provider for the properties of this Key Manager Provider type.

`pkcs11-key-manager-provider`

Default null: PKCS11 Key Manager Provider

Enabled by default: true

See PKCS11 Key Manager Provider for the properties of this Key Manager Provider type.

File Based Key Manager Provider

Key Manager Providers of type file-based-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Key Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well. If no value is provided, the JVM-default value is used. Changes to this configuration attribute will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

LDAP Key Manager Provider

Key Manager Providers of type ldap-key-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Key Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

PKCS11 Key Manager Provider

Key Manager Providers of type pkcs11-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Key Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11KeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig delete-log-publisher(1)

Name

dsconfig delete-log-publisher - Deletes Log Publishers

Synopsis

`dsconfig delete-log-publisher` {options}

Description

Deletes Log Publishers.

Options

The `dsconfig delete-log-publisher` command takes the following options:

`--publisher-name {name}`

The name of the Log Publisher.

Log Publisher properties depend on the Log Publisher type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

`csv-file-access-log-publisher`

Default {name}: Csv File Access Log Publisher

Enabled by default: true

See Csv File Access Log Publisher for the properties of this Log Publisher type.

`csv-file-http-access-log-publisher`

Default {name}: Csv File HTTP Access Log Publisher

Enabled by default: true

See Csv File HTTP Access Log Publisher for the properties of this Log Publisher type.

`external-access-log-publisher`

Default {name}: External Access Log Publisher

Enabled by default: true

See External Access Log Publisher for the properties of this Log Publisher type.

`external-http-access-log-publisher`

Default {name}: External HTTP Access Log Publisher

Enabled by default: true

See External HTTP Access Log Publisher for the properties of this Log Publisher type.

`file-based-access-log-publisher`

Default {name}: File Based Access Log Publisher

Enabled by default: true

See File Based Access Log Publisher for the properties of this Log Publisher type.

`file-based-audit-log-publisher`

Default {name}: File Based Audit Log Publisher

Enabled by default: true

See File Based Audit Log Publisher for the properties of this Log Publisher type.

`file-based-debug-log-publisher`

Default {name}: File Based Debug Log Publisher

Enabled by default: true

See File Based Debug Log Publisher for the properties of this Log Publisher type.

`file-based-error-log-publisher`

Default {name}: File Based Error Log Publisher

Enabled by default: true

See File Based Error Log Publisher for the properties of this Log Publisher type.

`file-based-http-access-log-publisher`

Default {name}: File Based HTTP Access Log Publisher

Enabled by default: true

See File Based HTTP Access Log Publisher for the properties of this Log Publisher type.

`json-file-access-log-publisher`

Default {name}: Json File Access Log Publisher

Enabled by default: true

See Json File Access Log Publisher for the properties of this Log Publisher type.

`json-file-http-access-log-publisher`

Default {name}: Json File HTTP Access Log Publisher

Enabled by default: true

See Json File HTTP Access Log Publisher for the properties of this Log Publisher type.

`-f | --force`

Ignore non-existent Log Publishers.

Log Publisher properties depend on the Log Publisher type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

`csv-file-access-log-publisher`

Default null: Csv File Access Log Publisher

Enabled by default: true

See Csv File Access Log Publisher for the properties of this Log Publisher type.

`csv-file-http-access-log-publisher`

Default null: Csv File HTTP Access Log Publisher

Enabled by default: true

See Csv File HTTP Access Log Publisher for the properties of this Log Publisher type.

`external-access-log-publisher`

Default null: External Access Log Publisher

Enabled by default: true

See External Access Log Publisher for the properties of this Log Publisher type.

`external-http-access-log-publisher`

Default null: External HTTP Access Log Publisher

Enabled by default: true

See External HTTP Access Log Publisher for the properties of this Log Publisher type.

`file-based-access-log-publisher`

Default null: File Based Access Log Publisher

Enabled by default: true

See File Based Access Log Publisher for the properties of this Log Publisher type.

`file-based-audit-log-publisher`

Default null: File Based Audit Log Publisher

Enabled by default: true

See File Based Audit Log Publisher for the properties of this Log Publisher type.

`file-based-debug-log-publisher`

Default null: File Based Debug Log Publisher

Enabled by default: true

See File Based Debug Log Publisher for the properties of this Log Publisher type.

`file-based-error-log-publisher`

Default null: File Based Error Log Publisher

Enabled by default: true

See File Based Error Log Publisher for the properties of this Log Publisher type.

`file-based-http-access-log-publisher`

Default null: File Based HTTP Access Log Publisher

Enabled by default: true

See File Based HTTP Access Log Publisher for the properties of this Log Publisher type.

`json-file-access-log-publisher`

Default null: Json File Access Log Publisher

Enabled by default: true

See Json File Access Log Publisher for the properties of this Log Publisher type.

`json-file-http-access-log-publisher`

Default null: Json File HTTP Access Log Publisher

Enabled by default: true

See Json File HTTP Access Log Publisher for the properties of this Log Publisher type.

Csv File Access Log Publisher

Log Publishers of type csv-file-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writting in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CsvFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Csv File Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when the tamper-evident option is enabled.

Default Value

3s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Csv File HTTP Access Log Publisher

Log Publishers of type csv-file-http-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File HTTP Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Csv File HTTP Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when secure option is enabled.

Default Value

3s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

External Access Log Publisher

Log Publishers of type external-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External Access Log Publisher. The content of the

JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External Access Log Publisher implementation.

Default Value

org.opends.server.loggers.ExternalAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

External HTTP Access Log Publisher

Log Publishers of type external-http-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External HTTP Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Access Log Publisher

Log Publishers of type file-based-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the access log.

Default Value

multi-line

Allowed Values

combined

Combine log records for operation requests and responses into a single record. This format should be used when log records are to be filtered based on response criteria (e.g. result code).

multi-line

Outputs separate log records for operation requests and responses.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Audit Log Publisher

Log Publishers of type file-based-audit-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Audit Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Audit Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAuditLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Audit Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Audit Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Audit Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Audit Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Debug Log Publisher

Log Publishers of type file-based-debug-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Debug Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-include-throwable-cause

Description

Indicates whether to include the cause of exceptions in exception thrown and caught messages logged by default.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-entry-arguments

Description

Indicates whether to include method arguments in debug messages logged by default.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-return-value

Description

Indicates whether to include the return value in debug messages logged by default.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-throwable-stack-frames

Description

Indicates the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Debug Log Publisher implementation.

Default Value

org.opends.server.loggers.TextDebugLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Debug Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Debug Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Debug Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Debug Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Error Log Publisher

Log Publishers of type file-based-error-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Error Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer will be flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-severity

Description

Specifies the default severity levels for the logger.

Default Value

error warning

Allowed Values

all

Messages of all severity levels are logged.

debug

The error log severity that is used for messages that provide debugging information triggered during processing.

error

The error log severity that is used for messages that provide information about errors which may force the server to shut down or operate in a significantly degraded state.

info

The error log severity that is used for messages that provide information about significant events within the server that are not warnings or errors.

none

No messages of any severity are logged by default. This value is intended to be used in conjunction with the override-severity property to define an error logger that will publish no error message beside the errors of a given category.

notice

The error log severity that is used for the most important informational messages (i.e., information that should almost always be logged but is not associated with a warning or error condition).

warning

The error log severity that is used for messages that provide information about warnings triggered during processing.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Error Log Publisher implementation.

Default Value

org.opends.server.loggers.TextErrorLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Error Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Error Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

override-severity

Description

Specifies the override severity levels for the logger based on the category of the messages. Each override severity level should include the category and the severity levels to log for that category, for example, core=error,info,warning. Valid categories are: core, extensions, protocol, config, log, util, schema, plugin, jeb, backend, tools, task, access-control, admin, sync, version, quicksetup, admin-tool, dsconfig, user-defined. Valid severities are: all, error, info, warning, notice, debug.

Default Value

All messages with the default severity levels are logged.

Allowed Values

A string in the form category=severity1,severity2...

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Error Log Publisher . When multiple policies are used, log files will be cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files will never be cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Error Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based HTTP Access Log Publisher

Log Publishers of type file-based-http-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based HTTP Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based HTTP Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the HTTP access log.

Default Value

cs-host c-ip cs-username x-datetime cs-method cs-uri-stem cs-uri-query cs-version sc-status cs(User-Agent) x-connection-id x-etime x-transaction-id

Allowed Values

A space separated list of fields describing the extended log format to be used for logging HTTP accesses. Available values are listed on the W3C working draft http://www.w3.org/TR/WD-logfile.html and Microsoft website http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/676400bc-8969-4aa7-851a-9319490a9bbb.mspx?mfr=true
OpenDJ supports the following standard fields: "c-ip", "c-port", "cs-host", "cs-method", "cs-uri", "cs-uri-stem", "cs-uri-query", "cs(User-Agent)", "cs-username", "cs-version", "s-computername", "s-ip", "s-port", "sc-status". OpenDJ supports the following application specific field extensions: "x-connection-id" displays the internal connection ID assigned to the HTTP client connection, "x-datetime" displays the completion date and time for the logged HTTP request and its ouput is controlled by the "ds-cfg-log-record-time-format" property, "x-etime" displays the total execution time for the logged HTTP request, "x-transaction-id" displays the transaction id associated to a request

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Json File Access Log Publisher

Log Publishers of type json-file-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.JsonFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Json File HTTP Access Log Publisher

Log Publishers of type json-file-http-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-log-retention-policy(1)

Name

dsconfig delete-log-retention-policy - Deletes Log Retention Policies

Synopsis

`dsconfig delete-log-retention-policy` {options}

Description

Deletes Log Retention Policies.

Options

The `dsconfig delete-log-retention-policy` command takes the following options:

`--policy-name {name}`

The name of the Log Retention Policy.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

`file-count-log-retention-policy`

Default {name}: File Count Log Retention Policy

Enabled by default: false

See File Count Log Retention Policy for the properties of this Log Retention Policy type.

`free-disk-space-log-retention-policy`

Default {name}: Free Disk Space Log Retention Policy

Enabled by default: false

See Free Disk Space Log Retention Policy for the properties of this Log Retention Policy type.

`size-limit-log-retention-policy`

Default {name}: Size Limit Log Retention Policy

Enabled by default: false

See Size Limit Log Retention Policy for the properties of this Log Retention Policy type.

`-f | --force`

Ignore non-existent Log Retention Policies.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

`file-count-log-retention-policy`

Default null: File Count Log Retention Policy

Enabled by default: false

See File Count Log Retention Policy for the properties of this Log Retention Policy type.

`free-disk-space-log-retention-policy`

Default null: Free Disk Space Log Retention Policy

Enabled by default: false

See Free Disk Space Log Retention Policy for the properties of this Log Retention Policy type.

`size-limit-log-retention-policy`

Default null: Size Limit Log Retention Policy

Enabled by default: false

See Size Limit Log Retention Policy for the properties of this Log Retention Policy type.

File Count Log Retention Policy

Log Retention Policies of type file-count-log-retention-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the File Count Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FileNumberRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

number-of-files

Description

Specifies the number of archived log files to retain before the oldest ones are cleaned.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Free Disk Space Log Retention Policy

Log Retention Policies of type free-disk-space-log-retention-policy have the following properties:

free-disk-space

Description

Specifies the minimum amount of free disk space that should be available on the file system on which the archived log files are stored.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Free Disk Space Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FreeDiskSpaceRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Size Limit Log Retention Policy

Log Retention Policies of type size-limit-log-retention-policy have the following properties:

disk-space-used

Description

Specifies the maximum total disk space used by the log files.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Retention Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-log-rotation-policy(1)

Name

dsconfig delete-log-rotation-policy - Deletes Log Rotation Policies

Synopsis

`dsconfig delete-log-rotation-policy` {options}

Description

Deletes Log Rotation Policies.

Options

The `dsconfig delete-log-rotation-policy` command takes the following options:

`--policy-name {name}`

The name of the Log Rotation Policy.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

`fixed-time-log-rotation-policy`

Default {name}: Fixed Time Log Rotation Policy

Enabled by default: false

See Fixed Time Log Rotation Policy for the properties of this Log Rotation Policy type.

`size-limit-log-rotation-policy`

Default {name}: Size Limit Log Rotation Policy

Enabled by default: false

See Size Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`time-limit-log-rotation-policy`

Default {name}: Time Limit Log Rotation Policy

Enabled by default: false

See Time Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`-f | --force`

Ignore non-existent Log Rotation Policies.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

`fixed-time-log-rotation-policy`

Default null: Fixed Time Log Rotation Policy

Enabled by default: false

See Fixed Time Log Rotation Policy for the properties of this Log Rotation Policy type.

`size-limit-log-rotation-policy`

Default null: Size Limit Log Rotation Policy

Enabled by default: false

See Size Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`time-limit-log-rotation-policy`

Default null: Time Limit Log Rotation Policy

Enabled by default: false

See Time Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

Fixed Time Log Rotation Policy

Log Rotation Policies of type fixed-time-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fixed Time Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.FixedTimeRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-of-day

Description

Specifies the time of day at which log rotation should occur.

Default Value

None

Allowed Values

24 hour time of day in HHmm format.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Size Limit Log Rotation Policy

Log Rotation Policies of type size-limit-log-rotation-policy have the following properties:

file-size-limit

Description

Specifies the maximum size that a log file can reach before it is rotated.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Time Limit Log Rotation Policy

Log Rotation Policies of type time-limit-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Time Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.TimeLimitRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

rotation-interval

Description

Specifies the time interval between rotations.

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-monitor-provider(1)

Name

dsconfig delete-monitor-provider - Deletes Monitor Providers

Synopsis

`dsconfig delete-monitor-provider` {options}

Description

Deletes Monitor Providers.

Options

The `dsconfig delete-monitor-provider` command takes the following options:

`--provider-name {name}`

The name of the Monitor Provider.

Monitor Provider properties depend on the Monitor Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

`client-connection-monitor-provider`

Default {name}: Client Connection Monitor Provider

Enabled by default: true

See Client Connection Monitor Provider for the properties of this Monitor Provider type.

`entry-cache-monitor-provider`

Default {name}: Entry Cache Monitor Provider

Enabled by default: true

See Entry Cache Monitor Provider for the properties of this Monitor Provider type.

`memory-usage-monitor-provider`

Default {name}: Memory Usage Monitor Provider

Enabled by default: true

See Memory Usage Monitor Provider for the properties of this Monitor Provider type.

`stack-trace-monitor-provider`

Default {name}: Stack Trace Monitor Provider

Enabled by default: true

See Stack Trace Monitor Provider for the properties of this Monitor Provider type.

`system-info-monitor-provider`

Default {name}: System Info Monitor Provider

Enabled by default: true

See System Info Monitor Provider for the properties of this Monitor Provider type.

`version-monitor-provider`

Default {name}: Version Monitor Provider

Enabled by default: true

See Version Monitor Provider for the properties of this Monitor Provider type.

`-f | --force`

Ignore non-existent Monitor Providers.

Monitor Provider properties depend on the Monitor Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

`client-connection-monitor-provider`

Default null: Client Connection Monitor Provider

Enabled by default: true

See Client Connection Monitor Provider for the properties of this Monitor Provider type.

`entry-cache-monitor-provider`

Default null: Entry Cache Monitor Provider

Enabled by default: true

See Entry Cache Monitor Provider for the properties of this Monitor Provider type.

`memory-usage-monitor-provider`

Default null: Memory Usage Monitor Provider

Enabled by default: true

See Memory Usage Monitor Provider for the properties of this Monitor Provider type.

`stack-trace-monitor-provider`

Default null: Stack Trace Monitor Provider

Enabled by default: true

See Stack Trace Monitor Provider for the properties of this Monitor Provider type.

`system-info-monitor-provider`

Default null: System Info Monitor Provider

Enabled by default: true

See System Info Monitor Provider for the properties of this Monitor Provider type.

`version-monitor-provider`

Default null: Version Monitor Provider

Enabled by default: true

See Version Monitor Provider for the properties of this Monitor Provider type.

Client Connection Monitor Provider

Monitor Providers of type client-connection-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Client Connection Monitor Provider implementation.

Default Value

org.opends.server.monitors.ClientConnectionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Entry Cache Monitor Provider

Monitor Providers of type entry-cache-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Entry Cache Monitor Provider implementation.

Default Value

org.opends.server.monitors.EntryCacheMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Memory Usage Monitor Provider

Monitor Providers of type memory-usage-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Memory Usage Monitor Provider implementation.

Default Value

org.opends.server.monitors.MemoryUsageMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Stack Trace Monitor Provider

Monitor Providers of type stack-trace-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Stack Trace Monitor Provider implementation.

Default Value

org.opends.server.monitors.StackTraceMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

System Info Monitor Provider

Monitor Providers of type system-info-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the System Info Monitor Provider implementation.

Default Value

org.opends.server.monitors.SystemInfoMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Version Monitor Provider

Monitor Providers of type version-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Version Monitor Provider implementation.

Default Value

org.opends.server.monitors.VersionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-password-generator(1)

Name

dsconfig delete-password-generator - Deletes Password Generators

Synopsis

`dsconfig delete-password-generator` {options}

Description

Deletes Password Generators.

Options

The `dsconfig delete-password-generator` command takes the following options:

`--generator-name {name}`

The name of the Password Generator.

Password Generator properties depend on the Password Generator type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

`random-password-generator`

Default {name}: Random Password Generator

Enabled by default: true

See Random Password Generator for the properties of this Password Generator type.

`-f | --force`

Ignore non-existent Password Generators.

Password Generator properties depend on the Password Generator type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Password Generator types:

`random-password-generator`

Default null: Random Password Generator

Enabled by default: true

See Random Password Generator for the properties of this Password Generator type.

Random Password Generator

Password Generators of type random-password-generator have the following properties:

enabled

Description

Indicates whether the Password Generator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Random Password Generator implementation.

Default Value

org.opends.server.extensions.RandomPasswordGenerator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordGenerator

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

password-character-set

Description

Specifies one or more named character sets. This is a multi-valued property, with each value defining a different character set. The format of the character set is the name of the set followed by a colon and the characters that are in that set. For example, the value "alpha:abcdefghijklmnopqrstuvwxyz" defines a character set named "alpha" containing all of the lower-case ASCII alphabetic characters.

Default Value

None

Allowed Values

A character set name (consisting of ASCII letters) followed by a colon and the set of characters that are included in that character set.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-format

Description

Specifies the format to use for the generated password. The value is a comma-delimited list of elements in which each of those elements is comprised of the name of a character set defined in the password-character-set property, a colon, and the number of characters to include from that set. For example, a value of "alpha:3,numeric:2,alpha:3" generates an 8-character password in which the first three characters are from the "alpha" set, the next two are from the "numeric"

set, and the final three are from the "alpha" set.

Default Value

None

Allowed Values

A comma-delimited list whose elements comprise a valid character set name, a colon, and a positive integer indicating the number of characters from that set to be included.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-password-policy(1)

Name

dsconfig delete-password-policy - Deletes Authentication Policies

Synopsis

`dsconfig delete-password-policy` {options}

Description

Deletes Authentication Policies.

Options

The `dsconfig delete-password-policy` command takes the following options:

`--policy-name {name}`

The name of the Authentication Policy.

Authentication Policy properties depend on the Authentication Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

`ldap-pass-through-authentication-policy`

Default {name}: LDAP Pass Through Authentication Policy

Enabled by default: false

See LDAP Pass Through Authentication Policy for the properties of this Authentication Policy type.

`password-policy`

Default {name}: Password Policy

Enabled by default: false

See Password Policy for the properties of this Authentication Policy type.

`-f | --force`

Ignore non-existent Authentication Policies.

Authentication Policy properties depend on the Authentication Policy type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

`ldap-pass-through-authentication-policy`

Default null: LDAP Pass Through Authentication Policy

Enabled by default: false

See LDAP Pass Through Authentication Policy for the properties of this Authentication Policy type.

`password-policy`

Default null: Password Policy

Enabled by default: false

See Password Policy for the properties of this Authentication Policy type.

LDAP Pass Through Authentication Policy

Authentication Policies of type ldap-pass-through-authentication-policy have the following properties:

cached-password-storage-scheme

Description

Specifies the name of a password storage scheme which should be used for encoding cached passwords. Changing the password storage scheme will cause all existing cached passwords to be discarded.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cached-password-ttl

Description

Specifies the maximum length of time that a locally cached password may be used for authentication before it is refreshed from the remote LDAP service. This property represents a cache timeout. Increasing the timeout period decreases the frequency that bind operations are delegated to the remote LDAP service, but increases the risk of users authenticating using stale passwords. Note that authentication attempts which fail because the provided password does not match the locally cached password will always be retried against the remote LDAP service.

Default Value

8 hours

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-timeout

Description

Specifies the timeout used when connecting to remote LDAP directory servers, performing SSL negotiation, and for individual search and bind requests. If the timeout expires then the current operation will be aborted and retried against another LDAP server if one is available.

Default Value

3 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the LDAP Pass Through Authentication Policy implementation.

Default Value

org.opends.server.extensions.LDAPPassThroughAuthenticationPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

mapped-attribute

Description

Specifies one or more attributes in the user's entry whose value(s) will determine the bind DN used when authenticating to the remote LDAP directory service. This property is mandatory when using the "mapped-bind" or "mapped-search" mapping policies. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory

server schema. At least one of the named attributes must exist in a user's local entry in order for authentication to proceed. When multiple attributes or values are found in the user's entry then the behavior is determined by the mapping policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-base-dn

Description

Specifies the set of base DNs below which to search for users in the remote LDAP directory service. This property is mandatory when using the "mapped-search" mapping policy. If multiple values are given, searches are performed below all specified base DNs.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-dn

Description

Specifies the bind DN which should be used to perform user searches in the remote LDAP directory service.

Default Value

Searches will be performed anonymously.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password

Description

Specifies the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-environment-variable

Description

Specifies the name of an environment variable containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-file

Description

Specifies the name of a file containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-property

Description

Specifies the name of a Java property containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-filter-template

Description

If defined, overrides the filter used when searching for the user, substituting %s with the value of the local entry's "mapped-attribute". The filter-template may include ZERO or ONE %s substitutions. If multiple mapped-attributes are configured, multiple renditions of this template will be aggregated into one larger filter using an OR (|) operator. An example use-case for this property would be to use a different attribute type on the mapped search. For example, mapped-attribute could be set to "uid" and filter-template to "(samAccountName=%s)". You can also use the filter to restrict search results. For example: "(&(uid=%s)(objectclass=student))"

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapping-policy

Description

Specifies the mapping algorithm for obtaining the bind DN from the user's entry.

Default Value

unmapped

Allowed Values

mapped-bind

Bind to the remote LDAP directory service using a DN obtained from an attribute in the user’s entry. This policy will check each attribute named in the "mapped-attribute" property. If more than one attribute or value is present then the first one will be used.

mapped-search

Bind to the remote LDAP directory service using the DN of an entry obtained using a search against the remote LDAP directory service. The search filter will comprise of an equality matching filter whose attribute type is the "mapped-attribute" property, and whose assertion

value is the attribute value obtained from the user's entry. If more than one attribute or value is present then the filter will be composed of multiple equality filters combined using a logical OR (union).

unmapped

Bind to the remote LDAP directory service using the DN of the user's entry in this directory server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

primary-remote-ldap-server

Description

Specifies the primary list of remote LDAP servers which should be used for pass through authentication. If more than one LDAP server is specified then operations may be distributed across them. If all of the primary LDAP servers are unavailable then operations will fail-over to the set of secondary LDAP servers, if defined.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-remote-ldap-server

Description

Specifies the secondary list of remote LDAP servers which should be used for pass through authentication in the event that the primary LDAP servers are unavailable. If more than one LDAP server is specified then operations may be distributed across them. Operations will be rerouted to the primary LDAP servers as soon as they are determined to be available.

Default Value

No secondary LDAP servers.

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols which are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with remote LDAP directory servers.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

use-password-caching

Description

Indicates whether passwords should be cached locally within the user's entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Pass Through Authentication Policy should use SSL. If enabled, the LDAP Pass Through Authentication Policy will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether LDAP connections should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether LDAP connections should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Policy

Authentication Policies of type password-policy have the following properties:

account-status-notification-handler

Description

Specifies the names of the account status notification handlers that are used with the associated password storage scheme.

Default Value

None

Allowed Values

The DN of any Account Status Notification Handler. The referenced account status notification handlers must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-expired-password-changes

Description

Indicates whether a user whose password is expired is still allowed to change that password using the password modify extended operation.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-multiple-password-values

Description

Indicates whether user entries can have multiple distinct values for the password attribute. This is potentially dangerous because many mechanisms used to change the password do not work well with such a configuration. If multiple password values are allowed, then any of them can be used to authenticate, and they are all subject to the same policy constraints.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-pre-encoded-passwords

Description

Indicates whether users can change their passwords by providing a pre-encoded value. This can cause a security risk because the clear-text version of the password is not known and therefore validation checks cannot be applied to it.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-user-password-changes

Description

Indicates whether users can change their own passwords. This check is made in addition to access control evaluation. Both must allow the password change for it to occur.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-password-storage-scheme

Description

Specifies the names of the password storage schemes that are used to encode clear-text passwords for this password policy.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

deprecated-password-storage-scheme

Description

Specifies the names of the password storage schemes that are considered deprecated for this password policy. If a user with this password policy authenticates to the server and his/her password is encoded with a deprecated scheme, those values are removed and replaced with values encoded using the default password storage scheme(s).

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

expire-passwords-without-warning

Description

Indicates whether the directory server allows a user's password to expire even if that user has never seen an expiration warning notification. If this property is true, accounts always expire when the expiration time arrives. If this property is false or disabled, the user always receives at least one warning notification, and the password expiration is set to the warning time plus the warning interval.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-add

Description

Indicates whether users are forced to change their passwords upon first authenticating to the directory server after their account has been created.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-reset

Description

Indicates whether users are forced to change their passwords if they are reset by an administrator. For this purpose, anyone with permission to change a given user's password other than that user is considered an administrator.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

grace-login-count

Description

Specifies the number of grace logins that a user is allowed after the account has expired to allow that user to choose a new password. A value of 0 indicates that no grace logins are allowed.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

idle-lockout-interval

Description

Specifies the maximum length of time that an account may remain idle (that is, the associated user does not authenticate to the server) before that user is locked out. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that idle accounts are not automatically locked out. This feature is available only if the last login time is maintained.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the Password Policy implementation.

Default Value

org.opends.server.core.PasswordPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

last-login-time-attribute

Description

Specifies the name or OID of the attribute type that is used to hold the last login time for users with the associated password policy. This attribute type must be defined in the directory server schema and must either be defined as an operational attribute or must be allowed by the set of objectClasses for all users with the associated password policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

last-login-time-format

Description

Specifies the format string that is used to generate the last login time value for users with the associated password policy. This format string conforms to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-duration

Description

Specifies the length of time that an account is locked after too many authentication failures. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the account must remain locked until an administrator resets the password.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-count

Description

Specifies the maximum number of authentication failures that a user is allowed before the account is locked out. A value of 0 indicates that accounts are never locked out due to failed attempts.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-expiration-interval

Description

Specifies the length of time before an authentication failure is no longer counted against a user for the purposes of account lockout. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the authentication failures must never expire. The failure count is always cleared upon a successful authentication.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-age

Description

Specifies the maximum length of time that a user can continue using the same password before it must be changed (that is, the password expiration interval). The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables password expiration.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-reset-age

Description

Specifies the maximum length of time that users have to change passwords after they have been reset by an administrator before they become locked. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables this feature.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-age

Description

Specifies the minimum length of time after a password change before the user is allowed to change the password again. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. This setting can be used to prevent users from changing their passwords repeatedly over a short period of time to flush an old password from the history so that it can be re-used.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-attribute

Description

Specifies the attribute type used to hold user passwords. This attribute type must be defined in the server schema, and it must have either the user password or auth password syntax.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-change-requires-current-password

Description

Indicates whether user password changes must use the password modify extended operation and must include the user's current password before the change is allowed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-expiration-warning-interval

Description

Specifies the maximum length of time before a user's password actually expires that the server begins to include warning notifications in bind responses for that user. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables the warning interval.

Default Value

5 days

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-generator

Description

Specifies the name of the password generator that is used with the associated password policy. This is used in conjunction with the password modify extended operation to generate a new password for a user when none was provided in the request.

Default Value

None

Allowed Values

The DN of any Password Generator. The referenced password generator must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-count

Description

Specifies the maximum number of former passwords to maintain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero indicates that either no password history is to be maintained (if the password history duration has a value of zero seconds), or that there is no maximum number of passwords to maintain in the history (if the password history duration has a value greater than zero seconds).

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-duration

Description

Specifies the maximum length of time that passwords remain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero seconds indicates that either no password history is to be maintained (if the password history count has a value of zero), or that there is no maximum duration for passwords in the history (if the password history count has a value greater than zero).

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-validator

Description

Specifies the names of the password validators that are used with the associated password storage scheme. The password validators are invoked when a user attempts to provide a new password, to determine whether the new password is acceptable.

Default Value

None

Allowed Values

The DN of any Password Validator. The referenced password validators must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

previous-last-login-time-format

Description

Specifies the format string(s) that might have been used with the last login time at any point in the past for users associated with the password policy. These values are used to make it possible to parse previous values, but are not used to set new values. The format strings conform to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-change-by-time

Description

Specifies the time by which all users with the associated password policy must change their

passwords. The value is expressed in a generalized time format. If this time is equal to the current time or is in the past, then all users are required to change their passwords immediately. The behavior of the server in this mode is identical to the behavior observed when users are forced to change their passwords after an administrative reset.

Default Value

None

Allowed Values

A valid timestamp in generalized time form (for example, a value of "20070409185811Z" indicates a value of April 9, 2007 at 6:58:11 pm GMT).

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-authentication

Description

Indicates whether users with the associated password policy are required to authenticate in a secure manner. This might mean either using a secure communication channel between the client and the server, or using a SASL mechanism that does not expose the credentials.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-password-changes

Description

Indicates whether users with the associated password policy are required to change their password in a secure manner that does not expose the credentials.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

skip-validation-for-administrators

Description

Indicates whether passwords set by administrators are allowed to bypass the password validation process that is required for user password changes.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

state-update-failure-policy

Description

Specifies how the server deals with the inability to update password policy state information during an authentication attempt. In particular, this property can be used to control whether an otherwise successful bind operation fails if a failure occurs while attempting to update password policy state information (for example, to clear a record of previous authentication failures or to update the last login time). It can also be used to control whether to reject a bind request if it is known ahead of time that it will not be possible to update the authentication failure times in the event of an unsuccessful bind attempt (for example, if the backend writability mode is disabled).

Default Value

reactive

Allowed Values

ignore

If a bind attempt would otherwise be successful, then do not reject it if a problem occurs while attempting to update the password policy state information for the user.

proactive

Proactively reject any bind attempt if it is known ahead of time that it would not be possible to update the user's password policy state information.

reactive

Even if a bind attempt would otherwise be successful, reject it if a problem occurs while attempting to update the password policy state information for the user.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-password-storage-scheme(1)

Name

dsconfig delete-password-storage-scheme - Deletes Password Storage Schemes

Synopsis

`dsconfig delete-password-storage-scheme` {options}

Description

Deletes Password Storage Schemes.

Options

The `dsconfig delete-password-storage-scheme` command takes the following options:

`--scheme-name {name}`

The name of the Password Storage Scheme.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

`aes-password-storage-scheme`

Default {name}: AES Password Storage Scheme

Enabled by default: true

See AES Password Storage Scheme for the properties of this Password Storage Scheme type.

`base64-password-storage-scheme`

Default {name}: Base64 Password Storage Scheme

Enabled by default: true

See Base64 Password Storage Scheme for the properties of this Password Storage Scheme type.

`bcrypt-password-storage-scheme`

Default {name}: Bcrypt Password Storage Scheme

Enabled by default: true

See Bcrypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`blowfish-password-storage-scheme`

Default {name}: Blowfish Password Storage Scheme

Enabled by default: true

See Blowfish Password Storage Scheme for the properties of this Password Storage Scheme type.

`clear-password-storage-scheme`

Default {name}: Clear Password Storage Scheme

Enabled by default: true

See Clear Password Storage Scheme for the properties of this Password Storage Scheme type.

`crypt-password-storage-scheme`

Default {name}: Crypt Password Storage Scheme

Enabled by default: true

See Crypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`md5-password-storage-scheme`

Default {name}: MD5 Password Storage Scheme

Enabled by default: true

See MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha256-password-storage-scheme`

Default {name}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha512-password-storage-scheme`

Default {name}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pkcs5s2-password-storage-scheme`

Default {name}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See PKCS5S2 Password Storage Scheme for the properties of this Password Storage Scheme

type.

`rc4-password-storage-scheme`

Default {name}: RC4 Password Storage Scheme

Enabled by default: true

See RC4 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-md5-password-storage-scheme`

Default {name}: Salted MD5 Password Storage Scheme

Enabled by default: true

See Salted MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha1-password-storage-scheme`

Default {name}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See Salted SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha256-password-storage-scheme`

Default {name}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See Salted SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha384-password-storage-scheme`

Default {name}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See Salted SHA384 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha512-password-storage-scheme`

Default {name}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See Salted SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`sha1-password-storage-scheme`

Default {name}: SHA1 Password Storage Scheme

Enabled by default: true

See SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`triple-des-password-storage-scheme`

Default {name}: Triple DES Password Storage Scheme

Enabled by default: true

See Triple DES Password Storage Scheme for the properties of this Password Storage Scheme type.

`-f | --force`

Ignore non-existent Password Storage Schemes.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

`aes-password-storage-scheme`

Default null: AES Password Storage Scheme

Enabled by default: true

See AES Password Storage Scheme for the properties of this Password Storage Scheme type.

`base64-password-storage-scheme`

Default null: Base64 Password Storage Scheme

Enabled by default: true

See Base64 Password Storage Scheme for the properties of this Password Storage Scheme type.

`bcrypt-password-storage-scheme`

Default null: Bcrypt Password Storage Scheme

Enabled by default: true

See Bcrypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`blowfish-password-storage-scheme`

Default null: Blowfish Password Storage Scheme

Enabled by default: true

See Blowfish Password Storage Scheme for the properties of this Password Storage Scheme type.

`clear-password-storage-scheme`

Default null: Clear Password Storage Scheme

Enabled by default: true

See Clear Password Storage Scheme for the properties of this Password Storage Scheme type.

`crypt-password-storage-scheme`

Default null: Crypt Password Storage Scheme

Enabled by default: true

See Crypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`md5-password-storage-scheme`

Default null: MD5 Password Storage Scheme

Enabled by default: true

See MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha256-password-storage-scheme`

Default null: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha512-password-storage-scheme`

Default null: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pkcs5s2-password-storage-scheme`

Default null: PKCS5S2 Password Storage Scheme

Enabled by default: true

See PKCS5S2 Password Storage Scheme for the properties of this Password Storage Scheme type.

`rc4-password-storage-scheme`

Default null: RC4 Password Storage Scheme

Enabled by default: true

See RC4 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-md5-password-storage-scheme`

Default null: Salted MD5 Password Storage Scheme

Enabled by default: true

See Salted MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha1-password-storage-scheme`

Default null: Salted SHA1 Password Storage Scheme

Enabled by default: true

See Salted SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha256-password-storage-scheme`

Default null: Salted SHA256 Password Storage Scheme

Enabled by default: true

See Salted SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha384-password-storage-scheme`

Default null: Salted SHA384 Password Storage Scheme

Enabled by default: true

See Salted SHA384 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha512-password-storage-scheme`

Default null: Salted SHA512 Password Storage Scheme

Enabled by default: true

See Salted SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`sha1-password-storage-scheme`

Default null: SHA1 Password Storage Scheme

Enabled by default: true

See SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`triple-des-password-storage-scheme`

Default null: Triple DES Password Storage Scheme

Enabled by default: true

See Triple DES Password Storage Scheme for the properties of this Password Storage Scheme type.

AES Password Storage Scheme

Password Storage Schemes of type aes-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the AES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.AESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Base64 Password Storage Scheme

Password Storage Schemes of type base64-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Base64 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.Base64PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Bcrypt Password Storage Scheme

Password Storage Schemes of type bcrypt-password-storage-scheme have the following properties:

bcrypt-cost

Description

The cost parameter specifies a key expansion iteration count as a power of two. A default value of 12 (2^12 iterations) is considered in 2016 as a reasonable balance between responsiveness and security for regular users.

Default Value

12

Allowed Values

An integer value. Lower value is 1. Upper value is 30.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Bcrypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BcryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Blowfish Password Storage Scheme

Password Storage Schemes of type blowfish-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Blowfish Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BlowfishPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Clear Password Storage Scheme

Password Storage Schemes of type clear-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Clear Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.ClearPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Crypt Password Storage Scheme

Password Storage Schemes of type crypt-password-storage-scheme have the following properties:

crypt-password-storage-encryption-algorithm

Description

Specifies the algorithm to use to encrypt new passwords. Select the crypt algorithm to use to encrypt new passwords. The value can either be "unix", which means the password is encrypted with the weak Unix crypt algorithm, or "md5" which means the password is encrypted with the BSD MD5 algorithm and has a 1 prefix, or "sha256" which means the password is encrypted with the SHA256 algorithm and has a 5 prefix, or "sha512" which means the password is encrypted with the SHA512 algorithm and has a 6 prefix.

Default Value

unix

Allowed Values

md5

New passwords are encrypted with the BSD MD5 algorithm.

sha256

New passwords are encrypted with the Unix crypt SHA256 algorithm.

sha512

New passwords are encrypted with the Unix crypt SHA512 algorithm.

unix

New passwords are encrypted with the Unix crypt algorithm. Passwords are truncated at 8 characters and the top bit of each character is ignored.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Crypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.CryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

MD5 Password Storage Scheme

Password Storage Schemes of type md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.MD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

PBKDF2 Hmac SHA256 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

PBKDF2 Hmac SHA512 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

PKCS5S2 Password Storage Scheme

Password Storage Schemes of type pkcs5s2-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PKCS5S2 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PKCS5S2PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

RC4 Password Storage Scheme

Password Storage Schemes of type rc4-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the RC4 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.RC4PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted MD5 Password Storage Scheme

Password Storage Schemes of type salted-md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedMD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA1 Password Storage Scheme

Password Storage Schemes of type salted-sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA256 Password Storage Scheme

Password Storage Schemes of type salted-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA384 Password Storage Scheme

Password Storage Schemes of type salted-sha384-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA384 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA384PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA512 Password Storage Scheme

Password Storage Schemes of type salted-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

SHA1 Password Storage Scheme

Password Storage Schemes of type sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Triple DES Password Storage Scheme

Password Storage Schemes of type triple-des-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Triple DES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.TripleDESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-password-validator(1)

Name

dsconfig delete-password-validator - Deletes Password Validators

Synopsis

`dsconfig delete-password-validator` {options}

Description

Deletes Password Validators.

Options

The `dsconfig delete-password-validator` command takes the following options:

`--validator-name {name}`

The name of the Password Validator.

Password Validator properties depend on the Password Validator type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

`attribute-value-password-validator`

Default {name}: Attribute Value Password Validator

Enabled by default: true

See Attribute Value Password Validator for the properties of this Password Validator type.

`character-set-password-validator`

Default {name}: Character Set Password Validator

Enabled by default: true

See Character Set Password Validator for the properties of this Password Validator type.

`dictionary-password-validator`

Default {name}: Dictionary Password Validator

Enabled by default: true

See Dictionary Password Validator for the properties of this Password Validator type.

`length-based-password-validator`

Default {name}: Length Based Password Validator

Enabled by default: true

See Length Based Password Validator for the properties of this Password Validator type.

`repeated-characters-password-validator`

Default {name}: Repeated Characters Password Validator

Enabled by default: true

See Repeated Characters Password Validator for the properties of this Password Validator type.

`similarity-based-password-validator`

Default {name}: Similarity Based Password Validator

Enabled by default: true

See Similarity Based Password Validator for the properties of this Password Validator type.

`unique-characters-password-validator`

Default {name}: Unique Characters Password Validator

Enabled by default: true

See Unique Characters Password Validator for the properties of this Password Validator type.

`-f | --force`

Ignore non-existent Password Validators.

Password Validator properties depend on the Password Validator type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Password Validator types:

`attribute-value-password-validator`

Default null: Attribute Value Password Validator

Enabled by default: true

See Attribute Value Password Validator for the properties of this Password Validator type.

`character-set-password-validator`

Default null: Character Set Password Validator

Enabled by default: true

See Character Set Password Validator for the properties of this Password Validator type.

`dictionary-password-validator`

Default null: Dictionary Password Validator

Enabled by default: true

See Dictionary Password Validator for the properties of this Password Validator type.

`length-based-password-validator`

Default null: Length Based Password Validator

Enabled by default: true

See Length Based Password Validator for the properties of this Password Validator type.

`repeated-characters-password-validator`

Default null: Repeated Characters Password Validator

Enabled by default: true

See Repeated Characters Password Validator for the properties of this Password Validator type.

`similarity-based-password-validator`

Default null: Similarity Based Password Validator

Enabled by default: true

See Similarity Based Password Validator for the properties of this Password Validator type.

`unique-characters-password-validator`

Default null: Unique Characters Password Validator

Enabled by default: true

See Unique Characters Password Validator for the properties of this Password Validator type.

Attribute Value Password Validator

Password Validators of type attribute-value-password-validator have the following properties:

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against attribute values. If "false" then only match the entire password against attribute values otherwise ("true") check whether the password contains attribute values.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.AttributeValuePasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name(s) of the attribute(s) whose values should be checked to determine whether they match the provided password. If no values are provided, then the server checks if the proposed password matches the value of any attribute in the user's entry.

Default Value

All attributes in the user entry will be checked.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator should test the reversed value of the provided password as well as the order in which it was given.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Character Set Password Validator

Password Validators of type character-set-password-validator have the following properties:

allow-unclassified-characters

Description

Indicates whether this password validator allows passwords to contain characters outside of any of the user-defined character sets and ranges. If this is "false", then only those characters in the user-defined character sets and ranges may be used in passwords. Any password containing a character not included in any character set or range will be rejected.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set

Description

Specifies a character set containing characters that a password may contain and a value indicating the minimum number of characters required from that set. Each value must be an integer (indicating the minimum required characters from the set which may be zero, indicating

that the character set is optional) followed by a colon and the characters to include in that set (for example, "3:abcdefghijklmnopqrstuvwxyz" indicates that a user password must contain at least three characters from the set of lowercase ASCII letters). Multiple character sets can be defined in separate values, although no character can appear in more than one character set.

Default Value

If no sets are specified, the validator only uses the defined character ranges.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set-ranges

Description

Specifies a character range containing characters that a password may contain and a value indicating the minimum number of characters required from that range. Each value must be an integer (indicating the minimum required characters from the range which may be zero, indicating that the character range is optional) followed by a colon and one or more range specifications. A range specification is 3 characters: the first character allowed, a minus, and the last character allowed. For example, "3:A-Za-z0-9". The ranges in each value should not overlap, and the characters in each range specification should be ordered.

Default Value

If no ranges are specified, the validator only uses the defined character sets.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.CharacterSetPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-character-sets

Description

Specifies the minimum number of character sets and ranges that a password must contain. This property should only be used in conjunction with optional character sets and ranges (those requiring zero characters). Its value must include any mandatory character sets and ranges (those requiring greater than zero characters). This is useful in situations where a password must contain characters from mandatory character sets and ranges, and characters from at least N optional character sets and ranges. For example, it is quite common to require that a password contains at least one non-alphanumeric character as well as characters from two alphanumeric character sets (lower-case, upper-case, digits). In this case, this property should be set to 3.

Default Value

The password must contain characters from each of the mandatory character sets and ranges and, if there are optional character sets and ranges, at least one character from one of the optional character sets and ranges.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Dictionary Password Validator

Password Validators of type dictionary-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator is to treat password characters in a case-sensitive manner. If it is set to true, then the validator rejects a password only if it appears in the dictionary with exactly the same capitalization as provided by the user.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against dictionary words. If "false" then only match the entire password against words otherwise ("true") check whether the password contains words.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dictionary-file

Description

Specifies the path to the file containing a list of words that cannot be used as passwords. It should be formatted with one word per line. The value can be an absolute path or a path that is relative to the OpenDJ instance root.

Default Value

For Unix and Linux systems: config/wordlist.txt. For Windows systems: config\wordlist.txt

Allowed Values

The path to any text file contained on the system that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.DictionaryPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator is to test the reversed value of the provided password as well as the order in which it was given. For example, if the user provides a new password of "password" and this configuration attribute is set to true, then the value "drowssap" is also tested against attribute values in the user's entry.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Length Based Password Validator

Password Validators of type length-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.LengthBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-password-length

Description

Specifies the maximum number of characters that can be included in a proposed password. A value of zero indicates that there will be no upper bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-length

Description

Specifies the minimum number of characters that must be included in a proposed password. A value of zero indicates that there will be no lower bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

6

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Repeated Characters Password Validator

Password Validators of type repeated-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. If the value of this property is false, the validator ignores any differences in capitalization when looking for consecutive characters in the password. If the value is true, the validator considers a character to be repeating only if all consecutive occurrences use the same capitalization.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.RepeatedCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-consecutive-length

Description

Specifies the maximum number of times that any character can appear consecutively in a password value. A value of zero indicates that no maximum limit is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Similarity Based Password Validator

Password Validators of type similarity-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.SimilarityBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-password-difference

Description

Specifies the minimum difference of new and old password. A value of zero indicates that no difference between passwords is acceptable.

Default Value

None

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Unique Characters Password Validator

Password Validators of type unique-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. A value of true indicates that the validator does not consider a capital letter to be the same as its lower-case counterpart. A value of false indicates that the validator ignores differences in capitalization when looking at the number of unique characters in the password.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.UniqueCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-unique-characters

Description

Specifies the minimum number of unique characters that a password will be allowed to contain. A value of zero indicates that no minimum value is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-plugin(1)

Name

dsconfig delete-plugin - Deletes Plugins

Synopsis

`dsconfig delete-plugin` {options}

Description

Deletes Plugins.

Options

The `dsconfig delete-plugin` command takes the following options:

`--plugin-name {name}`
: The name of the Plugin.

  Plugin properties depend on the Plugin type, which depends on the {name} you provide.

  By default, OpenDJ directory server supports the following Plugin types:

  `attribute-cleanup-plugin`
  : Default {name}: Attribute Cleanup Plugin

    Enabled by default: true

    See Attribute Cleanup Plugin for the properties of this Plugin type.

  `change-number-control-plugin`
  : Default {name}: Change Number Control Plugin

    Enabled by default: true

    See Change Number Control Plugin for the properties of this Plugin type.

  `entry-uuid-plugin`
  : Default {name}: Entry UUID Plugin

    Enabled by default: true

    See Entry UUID Plugin for the properties of this Plugin type.

  `fractional-ldif-import-plugin`
  : Default {name}: Fractional LDIF Import Plugin

Enabled by default: true

See Fractional LDIF Import Plugin for the properties of this Plugin type.

`last-mod-plugin`

Default {name}: Last Mod Plugin

Enabled by default: true

See Last Mod Plugin for the properties of this Plugin type.

`ldap-attribute-description-list-plugin`

Default {name}: LDAP Attribute Description List Plugin

Enabled by default: true

See LDAP Attribute Description List Plugin for the properties of this Plugin type.

`password-policy-import-plugin`

Default {name}: Password Policy Import Plugin

Enabled by default: true

See Password Policy Import Plugin for the properties of this Plugin type.

`profiler-plugin`

Default {name}: Profiler Plugin

Enabled by default: true

See Profiler Plugin for the properties of this Plugin type.

`referential-integrity-plugin`

Default {name}: Referential Integrity Plugin

Enabled by default: true

See Referential Integrity Plugin for the properties of this Plugin type.

`samba-password-plugin`

Default {name}: Samba Password Plugin

Enabled by default: true

See Samba Password Plugin for the properties of this Plugin type.

`seven-bit-clean-plugin`

Default {name}: Seven Bit Clean Plugin

Enabled by default: true

See Seven Bit Clean Plugin for the properties of this Plugin type.

`unique-attribute-plugin`

Default {name}: Unique Attribute Plugin

Enabled by default: true

See Unique Attribute Plugin for the properties of this Plugin type.

`-f | --force`

Ignore non-existent Plugins.

Plugin properties depend on the Plugin type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Plugin types:

`attribute-cleanup-plugin`

Default null: Attribute Cleanup Plugin

Enabled by default: true

See Attribute Cleanup Plugin for the properties of this Plugin type.

`change-number-control-plugin`

Default null: Change Number Control Plugin

Enabled by default: true

See Change Number Control Plugin for the properties of this Plugin type.

`entry-uuid-plugin`

Default null: Entry UUID Plugin

Enabled by default: true

See Entry UUID Plugin for the properties of this Plugin type.

`fractional-ldif-import-plugin`

Default null: Fractional LDIF Import Plugin

Enabled by default: true

See Fractional LDIF Import Plugin for the properties of this Plugin type.

`last-mod-plugin`

Default null: Last Mod Plugin

Enabled by default: true

See Last Mod Plugin for the properties of this Plugin type.

`ldap-attribute-description-list-plugin`

Default null: LDAP Attribute Description List Plugin

Enabled by default: true

See LDAP Attribute Description List Plugin for the properties of this Plugin type.

`password-policy-import-plugin`

Default null: Password Policy Import Plugin

Enabled by default: true

See Password Policy Import Plugin for the properties of this Plugin type.

`profiler-plugin`

Default null: Profiler Plugin

Enabled by default: true

See Profiler Plugin for the properties of this Plugin type.

`referential-integrity-plugin`

Default null: Referential Integrity Plugin

Enabled by default: true

See Referential Integrity Plugin for the properties of this Plugin type.

`samba-password-plugin`

Default null: Samba Password Plugin

Enabled by default: true

See Samba Password Plugin for the properties of this Plugin type.

`seven-bit-clean-plugin`

Default null: Seven Bit Clean Plugin

Enabled by default: true

See Seven Bit Clean Plugin for the properties of this Plugin type.

`unique-attribute-plugin`

Default null: Unique Attribute Plugin

Enabled by default: true

See Unique Attribute Plugin for the properties of this Plugin type.

Attribute Cleanup Plugin

Plugins of type attribute-cleanup-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.AttributeCleanupPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparseadd preparsemodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

remove-inbound-attributes

Description

A list of attributes which should be removed from incoming add or modify requests.

Default Value

No attributes will be removed

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rename-inbound-attributes

Description

A list of attributes which should be renamed in incoming add or modify requests.

Default Value

No attributes will be renamed

Allowed Values

An attribute name mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Change Number Control Plugin

Plugins of type change-number-control-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ChangeNumberControlPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postOperationAdd postOperationDelete postOperationModify postOperationModifyDN

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Entry UUID Plugin

Plugins of type entry-uuid-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.EntryUUIDPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport preoperationadd

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Fractional LDIF Import Plugin

Plugins of type fractional-ldif-import-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

None

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

None

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the

client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

Last Mod Plugin

Plugins of type last-mod-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LastModPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd preoperationmodify preoperationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

LDAP Attribute Description List Plugin

Plugins of type ldap-attribute-description-list-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LDAPADListPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparsesearch

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Policy Import Plugin

Plugins of type password-policy-import-plugin have the following properties:

default-auth-password-storage-scheme

Description

Specifies the names of password storage schemes that to be used for encoding passwords contained in attributes with the auth password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy should be used to govern them.

Default Value

If the default password policy uses an attribute with the auth password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes auth password values using the "SHA1" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import plug-in is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-user-password-storage-scheme

Description

Specifies the names of the password storage schemes to be used for encoding passwords contained in attributes with the user password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy is to be used to govern them.

Default Value

If the default password policy uses the attribute with the user password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes user password values using the "SSHA" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import Plugin is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.PasswordPolicyImportPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Profiler Plugin

Plugins of type profiler-plugin have the following properties:

enable-profiling-on-startup

Description

Indicates whether the profiler plug-in is to start collecting data automatically when the directory server is started. This property is read only when the server is started, and any changes take effect on the next restart. This property is typically set to "false" unless startup profiling is required, because otherwise the volume of data that can be collected can cause the server to run out of memory if it is not turned off in a timely manner.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.profiler.ProfilerPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

startup

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

profile-action

Description

Specifies the action that should be taken by the profiler. A value of "start" causes the profiler thread to start collecting data if it is not already active. A value of "stop" causes the profiler thread to stop collecting data and write it to disk, and a value of "cancel" causes the profiler thread to stop collecting data and discard anything that has been captured. These operations occur immediately.

Default Value

none

Allowed Values

cancel

Stop collecting profile data and discard what has been captured.

none

Do not take any action.

start

Start collecting profile data.

stop

Stop collecting profile data and write what has been captured to a file in the profile directory.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-directory

Description

Specifies the path to the directory where profile information is to be written. This path may be either an absolute path or a path that is relative to the root of the OpenDJ directory server instance. The directory must exist and the directory server must have permission to create new files in it.

Default Value

None

Allowed Values

The path to any directory that exists on the filesystem and that can be read and written by the server user.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-sample-interval

Description

Specifies the sample interval in milliseconds to be used when capturing profiling information in the server. When capturing data, the profiler thread sleeps for this length of time between calls to obtain traces for all threads running in the JVM.

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

NoneChanges to this configuration attribute take effect the next time the profiler is started.

Advanced Property

No

Read-only

No

Referential Integrity Plugin

Plugins of type referential-integrity-plugin have the following properties:

attribute-type

Description

Specifies the attribute types for which referential integrity is to be maintained. At least one attribute type must be specified, and the syntax of any attributes must be either a distinguished name (1.3.6.1.4.1.1466.115.121.1.12) or name and optional UID (1.3.6.1.4.1.1466.115.121.1.34).

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN that limits the scope within which referential integrity is maintained.

Default Value

Referential integrity is maintained in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references

Description

Specifies whether reference attributes must refer to existing entries. When this property is set to true, this plugin will ensure that any new references added as part of an add or modify operation point to existing entries, and that the referenced entries match the filter criteria for the referencing attribute, if specified.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-filter-criteria

Description

Specifies additional filter criteria which will be enforced when checking references. If a reference attribute has filter criteria defined then this plugin will ensure that any new references added as part of an add or modify operation refer to an existing entry which matches the specified filter.

Default Value

None

Allowed Values

An attribute-filter mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-scope-criteria

Description

Specifies whether referenced entries must reside within the same naming context as the entry containing the reference. The reference scope will only be enforced when reference checking is enabled.

Default Value

global

Allowed Values

global

References may refer to existing entries located anywhere in the Directory.

naming-context

References must refer to existing entries located within the same naming context.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ReferentialIntegrityPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

Specifies the log file location where the update records are written when the plug-in is in background-mode processing. The default location is the logs directory of the server instance, using the file name "referint".

Default Value

logs/referint

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postoperationdelete postoperationmodifydn subordinatemodifydn subordinatedelete preoperationadd preoperationmodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

update-interval

Description

Specifies the interval in seconds when referential integrity updates are made. If this value is 0, then the updates are made synchronously in the foreground.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Samba Password Plugin

Plugins of type samba-password-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SambaPasswordPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationmodify postoperationextended

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pwd-sync-policy

Description

Specifies which Samba passwords should be kept synchronized.

Default Value

sync-nt-password

Allowed Values

sync-lm-password

Synchronize the LanMan password attribute "sambaLMPassword"

sync-nt-password

Synchronize the NT password attribute "sambaNTPassword"

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

samba-administrator-dn

Description

Specifies the distinguished name of the user which Samba uses to perform Password Modify extended operations against this directory server in order to synchronize the userPassword attribute after the LanMan or NT passwords have been updated. The user must have the 'password-reset' privilege and should not be a root user. This user name can be used in order to identify Samba connections and avoid double re-synchronization of the same password. If this property is left undefined, then no password updates will be skipped.

Default Value

Synchronize all updates to user passwords

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Seven Bit Clean Plugin

Plugins of type seven-bit-clean-plugin have the following properties:

attribute-type

Description

Specifies the name or OID of an attribute type for which values should be checked to ensure that they are 7-bit clean.

Default Value

uid mail userPassword

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN below which the checking is performed. Any attempt to update a value for one of the configured attributes below this base DN must be 7-bit clean for the operation to be allowed.

Default Value

All entries below all public naming contexts will be checked.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SevenBitCleanPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport preparseadd preparsemodify preparsemodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Unique Attribute Plugin

Plugins of type unique-attribute-plugin have the following properties:

base-dn

Description

Specifies a base DN within which the attribute must be unique.

Default Value

The plug-in uses the server's public naming contexts in the searches.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.UniqueAttributePlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd preoperationmodify preoperationmodifydn postoperationadd postoperationmodify postoperationmodifydn postsynchronizationadd postsynchronizationmodify postsynchronizationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

type

Description

Specifies the type of attributes to check for value uniqueness.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-replication-domain(1)

Name

dsconfig delete-replication-domain - Deletes Replication Domains

Synopsis

`dsconfig delete-replication-domain` {options}

Description

Deletes Replication Domains.

Options

The `dsconfig delete-replication-domain` command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default {name}: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

`--domain-name {name}`

The name of the Replication Domain.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default {name}: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

`-f | --force`

Ignore non-existent Replication Domains.

Replication Domain properties depend on the Replication Domain type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default null: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

Replication Domain

Replication Domains of type replication-domain have the following properties:

assured-sd-level

Description

The level of acknowledgment for Safe Data assured sub mode. When assured replication is configured in Safe Data mode, this value defines the number of replication servers (with the same group ID of the local server) that should acknowledge the sent update before the LDAP client call can return.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-timeout

Description

The timeout value when waiting for assured replication acknowledgments. Defines the amount of milliseconds the server will wait for assured acknowledgments (in either Safe Data or Safe Read assured replication modes) before returning anyway the LDAP client call.

Default Value

2000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-type

Description

Defines the assured replication mode of the replicated domain. The assured replication can be disabled or enabled. When enabled, two modes are available: Safe Data or Safe Read modes.

Default Value

not-assured

Allowed Values

not-assured

Assured replication is not enabled. Updates sent for replication (for being replayed on other LDAP servers in the topology) are sent without waiting for any acknowledgment and the LDAP client call returns immediately.

safe-data

Assured replication is enabled in Safe Data mode: updates sent for replication are subject to acknowledgment from the replication servers that have the same group ID as the local server (defined with the group-id property). The number of acknowledgments to expect is defined by the assured-sd-level property. After acknowledgments are received, LDAP client call returns.

safe-read

Assured replication is enabled in Safe Read mode: updates sent for replication are subject to acknowledgments from the LDAP servers in the topology that have the same group ID as the local server (defined with the group-id property). After acknowledgments are received, LDAP client call returns.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN of the replicated data.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

changetime-heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when sending its local change time to the Replication Server. The directory server sends a regular heart-beat to the Replication within the specified interval. The heart-beat indicates the change time of the directory server to the Replication Server.

Default Value

1000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

conflicts-historical-purge-delay

Description

This delay indicates the time (in minutes) the domain keeps the historical information necessary to solve conflicts.When a change stored in the historical part of the user entry has a date (from its replication ChangeNumber) older than this delay, it is candidate to be purged. The purge is applied on 2 events: modify of the entry, dedicated purge task.

Default Value

1440m

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 minutes.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-exclude

Description

Allows to exclude some attributes to replicate to this server. If fractional-exclude configuration attribute is used, attributes specified in this attribute will be ignored (not added/modified/deleted) when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-include attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be excluded. The object class may be "*" indicating that the attribute type(s) should be excluded regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-include

Description

Allows to include some attributes to replicate to this server. If fractional-include configuration attribute is used, only attributes specified in this attribute will be added/modified/deleted when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the

fractional-exclude attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be included. The object class may be "*" indicating that the attribute type(s) should be included regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group ID associated with this replicated domain. This value defines the group ID of the replicated domain. The replication system will preferably connect and send updates to replicate to a replication server with the same group ID as its own one (the local server group ID).

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when communicating with Replication Servers. The directory server expects a regular heart-beat coming from the Replication Server within the specified interval. If a heartbeat is not received within the interval, the Directory Server closes its connection and connects to another Replication Server.

Default Value

10000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 100 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

initialization-window-size

Description

Specifies the window size that this directory server may use when communicating with remote Directory Servers for initialization.

Default Value

100

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

isolation-policy

Description

Specifies the behavior of the directory server if a write operation is attempted on the data within the Replication Domain when none of the configured Replication Servers are available.

Default Value

reject-all-updates

Allowed Values

accept-all-updates

Indicates that updates should be accepted even though it is not possible to send them to any Replication Server. Best effort is made to re-send those updates to a Replication Servers when one of them is available, however those changes are at risk because they are only available from the historical information. This mode can also introduce high replication latency.

reject-all-updates

Indicates that all updates attempted on this Replication Domain are rejected when no Replication Server is available.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-changenumber

Description

Indicates if this server logs the ChangeNumber in access log. This boolean indicates if the domain should log the ChangeNumber of replicated operations in the access log.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

referrals-url

Description

The URLs other LDAP servers should use to refer to the local server. URLs used by peer servers in the topology to refer to the local server through LDAP referrals. If this attribute is not defined, every URLs available to access this server will be used. If defined, only URLs specified here will be used.

Default Value

None

Allowed Values

A LDAP URL compliant with RFC 2255.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of the Replication Servers within the Replication Domain to which the directory server should try to connect at startup time. Addresses must be specified using the syntax: hostname:port

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

server-id

Description

Specifies a unique identifier for the directory server within the Replication Domain. Each directory server within the same Replication Domain must have a different server ID. A directory server which is a member of multiple Replication Domains may use the same server ID for each of its Replication Domain configurations.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

solve-conflicts

Description

Indicates if this server solves conflict. This boolean indicates if this domain keeps the historical information necessary to solve conflicts. When set to false the server will not maintain historical information and will therefore not be able to solve conflict. This should therefore be done only if the replication is used in a single master type of deployment.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the directory server will use when communicating with Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-replication-server(1)

Name

dsconfig delete-replication-server - Deletes Replication Servers

Synopsis

`dsconfig delete-replication-server` {options}

Description

Deletes Replication Servers.

Options

The `dsconfig delete-replication-server` command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Server properties depend on the Replication Server type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

`replication-server`

Default {name}: Replication Server

Enabled by default: false

See Replication Server for the properties of this Replication Server type.

`-f | --force`

Ignore non-existent Replication Servers.

Replication Server properties depend on the Replication Server type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Replication Server types:

`replication-server`

Default null: Replication Server

Enabled by default: false

See Replication Server for the properties of this Replication Server type.

Replication Server

Replication Servers of type replication-server have the following properties:

assured-timeout

Description

The timeout value when waiting for assured mode acknowledgments. Defines the number of milliseconds that the replication server will wait for assured acknowledgments (in either Safe Data or Safe Read assured sub modes) before forgetting them and answer to the entity that sent an update and is waiting for acknowledgment.

Default Value

1000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compute-change-number

Description

Whether the replication server will compute change numbers. This boolean tells the replication server to compute change numbers for each replicated change by maintaining a change number index database. Changenumbers are computed according to http://tools.ietf.org/html/draft-good-ldap-changelog-04. Note this functionality has an impact on CPU, disk accesses and storage. If changenumbers are not required, it is advisable to set this value to false.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the replication change-log should make records readable only by Directory Server. Throughput and disk space are affected by the more expensive operations taking place. Confidentiality is achieved by encrypting records on all domains managed by this replication server. Encrypting the records prevents unauthorized parties from accessing contents of LDAP operations. For complete protection, consider enabling secure communications between servers. Change number indexing is not affected by the setting.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect operations performed after the change.

Advanced Property

No

Read-only

No

degraded-status-threshold

Description

The number of pending changes as threshold value for putting a directory server in degraded status. This value represents a number of pending changes a replication server has in queue for sending to a directory server. Once this value is crossed, the matching directory server goes in degraded status. When number of pending changes goes back under this value, the directory server is put back in normal status. 0 means status analyzer is disabled and directory servers are never put in degraded status.

Default Value

5000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group id for the replication server. This value defines the group id of the replication server.

The replication system of a LDAP server uses the group id of the replicated domain and tries to connect, if possible, to a replication with the same group id.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

monitoring-period

Description

The period between sending of monitoring messages. Defines the duration that the replication server will wait before sending new monitoring messages to its peers (replication servers and directory servers). Larger values increase the length of time it takes for a directory server to detect and switch to a more suitable replication server, whereas smaller values increase the amount of background network traffic.

Default Value

60s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

Specifies the number of changes that are kept in memory for each directory server in the Replication Domain.

Default Value

10000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

replication-db-directory

Description

The path where the Replication Server stores all persistent information.

Default Value

changelogDb

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

replication-port

Description

The port on which this Replication Server waits for connections from other Replication Servers or Directory Servers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-purge-delay

Description

The time (in seconds) after which the Replication Server erases all persistent information.

Default Value

3 days

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of other Replication Servers to which this Replication Server tries to connect at startup time. Addresses must be specified using the syntax: "hostname:port". If IPv6 addresses are used as the hostname, they must be specified using the syntax "[IPv6Address]:port".

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server-id

Description

Specifies a unique identifier for the Replication Server. Each Replication Server must have a different server ID.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

weight

Description

The weight of the replication server. The weight affected to the replication server. Each replication server of the topology has a weight. When combined together, the weights of the replication servers of a same group can be translated to a percentage that determines the quantity of directory servers of the topology that should be connected to a replication server. For instance imagine a topology with 3 replication servers (with the same group id) with the following weights: RS1=1, RS2=1, RS3=2. This means that RS1 should have 25% of the directory servers connected in the topology, RS2 25%, and RS3 50%. This may be useful if the replication servers of the topology have a different power and one wants to spread the load between the replication servers according to their power.

Default Value

1

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the Replication Server uses when communicating with other Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-sasl-mechanism-handler(1)

Name

dsconfig delete-sasl-mechanism-handler - Deletes SASL Mechanism Handlers

Synopsis

`dsconfig delete-sasl-mechanism-handler` {options}

Description

Deletes SASL Mechanism Handlers.

Options

The `dsconfig delete-sasl-mechanism-handler` command takes the following options:

`--handler-name {name}`

The name of the SASL Mechanism Handler.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

`anonymous-sasl-mechanism-handler`

Default {name}: Anonymous SASL Mechanism Handler

Enabled by default: true

See Anonymous SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`cram-md5-sasl-mechanism-handler`

Default {name}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See Cram MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`digest-md5-sasl-mechanism-handler`

Default {name}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See Digest MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler

type.

`external-sasl-mechanism-handler`

Default {name}: External SASL Mechanism Handler

Enabled by default: true

See External SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`gssapi-sasl-mechanism-handler`

Default {name}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See GSSAPI SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`plain-sasl-mechanism-handler`

Default {name}: Plain SASL Mechanism Handler

Enabled by default: true

See Plain SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`-f | --force`

Ignore non-existent SASL Mechanism Handlers.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

`anonymous-sasl-mechanism-handler`

Default null: Anonymous SASL Mechanism Handler

Enabled by default: true

See Anonymous SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`cram-md5-sasl-mechanism-handler`

Default null: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See Cram MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`digest-md5-sasl-mechanism-handler`

Default null: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See Digest MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`external-sasl-mechanism-handler`

Default null: External SASL Mechanism Handler

Enabled by default: true

See External SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`gssapi-sasl-mechanism-handler`

Default null: GSSAPI SASL Mechanism Handler

Enabled by default: true

See GSSAPI SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`plain-sasl-mechanism-handler`

Default null: Plain SASL Mechanism Handler

Enabled by default: true

See Plain SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

Anonymous SASL Mechanism Handler

SASL Mechanism Handlers of type anonymous-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.AnonymousSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Cram MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type cram-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper used with this SASL mechanism handler to match the authentication ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Cram MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.CRAMMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Digest MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type digest-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Digest MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.DigestMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realms that is to be used by the server for DIGEST-MD5 authentication. If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Default Value

If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Allowed Values

Any realm string that does not contain a comma.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the server that is used when validating the digest-uri parameter during the authentication process. If this configuration attribute is present, then the server expects that clients use a digest-uri equal to "ldap/" followed by the value of this attribute. For example, if the attribute has a value of "directory.example.com", then the server expects clients to use a digest-uri of "ldap/directory.example.com". If no value is provided, then the server does not attempt to validate the digest-uri provided by the client and accepts any value.

Default Value

The server attempts to determine the fully-qualified domain name dynamically.

Allowed Values

The fully-qualified address that is expected for clients to use when connecting to the server and authenticating via DIGEST-MD5.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

External SASL Mechanism Handler

SASL Mechanism Handlers of type external-sasl-mechanism-handler have the following properties:

certificate-attribute

Description

Specifies the name of the attribute to hold user certificates. This property must specify the name of a valid attribute type defined in the server schema.

Default Value

userCertificate

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-mapper

Description

Specifies the name of the certificate mapper that should be used to match client certificates to user entries.

Default Value

None

Allowed Values

The DN of any Certificate Mapper. The referenced certificate mapper must be enabled when the External SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-validation-policy

Description

Indicates whether to attempt to validate the peer certificate against a certificate held in the user's entry.

Default Value

None

Allowed Values

always

Always require the peer certificate to be present in the user’s entry.

ifpresent

If the user's entry contains one or more certificates, require that one of them match the peer certificate.

never

Do not look for the peer certificate to be present in the user's entry.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.ExternalSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

GSSAPI SASL Mechanism Handler

SASL Mechanism Handlers of type gssapi-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the Kerberos principal included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the GSSAPI SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.GSSAPISASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

kdc-address

Description

Specifies the address of the KDC that is to be used for Kerberos processing. If provided, this property must be a fully-qualified DNS-resolvable name. If this property is not provided, then the server attempts to determine it from the system-wide Kerberos configuration.

Default Value

The server attempts to determine the KDC address from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

keytab

Description

Specifies the path to the keytab file that should be used for Kerberos processing. If provided, this is either an absolute path or one that is relative to the server instance root.

Default Value

The server attempts to use the system-wide default keytab.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

principal-name

Description

Specifies the principal name. It can either be a simple user name or a service name such as host/example.com. If this property is not provided, then the server attempts to build the principal name by appending the fully qualified domain name to the string "ldap/".

Default Value

The server attempts to determine the principal name from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realm to be used for GSSAPI authentication.

Default Value

The server attempts to determine the realm from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the system.

Default Value

The server attempts to determine the fully-qualified domain name dynamically .

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Plain SASL Mechanism Handler

SASL Mechanism Handlers of type plain-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Plain SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.PlainSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-schema-provider(1)

Name

dsconfig delete-schema-provider - Deletes Schema Providers

Synopsis

`dsconfig delete-schema-provider` {options}

Description

Deletes Schema Providers.

Options

The `dsconfig delete-schema-provider` command takes the following options:

`--provider-name {name}`

The name of the Schema Provider.

Schema Provider properties depend on the Schema Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

`core-schema`

Default {name}: Core Schema

Enabled by default: true

See Core Schema for the properties of this Schema Provider type.

`json-schema`

Default {name}: Json Schema

Enabled by default: true

See Json Schema for the properties of this Schema Provider type.

`-f | --force`

Ignore non-existent Schema Providers.

Schema Provider properties depend on the Schema Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

`core-schema`

Default null: Core Schema

Enabled by default: true

See Core Schema for the properties of this Schema Provider type.

`json-schema`

Default null: Json Schema

Enabled by default: true

See Json Schema for the properties of this Schema Provider type.

Core Schema

Schema Providers of type core-schema have the following properties:

allow-attribute-types-with-no-sup-or-syntax

Description

Indicates whether the schema should allow attribute type definitions that do not declare a superior attribute type or syntax When set to true, invalid attribute type definitions will use the default syntax.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-zero-length-values-directory-string

Description

Indicates whether zero-length (that is, an empty string) values are allowed for directory string. This is technically not allowed by the revised LDAPv3 specification, but some environments may require it for backward compatibility with servers that do allow it.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disabled-matching-rule

Description

The set of disabled matching rules. Matching rules must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled matching rule.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

disabled-syntax

Description

The set of disabled syntaxes. Syntaxes must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled syntax, or NONE

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Core Schema implementation.

Default Value

org.opends.server.schema.CoreSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

json-validation-policy

Description

Specifies the policy that will be used when validating JSON syntax values.

Default Value

strict

Allowed Values

disabled

JSON syntax values will not be validated and, as a result any sequence of bytes will be acceptable.

lenient

JSON syntax values must comply with RFC 7159 except: 1) comments are allowed, 2) single quotes may be used instead of double quotes, and 3) unquoted control characters are allowed in strings.

strict

JSON syntax values must strictly conform to RFC 7159.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-certificates

Description

Indicates whether X.509 Certificate values are required to strictly comply with the standard definition for this syntax. When set to false, certificates will not be validated and, as a result any sequence of bytes will be acceptable.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-country-string

Description

Indicates whether country code values are required to strictly comply with the standard definition for this syntax. When set to false, country codes will not be validated and, as a result any string containing 2 characters will be acceptable.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-jpeg-photos

Description

Indicates whether to require JPEG values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-telephone-numbers

Description

Indicates whether to require telephone number values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strip-syntax-min-upper-bound-attribute-type-description

Description

Indicates whether the suggested minimum upper bound appended to an attribute's syntax OID in it's schema definition Attribute Type Description is stripped off. When retrieving the server's schema, some APIs (JNDI) fail in their syntax lookup methods, because they do not parse this

value correctly. This configuration option allows the server to be configured to provide schema definitions these APIs can parse correctly.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Json Schema

Schema Providers of type json-schema have the following properties:

case-sensitive-strings

Description

Indicates whether JSON string comparisons should be case-sensitive.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ignore-white-space

Description

Indicates whether JSON string comparisons should ignore white-space. When enabled all leading and trailing white space will be removed and intermediate white space will be reduced to a single character.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

indexed-field

Description

Specifies which JSON fields should be indexed. A field will be indexed if it matches any of the configured field patterns.

Default Value

All JSON fields will be indexed.

Allowed Values

A JSON pointer which may include wild-cards. A single **'** **wild-card matches at most a single path element, whereas a double** **'*'** matches zero or more path elements.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Json Schema implementation.

Default Value

org.opends.server.schema.JsonSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

matching-rule-name

Description

The name of the custom JSON matching rule.

Default Value

The matching rule will not have a name.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

matching-rule-oid

Description

The numeric OID of the custom JSON matching rule.

Default Value

None

Allowed Values

The OID of the matching rule.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-service-discovery-mechanism(1)

Name

dsconfig delete-service-discovery-mechanism - Deletes Service Discovery Mechanisms

Synopsis

`dsconfig delete-service-discovery-mechanism` {options}

Description

Deletes Service Discovery Mechanisms.

Options

The `dsconfig delete-service-discovery-mechanism` command takes the following options:

`--mechanism-name {name}`

The name of the Service Discovery Mechanism.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

`replication-service-discovery-mechanism`

Default {name}: Replication Service Discovery Mechanism

Enabled by default: false

See Replication Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`static-service-discovery-mechanism`

Default {name}: Static Service Discovery Mechanism

Enabled by default: false

See Static Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`-f | --force`

Ignore non-existent Service Discovery Mechanisms.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type,

which depends on the null you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

`replication-service-discovery-mechanism`

Default null: Replication Service Discovery Mechanism

Enabled by default: false

See Replication Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`static-service-discovery-mechanism`

Default null: Static Service Discovery Mechanism

Enabled by default: false

See Static Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

Replication Service Discovery Mechanism

Service Discovery Mechanisms of type replication-service-discovery-mechanism have the following properties:

bind-dn

Description

The bind DN for periodically reading replication server configurations The bind DN must be present on all replication servers and directory servers, it must be able to read the server configuration.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

bind-password

Description

The bind password for periodically reading replication server configurations The bind password must be the same on all replication and directory servers

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

discovery-interval

Description

Interval between two replication server configuration discovery queries. Specifies how frequently to query a replication server configuration in order to discover information about available directory server replicas.

Default Value

60s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.ReplicationServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-group-id

Description

Replication domain group ID of preferred directory server replicas. Directory server replicas with this replication domain group ID will be preferred over other directory server replicas. Secondary server replicas will only be used when all primary server replicas become unavailable.

Default Value

All the server replicas will be treated the same.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the list of replication servers to contact periodically when discovering server replicas.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

Static Service Discovery Mechanism

Service Discovery Mechanisms of type static-service-discovery-mechanism have the following properties:

discovery-interval

Description

Interval between two server configuration discovery executions. Specifies how frequently to read the configuration of the servers in order to discover their new information.

Default Value

60s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.StaticServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-server

Description

Specifies a list of servers that will be used in preference to secondary servers when available.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-server

Description

Specifies a list of servers that will be used in place of primary servers when all primary servers are unavailable.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled

when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig delete-synchronization-provider(1)

Name

dsconfig delete-synchronization-provider - Deletes Synchronization Providers

Synopsis

`dsconfig delete-synchronization-provider` {options}

Description

Deletes Synchronization Providers.

Options

The `dsconfig delete-synchronization-provider` command takes the following options:

`--provider-name {name}`

The name of the Synchronization Provider.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

`replication-synchronization-provider`

Default {name}: Replication Synchronization Provider

Enabled by default: true

See Replication Synchronization Provider for the properties of this Synchronization Provider type.

`-f | --force`

Ignore non-existent Synchronization Providers.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

`replication-synchronization-provider`

Default null: Replication Synchronization Provider

Enabled by default: true

See Replication Synchronization Provider for the properties of this Synchronization Provider

type.

Replication Synchronization Provider

Synchronization Providers of type replication-synchronization-provider have the following properties:

connection-timeout

Description

Specifies the timeout used when connecting to peers and when performing SSL negotiation.

Default Value

5 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Synchronization Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Synchronization Provider implementation.

Default Value

org.opends.server.replication.plugin.MultimasterReplication

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SynchronizationProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-update-replay-threads

Description

Specifies the number of update replay threads. This value is the number of threads created for replaying every updates received for all the replication domains.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-trust-manager-provider(1)

Name

dsconfig delete-trust-manager-provider - Deletes Trust Manager Providers

Synopsis

`dsconfig delete-trust-manager-provider` {options}

Description

Deletes Trust Manager Providers.

Options

The `dsconfig delete-trust-manager-provider` command takes the following options:

`--provider-name {name}`

The name of the Trust Manager Provider.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

`blind-trust-manager-provider`

Default {name}: Blind Trust Manager Provider

Enabled by default: true

See Blind Trust Manager Provider for the properties of this Trust Manager Provider type.

`file-based-trust-manager-provider`

Default {name}: File Based Trust Manager Provider

Enabled by default: true

See File Based Trust Manager Provider for the properties of this Trust Manager Provider type.

`ldap-trust-manager-provider`

Default {name}: LDAP Trust Manager Provider

Enabled by default: true

See LDAP Trust Manager Provider for the properties of this Trust Manager Provider type.

`pkcs11-trust-manager-provider`

Default {name}: PKCS11 Trust Manager Provider

Enabled by default: true

See PKCS11 Trust Manager Provider for the properties of this Trust Manager Provider type.

`-f | --force`

Ignore non-existent Trust Manager Providers.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

`blind-trust-manager-provider`

Default null: Blind Trust Manager Provider

Enabled by default: true

See Blind Trust Manager Provider for the properties of this Trust Manager Provider type.

`file-based-trust-manager-provider`

Default null: File Based Trust Manager Provider

Enabled by default: true

See File Based Trust Manager Provider for the properties of this Trust Manager Provider type.

`ldap-trust-manager-provider`

Default null: LDAP Trust Manager Provider

Enabled by default: true

See LDAP Trust Manager Provider for the properties of this Trust Manager Provider type.

`pkcs11-trust-manager-provider`

Default null: PKCS11 Trust Manager Provider

Enabled by default: true

See PKCS11 Trust Manager Provider for the properties of this Trust Manager Provider type.

Blind Trust Manager Provider

Trust Manager Providers of type blind-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Blind Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.BlindTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Trust Manager Provider

Trust Manager Providers of type file-based-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file containing the trust information. It can be an absolute path or a path that is relative to the OpenDJ instance root. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

An absolute path or a path that is relative to the OpenDJ directory server instance root.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the trust store file. Valid values always include 'JKS' and 'PKCS12', but different implementations can allow other values as well. If no value is provided, then the JVM default value is used. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment. The "JKS" and "PKCS12" formats are typically available in Java environments.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

LDAP Trust Manager Provider

Trust Manager Providers of type ldap-trust-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager

Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

PKCS11 Trust Manager Provider

Trust Manager Providers of type pkcs11-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11TrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig delete-virtual-attribute(1)

Name

dsconfig delete-virtual-attribute - Deletes Virtual Attributes

Synopsis

`dsconfig delete-virtual-attribute` {options}

Description

Deletes Virtual Attributes.

Options

The `dsconfig delete-virtual-attribute` command takes the following options:

`--name {name}`

The name of the Virtual Attribute.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

`collective-attribute-subentries-virtual-attribute`

Default {name}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See Collective Attribute Subentries Virtual Attribute for the properties of this Virtual Attribute type.

`entity-tag-virtual-attribute`

Default {name}: Entity Tag Virtual Attribute

Enabled by default: true

See Entity Tag Virtual Attribute for the properties of this Virtual Attribute type.

`entry-dn-virtual-attribute`

Default {name}: Entry DN Virtual Attribute

Enabled by default: true

See Entry DN Virtual Attribute for the properties of this Virtual Attribute type.

`entry-uuid-virtual-attribute`

Default {name}: Entry UUID Virtual Attribute

Enabled by default: true

See Entry UUID Virtual Attribute for the properties of this Virtual Attribute type.

`governing-structure-rule-virtual-attribute`

Default {name}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See Governing Structure Rule Virtual Attribute for the properties of this Virtual Attribute type.

`has-subordinates-virtual-attribute`

Default {name}: Has Subordinates Virtual Attribute

Enabled by default: true

See Has Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`is-member-of-virtual-attribute`

Default {name}: Is Member Of Virtual Attribute

Enabled by default: true

See Is Member Of Virtual Attribute for the properties of this Virtual Attribute type.

`member-virtual-attribute`

Default {name}: Member Virtual Attribute

Enabled by default: true

See Member Virtual Attribute for the properties of this Virtual Attribute type.

`num-subordinates-virtual-attribute`

Default {name}: Num Subordinates Virtual Attribute

Enabled by default: true

See Num Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`password-expiration-time-virtual-attribute`

Default {name}: Password Expiration Time Virtual Attribute

Enabled by default: true

See Password Expiration Time Virtual Attribute for the properties of this Virtual Attribute type.

`password-policy-subentry-virtual-attribute`

Default {name}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See Password Policy Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`structural-object-class-virtual-attribute`

Default {name}: Structural Object Class Virtual Attribute

Enabled by default: true

See Structural Object Class Virtual Attribute for the properties of this Virtual Attribute type.

`subschema-subentry-virtual-attribute`

Default {name}: Subschema Subentry Virtual Attribute

Enabled by default: true

See Subschema Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`user-defined-virtual-attribute`

Default {name}: User Defined Virtual Attribute

Enabled by default: true

See User Defined Virtual Attribute for the properties of this Virtual Attribute type.

`-f | --force`

Ignore non-existent Virtual Attributes.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

`collective-attribute-subentries-virtual-attribute`

Default null: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See Collective Attribute Subentries Virtual Attribute for the properties of this Virtual Attribute type.

`entity-tag-virtual-attribute`

Default null: Entity Tag Virtual Attribute

Enabled by default: true

See Entity Tag Virtual Attribute for the properties of this Virtual Attribute type.

`entry-dn-virtual-attribute`

Default null: Entry DN Virtual Attribute

Enabled by default: true

See Entry DN Virtual Attribute for the properties of this Virtual Attribute type.

`entry-uuid-virtual-attribute`

Default null: Entry UUID Virtual Attribute

Enabled by default: true

See Entry UUID Virtual Attribute for the properties of this Virtual Attribute type.

`governing-structure-rule-virtual-attribute`

Default null: Governing Structure Rule Virtual Attribute

Enabled by default: true

See Governing Structure Rule Virtual Attribute for the properties of this Virtual Attribute type.

`has-subordinates-virtual-attribute`

Default null: Has Subordinates Virtual Attribute

Enabled by default: true

See Has Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`is-member-of-virtual-attribute`

Default null: Is Member Of Virtual Attribute

Enabled by default: true

See Is Member Of Virtual Attribute for the properties of this Virtual Attribute type.

`member-virtual-attribute`

Default null: Member Virtual Attribute

Enabled by default: true

See Member Virtual Attribute for the properties of this Virtual Attribute type.

`num-subordinates-virtual-attribute`

Default null: Num Subordinates Virtual Attribute

Enabled by default: true

See Num Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`password-expiration-time-virtual-attribute`

Default null: Password Expiration Time Virtual Attribute

Enabled by default: true

See Password Expiration Time Virtual Attribute for the properties of this Virtual Attribute type.

`password-policy-subentry-virtual-attribute`

Default null: Password Policy Subentry Virtual Attribute

Enabled by default: true

See Password Policy Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`structural-object-class-virtual-attribute`

Default null: Structural Object Class Virtual Attribute

Enabled by default: true

See Structural Object Class Virtual Attribute for the properties of this Virtual Attribute type.

`subschema-subentry-virtual-attribute`

Default null: Subschema Subentry Virtual Attribute

Enabled by default: true

See Subschema Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`user-defined-virtual-attribute`

Default null: User Defined Virtual Attribute

Enabled by default: true

See User Defined Virtual Attribute for the properties of this Virtual Attribute type.

Collective Attribute Subentries Virtual Attribute

Virtual Attributes of type collective-attribute-subentries-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

collectiveAttributeSubentries

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no

values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.CollectiveAttributeSubentriesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Entity Tag Virtual Attribute

Virtual Attributes of type entity-tag-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

etag

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

checksum-algorithm

Description

The algorithm which should be used for calculating the entity tag checksum value.

Default Value

adler-32

Allowed Values

adler-32

The Adler-32 checksum algorithm which is almost as reliable as a CRC-32 but can be computed much faster.

crc-32

The CRC-32 checksum algorithm.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

excluded-attribute

Description

The list of attributes which should be ignored when calculating the entity tag checksum value. Certain attributes like "ds-sync-hist" may vary between replicas due to different purging schedules and should not be included in the checksum.

Default Value

ds-sync-hist

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntityTagVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Entry DN Virtual Attribute

Virtual Attributes of type entry-dn-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryDN

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry

and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those

filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryDNVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Entry UUID Virtual Attribute

Virtual Attributes of type entry-uuid-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryUUID

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryUUIDVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Governing Structure Rule Virtual Attribute

Virtual Attributes of type governing-structure-rule-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

governingStructureRule

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no

values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.GoverningSturctureRuleVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Has Subordinates Virtual Attribute

Virtual Attributes of type has-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

hasSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.HasSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Is Member Of Virtual Attribute

Virtual Attributes of type is-member-of-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

isMemberOf

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.IsMemberOfVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Member Virtual Attribute

Virtual Attributes of type member-virtual-attribute have the following properties:

allow-retrieving-membership

Description

Indicates whether to handle requests that request all values for the virtual attribute. This operation can be very expensive in some cases and is not consistent with the primary function of virtual static groups, which is to make it possible to use static group idioms to determine whether a given user is a member. If this attribute is set to false, attempts to retrieve the entire set of values receive an empty set, and only attempts to determine whether the attribute has a specific value or set of values (which is the primary anticipated use for virtual static groups) are handled properly.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.MemberVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Num Subordinates Virtual Attribute

Virtual Attributes of type num-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

numSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.NumSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Password Expiration Time Virtual Attribute

Virtual Attributes of type password-expiration-time-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

ds-pwp-password-expiration-time

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordExpirationTimeVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Password Policy Subentry Virtual Attribute

Virtual Attributes of type password-policy-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

pwdPolicySubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to

use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordPolicySubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Structural Object Class Virtual Attribute

Virtual Attributes of type structural-object-class-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

structuralObjectClass

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no

values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.StructuralObjectClassVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subschema Subentry Virtual Attribute

Virtual Attributes of type subschema-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

subschemaSubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.SubschemaSubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

User Defined Virtual Attribute

Virtual Attributes of type user-defined-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.UserDefinedVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

value

Description

Specifies the values to be included in the virtual attribute.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-access-control-handler-prop(1)

Name

dsconfig get-access-control-handler-prop - Shows Access Control Handler properties

Synopsis

`dsconfig get-access-control-handler-prop` {options}

Description

Shows Access Control Handler properties.

Options

The `dsconfig get-access-control-handler-prop` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Access Control Handler properties depend on the Access Control Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Access Control Handler types:

`dsee-compat-access-control-handler`

Default {property}: Dsee Compat Access Control Handler

Enabled by default: true

See Dsee Compat Access Control Handler for the properties of this Access Control Handler type.

`-E | --record`

Modifies the display output to show one property value per line.

Access Control Handler properties depend on the Access Control Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Access Control Handler types:

`dsee-compat-access-control-handler`

Default null: Dsee Compat Access Control Handler

Enabled by default: true

See Dsee Compat Access Control Handler for the properties of this Access Control Handler

type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Access Control Handler properties depend on the Access Control Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Access Control Handler types:

`dsee-compat-access-control-handler`

Default {unit}: Dsee Compat Access Control Handler

Enabled by default: true

See Dsee Compat Access Control Handler for the properties of this Access Control Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Access Control Handler properties depend on the Access Control Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Access Control Handler types:

`dsee-compat-access-control-handler`

Default {unit}: Dsee Compat Access Control Handler

Enabled by default: true

See Dsee Compat Access Control Handler for the properties of this Access Control Handler type.

Dsee Compat Access Control Handler

Access Control Handlers of type dsee-compat-access-control-handler have the following properties:

enabled

Description

Indicates whether the Access Control Handler is enabled. If set to FALSE, then no access control is enforced, and any client (including unauthenticated or anonymous clients) could be allowed to perform any operation if not subject to other restrictions, such as those enforced by the privilege subsystem.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

global-aci

Description

Defines global access control rules. Global access control rules apply to all entries anywhere in the data managed by the OpenDJ directory server. The global access control rules may be overridden by more specific access control rules placed in the data.

Default Value

No global access control rules are defined, which means that no access is allowed for any data in the server unless specifically granted by access control rules in the data.

Allowed Values

<olink targetdoc="admin-guide" targetptr="about-acis" />

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Dsee Compat Access Control Handler implementation.

Default Value

org.opends.server.authorization.dseecompat.AciHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccessControlHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Access Control Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-access-log-filtering-criteria-prop(1)

Name

dsconfig get-access-log-filtering-criteria-prop - Shows Access Log Filtering Criteria properties

Synopsis

`dsconfig get-access-log-filtering-criteria-prop` {options}

Description

Shows Access Log Filtering Criteria properties.

Options

The `dsconfig get-access-log-filtering-criteria-prop` command takes the following options:

`--publisher-name {name}`

The name of the Access Log Publisher.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

`--criteria-name {name}`

The name of the Access Log Filtering Criteria.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

`--property {property}`

The name of a property to be displayed.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default {property}: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

`-E | --record`

Modifies the display output to show one property value per line.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default null: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default {unit}: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default {unit}: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

Access Log Filtering Criteria

Access Log Filtering Criteria of type access-log-filtering-criteria have the following properties:

connection-client-address-equal-to

Description

Filters log records associated with connections which match at least one of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-client-address-not-equal-to

Description

Filters log records associated with connections which do not match any of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a

domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-port-equal-to

Description

Filters log records associated with connections to any of the specified listener port numbers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-protocol-equal-to

Description

Filters log records associated with connections which match any of the specified protocols. Typical values include "ldap", "ldaps", or "jmx".

Default Value

None

Allowed Values

The protocol name as reported in the access log.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-type

Description

Filters log records based on their type.

Default Value

None

Allowed Values

abandon

Abandon operations

add

Add operations

bind

Bind operations

compare

Compare operations

connect

Client connections

delete

Delete operations

disconnect

Client disconnections

extended

Extended operations

modify

Modify operations

rename

Rename operations

search

Search operations

unbind

Unbind operations

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-equal-to

Description

Filters operation log records associated with operations which target entries matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-not-equal-to

Description

Filters operation log records associated with operations which target entries matching none of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-greater-than

Description

Filters operation response log records associated with operations which took longer than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-less-than

Description

Filters operation response log records associated with operations which took less than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-equal-to

Description

Filters operation response log records associated with operations which include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-not-equal-to

Description

Filters operation response log records associated with operations which do not include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-is-indexed

Description

Filters search operation response log records associated with searches which were either indexed or unindexed. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-greater-than

Description

Filters search operation response log records associated with searches which returned more than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-less-than

Description

Filters search operation response log records associated with searches which returned less than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-equal-to

Description

Filters log records associated with users matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-not-equal-to

Description

Filters log records associated with users which do not match any of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard *

replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-member-of

Description

Filters log records associated with users which are members of at least one of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-not-member-of

Description

Filters log records associated with users which are not members of any of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-account-status-notification-handler-prop(1)

Name

dsconfig get-account-status-notification-handler-prop - Shows Account Status Notification Handler properties

Synopsis

`dsconfig get-account-status-notification-handler-prop` {options}

Description

Shows Account Status Notification Handler properties.

Options

The `dsconfig get-account-status-notification-handler-prop` command takes the following options:

`--handler-name {name}`

The name of the Account Status Notification Handler.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

`error-log-account-status-notification-handler`

Default {name}: Error Log Account Status Notification Handler

Enabled by default: true

See Error Log Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`smtp-account-status-notification-handler`

Default {name}: SMTP Account Status Notification Handler

Enabled by default: true

See SMTP Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`--property {property}`

The name of a property to be displayed.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

`error-log-account-status-notification-handler`

Default {property}: Error Log Account Status Notification Handler

Enabled by default: true

See Error Log Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`smtp-account-status-notification-handler`

Default {property}: SMTP Account Status Notification Handler

Enabled by default: true

See SMTP Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`-E | --record`

Modifies the display output to show one property value per line.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

`error-log-account-status-notification-handler`

Default null: Error Log Account Status Notification Handler

Enabled by default: true

See Error Log Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`smtp-account-status-notification-handler`

Default null: SMTP Account Status Notification Handler

Enabled by default: true

See SMTP Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

`error-log-account-status-notification-handler`

Default {unit}: Error Log Account Status Notification Handler

Enabled by default: true

See Error Log Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`smtp-account-status-notification-handler`

Default {unit}: SMTP Account Status Notification Handler

Enabled by default: true

See SMTP Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

`error-log-account-status-notification-handler`

Default {unit}: Error Log Account Status Notification Handler

Enabled by default: true

See Error Log Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`smtp-account-status-notification-handler`

Default {unit}: SMTP Account Status Notification Handler

Enabled by default: true

See SMTP Account Status Notification Handler for the properties of this Account Status

Notification Handler type.

Error Log Account Status Notification Handler

Account Status Notification Handlers of type error-log-account-status-notification-handler have the following properties:

account-status-notification-type

Description

Indicates which types of event can trigger an account status notification.

Default Value

None

Allowed Values

account-disabled

Generate a notification whenever a user account has been disabled by an administrator.

account-enabled

Generate a notification whenever a user account has been enabled by an administrator.

account-expired

Generate a notification whenever a user authentication has failed because the account has expired.

account-idle-locked

Generate a notification whenever a user account has been locked because it was idle for too long.

account-permanently-locked

Generate a notification whenever a user account has been permanently locked after too many failed attempts.

account-reset-locked

Generate a notification whenever a user account has been locked, because the password had been reset by an administrator but not changed by the user within the required interval.

account-temporarily-locked

Generate a notification whenever a user account has been temporarily locked after too many failed attempts.

account-unlocked

Generate a notification whenever a user account has been unlocked by an administrator.

password-changed

Generate a notification whenever a user changes his/her own password.

password-expired

Generate a notification whenever a user authentication has failed because the password has expired.

password-expiring

Generate a notification whenever a password expiration warning is encountered for a user password for the first time.

password-reset

Generate a notification whenever a user's password is reset by an administrator.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Error Log Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.ErrorLogAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

SMTP Account Status Notification Handler

Account Status Notification Handlers of type smtp-account-status-notification-handler have the following properties:

email-address-attribute-type

Description

Specifies which attribute in the user's entries may be used to obtain the email address when notifying the end user. You can specify more than one email address as separate values. In this case, the OpenDJ server sends a notification to all email addresses identified.

Default Value

If no email address attribute types are specified, then no attempt is made to send email notification messages to end users. Only those users specified in the set of additional recipient addresses are sent the notification messages.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.SMTPAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this account status notification handler. The values for this property should begin with the name of an account status notification type followed by a colon and the subject that should be used for the associated notification message. If an email message is generated for an account status notification type for which no subject is defined, then that message is given a generic subject.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-template-file

Description

Specifies the path to the file containing the message template to generate the email notification messages. The values for this property should begin with the name of an account status notification type followed by a colon and the path to the template file that should be used for that notification type. If an account status notification has a notification type that is not associated with a message template file, then no email message is generated for that notification.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which notification messages are sent, either instead of or in addition to the end user for whom the notification has been generated. This may be used to ensure that server administrators also receive a copy of any notification messages that are generated.

Default Value

If no additional recipient addresses are specified, then only the end users that are the subjects of the account status notifications receive the notification messages.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

send-email-as-html

Description

Indicates whether an email notification message should be sent as HTML. If this value is true, email notification messages are marked as text/html. Otherwise outgoing email messages are assumed to be plaintext and marked as text/plain.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-message-without-end-user-address

Description

Indicates whether an email notification message should be generated and sent to the set of notification recipients even if the user entry does not contain any values for any of the email address attributes (that is, in cases when it is not be possible to notify the end user). This is only applicable if both one or more email address attribute types and one or more additional recipient addresses are specified.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

sender-address

Description

Specifies the email address from which the message is sent. Note that this does not necessarily have to be a legitimate email address.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-administration-connector-prop(1)

Name

dsconfig get-administration-connector-prop - Shows Administration Connector properties

Synopsis

`dsconfig get-administration-connector-prop` {options}

Description

Shows Administration Connector properties.

Options

The `dsconfig get-administration-connector-prop` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Administration Connector properties depend on the Administration Connector type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Administration Connector types:

`administration-connector`

Default {property}: Administration Connector

Enabled by default: false

See Administration Connector for the properties of this Administration Connector type.

`-E | --record`

Modifies the display output to show one property value per line.

Administration Connector properties depend on the Administration Connector type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Administration Connector types:

`administration-connector`

Default null: Administration Connector

Enabled by default: false

See Administration Connector for the properties of this Administration Connector type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Administration Connector properties depend on the Administration Connector type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Administration Connector types:

`administration-connector`

Default {unit}: Administration Connector

Enabled by default: false

See Administration Connector for the properties of this Administration Connector type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Administration Connector properties depend on the Administration Connector type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Administration Connector types:

`administration-connector`

Default {unit}: Administration Connector

Enabled by default: false

See Administration Connector for the properties of this Administration Connector type.

Administration Connector

Administration Connectors of type administration-connector have the following properties:

key-manager-provider

Description

Specifies the name of the key manager that is used with the Administration Connector .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

Yes

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this Administration Connector should listen for connections from LDAP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the Administration Connector listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the Administration Connector will listen for connections

from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Administration Connector must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Administration Connector should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that is used with the Administration Connector .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

dsconfig get-alert-handler-prop(1)

Name

dsconfig get-alert-handler-prop - Shows Alert Handler properties

Synopsis

`dsconfig get-alert-handler-prop` {options}

Description

Shows Alert Handler properties.

Options

The `dsconfig get-alert-handler-prop` command takes the following options:

`--handler-name {name}`

The name of the Alert Handler.

Alert Handler properties depend on the Alert Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

`jmx-alert-handler`

Default {name}: JMX Alert Handler

Enabled by default: true

See JMX Alert Handler for the properties of this Alert Handler type.

`smtp-alert-handler`

Default {name}: SMTP Alert Handler

Enabled by default: true

See SMTP Alert Handler for the properties of this Alert Handler type.

`--property {property}`

The name of a property to be displayed.

Alert Handler properties depend on the Alert Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

`jmx-alert-handler`

Default {property}: JMX Alert Handler

Enabled by default: true

See JMX Alert Handler for the properties of this Alert Handler type.

`smtp-alert-handler`

Default {property}: SMTP Alert Handler

Enabled by default: true

See SMTP Alert Handler for the properties of this Alert Handler type.

`-E | --record`

Modifies the display output to show one property value per line.

Alert Handler properties depend on the Alert Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

`jmx-alert-handler`

Default null: JMX Alert Handler

Enabled by default: true

See JMX Alert Handler for the properties of this Alert Handler type.

`smtp-alert-handler`

Default null: SMTP Alert Handler

Enabled by default: true

See SMTP Alert Handler for the properties of this Alert Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Alert Handler properties depend on the Alert Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

`jmx-alert-handler`

Default {unit}: JMX Alert Handler

Enabled by default: true

See JMX Alert Handler for the properties of this Alert Handler type.

`smtp-alert-handler`

Default {unit}: SMTP Alert Handler

Enabled by default: true

See SMTP Alert Handler for the properties of this Alert Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Alert Handler properties depend on the Alert Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

`jmx-alert-handler`

Default {unit}: JMX Alert Handler

Enabled by default: true

See JMX Alert Handler for the properties of this Alert Handler type.

`smtp-alert-handler`

Default {unit}: SMTP Alert Handler

Enabled by default: true

See SMTP Alert Handler for the properties of this Alert Handler type.

JMX Alert Handler

Alert Handlers of type jmx-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Alert Handler implementation.

Default Value

org.opends.server.extensions.JMXAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

SMTP Alert Handler

Alert Handlers of type smtp-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Alert Handler implementation.

Default Value

org.opends.server.extensions.SMTPAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-body

Description

Specifies the body that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which the messages should be sent. Multiple values may be provided if there should be more than one recipient.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

sender-address

Description

Specifies the email address to use as the sender for messages generated by this alert handler.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-backend-index-prop(1)

Name

dsconfig get-backend-index-prop - Shows Backend Index properties

Synopsis

`dsconfig get-backend-index-prop` {options}

Description

Shows Backend Index properties.

Options

The `dsconfig get-backend-index-prop` command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend Index properties depend on the Backend Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default {name}: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

`--index-name {name}`

The name of the Backend Index.

Backend Index properties depend on the Backend Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default {name}: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

`--property {property}`

The name of a property to be displayed.

Backend Index properties depend on the Backend Index type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default {property}: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

`-E | --record`

Modifies the display output to show one property value per line.

Backend Index properties depend on the Backend Index type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default null: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Backend Index properties depend on the Backend Index type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default {unit}: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Backend Index properties depend on the Backend Index type, which depends on the {unit} you

provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default {unit}: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

Backend Index

Backend Indexes of type backend-index have the following properties:

attribute

Description

Specifies the name of the attribute for which the index is to be maintained.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

confidentiality-enabled

Description

Specifies whether contents of the index should be confidential. Setting the flag to true will hash keys for equality type indexes using SHA-1 and encrypt the list of entries matching a substring key for substring indexes.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

If the index for the attribute must be protected for security purposes and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate. The property cannot be set on a backend for which confidentiality is not enabled.

Advanced Property

No

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that are allowed to match a given index key before that particular index key is no longer maintained. This is analogous to the ALL IDs threshold in the Sun Java System Directory Server. If this is specified, its value overrides the JE backend-wide configuration. For no limit, use 0 for the value.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

If any index keys have already reached this limit, indexes must be rebuilt before they will be allowed to use the new limit.

Advanced Property

No

Read-only

No

index-extensible-matching-rule

Description

The extensible matching rule in an extensible index. An extensible matching rule must be specified using either LOCALE or OID of the matching rule.

Default Value

No extensible matching rules will be indexed.

Allowed Values

A Locale or an OID.

Multi-valued

Yes

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

No

Read-only

No

index-type

Description

Specifies the type(s) of indexing that should be performed for the associated attribute. For equality, presence, and substring index types, the associated attribute type must have a corresponding matching rule.

Default Value

None

Allowed Values

approximate

This index type is used to improve the efficiency of searches using approximate matching search filters.

equality

This index type is used to improve the efficiency of searches using equality search filters.

extensible

This index type is used to improve the efficiency of searches using extensible matching search filters.

ordering

This index type is used to improve the efficiency of searches using "greater than or equal to" or "less then or equal to" search filters.

presence

This index type is used to improve the efficiency of searches using the presence search filters.

substring

This index type is used to improve the efficiency of searches using substring search filters.

Multi-valued

Yes

Required

Yes

Admin Action Required

If any new index types are added for an attribute, and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate.

Advanced Property

No

Read-only

No

substring-length

Description

The length of substrings in a substring index.

Default Value

6

Allowed Values

An integer value. Lower value is 3.

Multi-valued

No

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-backend-prop(1)

Name

dsconfig get-backend-prop - Shows Backend properties

Synopsis

`dsconfig get-backend-prop` {options}

Description

Shows Backend properties.

Options

The `dsconfig get-backend-prop` command takes the following options:

`--backend-name {name}`

The name of the Backend.

Backend properties depend on the Backend type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend types:

`backup-backend`

Default {name}: Backup Backend

Enabled by default: true

See Backup Backend for the properties of this Backend type.

`cas-backend`

Default {name}: CAS Backend

Enabled by default: true

See CAS Backend for the properties of this Backend type.

`jdbc-backend`

Default {name}: JDBC Backend

Enabled by default: true

See JDBC Backend for the properties of this Backend type.

`je-backend`

Default {name}: JE Backend

Enabled by default: true

See JE Backend for the properties of this Backend type.

`ldif-backend`

Default {name}: LDIF Backend

Enabled by default: true

See LDIF Backend for the properties of this Backend type.

`memory-backend`

Default {name}: Memory Backend

Enabled by default: true

See Memory Backend for the properties of this Backend type.

`monitor-backend`

Default {name}: Monitor Backend

Enabled by default: true

See Monitor Backend for the properties of this Backend type.

`null-backend`

Default {name}: Null Backend

Enabled by default: true

See Null Backend for the properties of this Backend type.

`pdb-backend`

Default {name}: PDB Backend

Enabled by default: true

See PDB Backend for the properties of this Backend type.

`schema-backend`

Default {name}: Schema Backend

Enabled by default: true

See Schema Backend for the properties of this Backend type.

`task-backend`

Default {name}: Task Backend

Enabled by default: true

See Task Backend for the properties of this Backend type.

`trust-store-backend`

Default {name}: Trust Store Backend

Enabled by default: true

See Trust Store Backend for the properties of this Backend type.

`--property {property}`

The name of a property to be displayed.

Backend properties depend on the Backend type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Backend types:

`backup-backend`

Default {property}: Backup Backend

Enabled by default: true

See Backup Backend for the properties of this Backend type.

`cas-backend`

Default {property}: CAS Backend

Enabled by default: true

See CAS Backend for the properties of this Backend type.

`jdbc-backend`

Default {property}: JDBC Backend

Enabled by default: true

See JDBC Backend for the properties of this Backend type.

`je-backend`

Default {property}: JE Backend

Enabled by default: true

See JE Backend for the properties of this Backend type.

`ldif-backend`

Default {property}: LDIF Backend

Enabled by default: true

See LDIF Backend for the properties of this Backend type.

`memory-backend`

Default {property}: Memory Backend

Enabled by default: true

See Memory Backend for the properties of this Backend type.

`monitor-backend`

Default {property}: Monitor Backend

Enabled by default: true

See Monitor Backend for the properties of this Backend type.

`null-backend`

Default {property}: Null Backend

Enabled by default: true

See Null Backend for the properties of this Backend type.

`pdb-backend`

Default {property}: PDB Backend

Enabled by default: true

See PDB Backend for the properties of this Backend type.

`schema-backend`

Default {property}: Schema Backend

Enabled by default: true

See Schema Backend for the properties of this Backend type.

`task-backend`

Default {property}: Task Backend

Enabled by default: true

See Task Backend for the properties of this Backend type.

`trust-store-backend`

Default {property}: Trust Store Backend

Enabled by default: true

See Trust Store Backend for the properties of this Backend type.

`-E | --record`

Modifies the display output to show one property value per line.

Backend properties depend on the Backend type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Backend types:

`backup-backend`

Default null: Backup Backend

Enabled by default: true

See Backup Backend for the properties of this Backend type.

`cas-backend`

Default null: CAS Backend

Enabled by default: true

See CAS Backend for the properties of this Backend type.

`jdbc-backend`

Default null: JDBC Backend

Enabled by default: true

See JDBC Backend for the properties of this Backend type.

`je-backend`

Default null: JE Backend

Enabled by default: true

See JE Backend for the properties of this Backend type.

`ldif-backend`

Default null: LDIF Backend

Enabled by default: true

See LDIF Backend for the properties of this Backend type.

`memory-backend`

Default null: Memory Backend

Enabled by default: true

See Memory Backend for the properties of this Backend type.

`monitor-backend`

Default null: Monitor Backend

Enabled by default: true

See Monitor Backend for the properties of this Backend type.

`null-backend`

Default null: Null Backend

Enabled by default: true

See Null Backend for the properties of this Backend type.

`pdb-backend`

Default null: PDB Backend

Enabled by default: true

See PDB Backend for the properties of this Backend type.

`schema-backend`

Default null: Schema Backend

Enabled by default: true

See Schema Backend for the properties of this Backend type.

`task-backend`

Default null: Task Backend

Enabled by default: true

See Task Backend for the properties of this Backend type.

`trust-store-backend`

Default null: Trust Store Backend

Enabled by default: true

See Trust Store Backend for the properties of this Backend type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Backend properties depend on the Backend type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend types:

`backup-backend`

Default {unit}: Backup Backend

Enabled by default: true

See Backup Backend for the properties of this Backend type.

`cas-backend`

Default {unit}: CAS Backend

Enabled by default: true

See CAS Backend for the properties of this Backend type.

`jdbc-backend`

Default {unit}: JDBC Backend

Enabled by default: true

See JDBC Backend for the properties of this Backend type.

`je-backend`

Default {unit}: JE Backend

Enabled by default: true

See JE Backend for the properties of this Backend type.

`ldif-backend`

Default {unit}: LDIF Backend

Enabled by default: true

See LDIF Backend for the properties of this Backend type.

`memory-backend`

Default {unit}: Memory Backend

Enabled by default: true

See Memory Backend for the properties of this Backend type.

`monitor-backend`

Default {unit}: Monitor Backend

Enabled by default: true

See Monitor Backend for the properties of this Backend type.

`null-backend`

Default {unit}: Null Backend

Enabled by default: true

See Null Backend for the properties of this Backend type.

`pdb-backend`

Default {unit}: PDB Backend

Enabled by default: true

See PDB Backend for the properties of this Backend type.

`schema-backend`

Default {unit}: Schema Backend

Enabled by default: true

See Schema Backend for the properties of this Backend type.

`task-backend`

Default {unit}: Task Backend

Enabled by default: true

See Task Backend for the properties of this Backend type.

`trust-store-backend`

Default {unit}: Trust Store Backend

Enabled by default: true

See Trust Store Backend for the properties of this Backend type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Backend properties depend on the Backend type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend types:

`backup-backend`

Default {unit}: Backup Backend

Enabled by default: true

See Backup Backend for the properties of this Backend type.

`cas-backend`

Default {unit}: CAS Backend

Enabled by default: true

See CAS Backend for the properties of this Backend type.

`jdbc-backend`

Default {unit}: JDBC Backend

Enabled by default: true

See JDBC Backend for the properties of this Backend type.

`je-backend`

Default {unit}: JE Backend

Enabled by default: true

See JE Backend for the properties of this Backend type.

`ldif-backend`

Default {unit}: LDIF Backend

Enabled by default: true

See LDIF Backend for the properties of this Backend type.

`memory-backend`

Default {unit}: Memory Backend

Enabled by default: true

See Memory Backend for the properties of this Backend type.

`monitor-backend`

Default {unit}: Monitor Backend

Enabled by default: true

See Monitor Backend for the properties of this Backend type.

`null-backend`

Default {unit}: Null Backend

Enabled by default: true

See Null Backend for the properties of this Backend type.

`pdb-backend`

Default {unit}: PDB Backend

Enabled by default: true

See PDB Backend for the properties of this Backend type.

`schema-backend`

Default {unit}: Schema Backend

Enabled by default: true

See Schema Backend for the properties of this Backend type.

`task-backend`

Default {unit}: Task Backend

Enabled by default: true

See Task Backend for the properties of this Backend type.

`trust-store-backend`

Default {unit}: Trust Store Backend

Enabled by default: true

See Trust Store Backend for the properties of this Backend type.

Backup Backend

Backends of type backup-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

backup-directory

Description

Specifies the path to a backup directory containing one or more backups for a particular backend. This is a multivalued property. Each value may specify a different backup directory if desired (one for each backend for which backups are taken). Values may be either absolute

paths or paths that are relative to the base of the OpenDJ directory server installation.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.BackupBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

CAS Backend

Backends of type cas-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to

supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-directory

Description

Specifies the keyspace name The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

ldap_opendj

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.cassandra.Backend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

JDBC Backend

Backends of type jdbc-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using

NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-directory

Description

Specifies the connection string jdbc:postgresql://localhost/test

Default Value

jdbc:postgresql://localhost/test

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained

in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.jdbc.Backend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

JE Backend

Backends of type je-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-bytes-interval

Description

Specifies the maximum number of bytes that may be written to the database before it is forced to perform a checkpoint. This can be used to bound the recovery time that may be required if the database environment is opened without having been properly closed. If this property is set to a non-zero value, the checkpointer wakeup interval is not used. To use time-based checkpointing, set this property to zero.

Default Value

500mb

Allowed Values

Upper value is 9223372036854775807.

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. Note that this is only used if the value of the checkpointer bytes interval is zero.

Default Value

30s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.Upper limit is 4294 seconds.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-cleaner-min-utilization

Description

Specifies the occupancy percentage for "live" data in this backend's database. When the amount of "live" data in the database drops below this value, cleaners will act to increase the occupancy percentage by compacting the database.

Default Value

50

Allowed Values

An integer value. Lower value is 0. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Berkeley DB Java Edition database files containing the data for this backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-core-threads

Description

Specifies the core number of threads in the eviction thread pool. Specifies the core number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-

threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

1

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-keep-alive

Description

The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

600s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.Upper limit is 86400 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-lru-only

Description

Indicates whether the database should evict existing data from the cache based on an LRU policy (where the least recently used information will be evicted first). If set to "false", then the eviction keeps internal nodes of the underlying Btree in the cache over leaf nodes, even if the leaf nodes have been accessed more recently. This may be a better configuration for databases in which only a very small portion of the data is cached.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-max-threads

Description

Specifies the maximum number of threads in the eviction thread pool. Specifies the maximum number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-nodes-per-scan

Description

Specifies the number of Btree nodes that should be evicted from the cache in a single pass if it is determined that it is necessary to free existing data in order to make room for new information. Changes to this property do not take effect until the backend is restarted. It is recommended that you also change this property when you set db-evictor-lru-only to false. This setting controls the number of Btree nodes that are considered, or sampled, each time a node is evicted. A setting of 10 often produces good results, but this may vary from application to application. The larger the nodes per scan, the more accurate the algorithm. However, don't set it too high. When considering larger numbers of nodes for each eviction, the evictor may delay the completion of a given database operation, which impacts the response time of the application thread. In JE 4.1 and later, setting this value too high in an application that is largely CPU bound can reduce the effectiveness of cache eviction. It's best to start with the default value, and increase it gradually to see if it is beneficial for your application.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 1000.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-file-max

Description

Specifies the maximum size for a database log file.

Default Value

100mb

Allowed Values

Lower value is 1000000.Upper value is 4294967296.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-filecache-size

Description

Specifies the size of the file handle cache. The file handle cache is used to keep as much opened log files as possible. When the cache is smaller than the number of logs, the database needs to close some handles and open log files it needs, resulting in less optimal performances. Ideally, the size of the cache should be higher than the number of files contained in the database. Make sure the OS number of open files per process is also tuned appropriately.

Default Value

100

Allowed Values

An integer value. Lower value is 3. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-file-handler-on

Description

Indicates whether the database should maintain a je.info file in the same directory as the database log directory. This file contains information about the internal processing performed by the underlying database.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-level

Description

Specifies the log level that should be used by the database when it is writing information into the je.info file. The database trace logging level is (in increasing order of verbosity) chosen from:

OFF, SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST, ALL.

Default Value

CONFIG

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-cleaner-threads

Description

Specifies the number of threads that the backend should maintain to keep the database log files at or near the desired utilization. In environments with high write throughput, multiple cleaner threads may be required to maintain the desired utilization.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-lock-tables

Description

Specifies the number of lock tables that are used by the underlying database. This can be particularly important to help improve scalability by avoiding contention on systems with large numbers of CPUs. The value of this configuration property should be set to a prime number that is less than or equal to the number of worker threads configured for use in the server.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 32767.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-run-cleaner

Description

Indicates whether the cleaner threads should be enabled to compact the database. The cleaner threads are used to periodically compact the database when it reaches a percentage of occupancy lower than the amount specified by the db-cleaner-min-utilization property. They identify database files with a low percentage of live data, and relocate their remaining live data to the end of the log.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-write-no-sync

Description

Indicates whether the database should synchronously flush data as it is written to disk. If this value is set to "false", then all data written to disk is synchronously flushed to persistent storage and thereby providing full durability. If it is set to "true", then data may be cached for a period of time by the underlying operating system before actually being written to disk. This may improve performance, but could cause the most recent changes to be lost in the event of an underlying OS or hardware failure (but not in the case that the OpenDJ directory server or the JVM exits abnormally).

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.jeb.JEBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

je-property

Description

Specifies the database and environment properties for the Berkeley DB Java Edition database serving the data for this backend. Any Berkeley DB Java Edition property can be specified using

the following form: property-name=property-value. Refer to OpenDJ documentation for further information on related properties, their implications, and range values. The definitive identification of all the property parameters is available in the example.properties file of Berkeley DB Java Edition distribution.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

LDIF Backend

Backends of type ldif-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

is-private-backend

Description

Indicates whether the backend should be considered a private backend, which indicates that it is used for storing operational data rather than user-defined information.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.LDIFBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-file

Description

Specifies the path to the LDIF file containing the data for this backend.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Memory Backend

Backends of type memory-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base

DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MemoryBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Monitor Backend

Backends of type monitor-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MonitorBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Null Backend

Backends of type null-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.NullBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

PDB Backend

Backends of type pdb-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. This setting controls the elapsed time between attempts to write a checkpoint to the journal. A longer interval allows more updates to accumulate in buffers before they are required to be written to disk, but also potentially causes recovery from an abrupt termination (crash) to take more time.

Default Value

15s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 10 seconds.Upper limit is 3600 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Persistit database files containing the data for this backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the

directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the

index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.pdb.PDBBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Schema Backend

Backends of type schema-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.SchemaBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

schema-entry-dn

Description

Defines the base DNs of the subtrees in which the schema information is published in addition to the value included in the base-dn property. The value provided in the base-dn property is the only one that appears in the subschemaSubentry operational attribute of the server's root DSE (which is necessary because that is a single-valued attribute) and as a virtual attribute in other entries. The schema-entry-dn attribute may be used to make the schema information available in other locations to accommodate certain client applications that have been hard-coded to expect the schema to reside in a specific location.

Default Value

cn=schema

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

show-all-attributes

Description

Indicates whether to treat all attributes in the schema entry as if they were user attributes regardless of their configuration. This may provide compatibility with some applications that expect schema attributes like attributeTypes and objectClasses to be included by default even if they are not requested. Note that the ldapSyntaxes attribute is always treated as operational in order to avoid problems with attempts to modify the schema over protocol.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Task Backend

Backends of type task-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.task.TaskBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

notification-sender-address

Description

Specifies the email address to use as the sender (that is, the "From:" address) address for notification mail messages generated when a task completes execution.

Default Value

The default sender address used is "opendj-task-notification@" followed by the canonical address of the system on which the server is running.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

task-backing-file

Description

Specifies the path to the backing file for storing information about the tasks configured in the server. It may be either an absolute path or a relative path to the base of the OpenDJ directory server instance.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

task-retention-time

Description

Specifies the length of time that task entries should be retained after processing on the associated task has been completed.

Default Value

24 hours

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Trust Store Backend

Backends of type trust-store-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base

DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.TrustStoreBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file that stores the trust information. It may be an absolute path, or a path that is relative to the OpenDJ instance root.

Default Value

config/ads-truststore

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the

Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well.

Default Value

The JVM default value is used.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect the next time that the key manager is accessed.

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-backend-vlv-index-prop(1)

Name

dsconfig get-backend-vlv-index-prop - Shows Backend VLV Index properties

Synopsis

`dsconfig get-backend-vlv-index-prop` {options}

Description

Shows Backend VLV Index properties.

Options

The `dsconfig get-backend-vlv-index-prop` command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default {name}: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

`--index-name {name}`

The name of the Backend VLV Index.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default {name}: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

`--property {property}`

The name of a property to be displayed.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default {property}: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

`-E | --record`

Modifies the display output to show one property value per line.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default null: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default {unit}: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the

{unit} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default {unit}: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

Backend VLV Index

Backend VLV Indexes of type backend-vlv-index have the following properties:

base-dn

Description

Specifies the base DN used in the search query that is being indexed.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

filter

Description

Specifies the LDAP filter used in the query that is being indexed.

Default Value

None

Allowed Values

A valid LDAP search filter.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

name

Description

Specifies a unique name for this VLV index.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

NoneThe VLV index name cannot be altered after the index is created.

Advanced Property

No

Read-only

Yes

scope

Description

Specifies the LDAP scope of the query that is being indexed.

Default Value

None

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

sort-order

Description

Specifies the names of the attributes that are used to sort the entries for the query being indexed. Multiple attributes can be used to determine the sort order by listing the attribute names from highest to lowest precedence. Optionally, + or - can be prefixed to the attribute name to sort the attribute in ascending order or descending order respectively.

Default Value

None

Allowed Values

Valid attribute types defined in the schema, separated by a space and optionally prefixed by + or -.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

dsconfig get-certificate-mapper-prop(1)

Name

dsconfig get-certificate-mapper-prop - Shows Certificate Mapper properties

Synopsis

`dsconfig get-certificate-mapper-prop` {options}

Description

Shows Certificate Mapper properties.

Options

The `dsconfig get-certificate-mapper-prop` command takes the following options:

`--mapper-name {name}`

The name of the Certificate Mapper.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

`fingerprint-certificate-mapper`

Default {name}: Fingerprint Certificate Mapper

Enabled by default: true

See Fingerprint Certificate Mapper for the properties of this Certificate Mapper type.

`subject-attribute-to-user-attribute-certificate-mapper`

Default {name}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See Subject Attribute To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-dn-to-user-attribute-certificate-mapper`

Default {name}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See Subject DN To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-equals-dn-certificate-mapper`

Default {name}: Subject Equals DN Certificate Mapper

Enabled by default: true

See Subject Equals DN Certificate Mapper for the properties of this Certificate Mapper type.

`--property {property}`

The name of a property to be displayed.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

`fingerprint-certificate-mapper`

Default {property}: Fingerprint Certificate Mapper

Enabled by default: true

See Fingerprint Certificate Mapper for the properties of this Certificate Mapper type.

`subject-attribute-to-user-attribute-certificate-mapper`

Default {property}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See Subject Attribute To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-dn-to-user-attribute-certificate-mapper`

Default {property}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See Subject DN To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-equals-dn-certificate-mapper`

Default {property}: Subject Equals DN Certificate Mapper

Enabled by default: true

See Subject Equals DN Certificate Mapper for the properties of this Certificate Mapper type.

`-E | --record`

Modifies the display output to show one property value per line.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

`fingerprint-certificate-mapper`

Default null: Fingerprint Certificate Mapper

Enabled by default: true

See Fingerprint Certificate Mapper for the properties of this Certificate Mapper type.

`subject-attribute-to-user-attribute-certificate-mapper`

Default null: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See Subject Attribute To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-dn-to-user-attribute-certificate-mapper`

Default null: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See Subject DN To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-equals-dn-certificate-mapper`

Default null: Subject Equals DN Certificate Mapper

Enabled by default: true

See Subject Equals DN Certificate Mapper for the properties of this Certificate Mapper type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

`fingerprint-certificate-mapper`

Default {unit}: Fingerprint Certificate Mapper

Enabled by default: true

See Fingerprint Certificate Mapper for the properties of this Certificate Mapper type.

`subject-attribute-to-user-attribute-certificate-mapper`

Default {unit}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See Subject Attribute To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-dn-to-user-attribute-certificate-mapper`

Default {unit}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See Subject DN To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-equals-dn-certificate-mapper`

Default {unit}: Subject Equals DN Certificate Mapper

Enabled by default: true

See Subject Equals DN Certificate Mapper for the properties of this Certificate Mapper type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

`fingerprint-certificate-mapper`

Default {unit}: Fingerprint Certificate Mapper

Enabled by default: true

See Fingerprint Certificate Mapper for the properties of this Certificate Mapper type.

`subject-attribute-to-user-attribute-certificate-mapper`

Default {unit}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See Subject Attribute To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-dn-to-user-attribute-certificate-mapper`

Default {unit}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See Subject DN To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-equals-dn-certificate-mapper`

Default {unit}: Subject Equals DN Certificate Mapper

Enabled by default: true

See Subject Equals DN Certificate Mapper for the properties of this Certificate Mapper type.

Fingerprint Certificate Mapper

Certificate Mappers of type fingerprint-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-algorithm

Description

Specifies the name of the digest algorithm to compute the fingerprint of client certificates.

Default Value

None

Allowed Values

md5

Use the MD5 digest algorithm to compute certificate fingerprints.

sha1

Use the SHA-1 digest algorithm to compute certificate fingerprints.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-attribute

Description

Specifies the attribute in which to look for the fingerprint. Values of the fingerprint attribute should exactly match the MD5 or SHA1 representation of the certificate fingerprint.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fingerprint Certificate Mapper implementation.

Default Value

org.opends.server.extensions.FingerprintCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs are used when performing searches to map the client certificates to a user entry.

Default Value

The server performs the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subject Attribute To User Attribute Certificate Mapper

Certificate Mappers of type subject-attribute-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Attribute To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectAttributeToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute-mapping

Description

Specifies a mapping between certificate attributes and user attributes. Each value should be in the form "certattr:userattr" where certattr is the name of the attribute in the certificate subject and userattr is the name of the corresponding attribute in user entries. There may be multiple mappings defined, and when performing the mapping values for all attributes present in the certificate subject that have mappings defined must be present in the corresponding user entries.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subject DN To User Attribute Certificate Mapper

Certificate Mappers of type subject-dn-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject DN To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectDNToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute

Description

Specifies the name or OID of the attribute whose value should exactly match the certificate subject DN.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subject Equals DN Certificate Mapper

Certificate Mappers of type subject-equals-dn-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Equals DN Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectEqualsDNCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-connection-handler-prop(1)

Name

dsconfig get-connection-handler-prop - Shows Connection Handler properties

Synopsis

`dsconfig get-connection-handler-prop` {options}

Description

Shows Connection Handler properties.

Options

The `dsconfig get-connection-handler-prop` command takes the following options:

`--handler-name {name}`

The name of the Connection Handler.

Connection Handler properties depend on the Connection Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

`http-connection-handler`

Default {name}: HTTP Connection Handler

Enabled by default: true

See HTTP Connection Handler for the properties of this Connection Handler type.

`jmx-connection-handler`

Default {name}: JMX Connection Handler

Enabled by default: true

See JMX Connection Handler for the properties of this Connection Handler type.

`ldap-connection-handler`

Default {name}: LDAP Connection Handler

Enabled by default: true

See LDAP Connection Handler for the properties of this Connection Handler type.

`ldif-connection-handler`

Default {name}: LDIF Connection Handler

Enabled by default: true

See LDIF Connection Handler for the properties of this Connection Handler type.

`snmp-connection-handler`

Default {name}: SNMP Connection Handler

Enabled by default: true

See SNMP Connection Handler for the properties of this Connection Handler type.

`--property {property}`

The name of a property to be displayed.

Connection Handler properties depend on the Connection Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

`http-connection-handler`

Default {property}: HTTP Connection Handler

Enabled by default: true

See HTTP Connection Handler for the properties of this Connection Handler type.

`jmx-connection-handler`

Default {property}: JMX Connection Handler

Enabled by default: true

See JMX Connection Handler for the properties of this Connection Handler type.

`ldap-connection-handler`

Default {property}: LDAP Connection Handler

Enabled by default: true

See LDAP Connection Handler for the properties of this Connection Handler type.

`ldif-connection-handler`

Default {property}: LDIF Connection Handler

Enabled by default: true

See LDIF Connection Handler for the properties of this Connection Handler type.

`snmp-connection-handler`

Default {property}: SNMP Connection Handler

Enabled by default: true

See SNMP Connection Handler for the properties of this Connection Handler type.

`-E | --record`

Modifies the display output to show one property value per line.

Connection Handler properties depend on the Connection Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

`http-connection-handler`

Default null: HTTP Connection Handler

Enabled by default: true

See HTTP Connection Handler for the properties of this Connection Handler type.

`jmx-connection-handler`

Default null: JMX Connection Handler

Enabled by default: true

See JMX Connection Handler for the properties of this Connection Handler type.

`ldap-connection-handler`

Default null: LDAP Connection Handler

Enabled by default: true

See LDAP Connection Handler for the properties of this Connection Handler type.

`ldif-connection-handler`

Default null: LDIF Connection Handler

Enabled by default: true

See LDIF Connection Handler for the properties of this Connection Handler type.

`snmp-connection-handler`

Default null: SNMP Connection Handler

Enabled by default: true

See SNMP Connection Handler for the properties of this Connection Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Connection Handler properties depend on the Connection Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

`http-connection-handler`

Default {unit}: HTTP Connection Handler

Enabled by default: true

See HTTP Connection Handler for the properties of this Connection Handler type.

`jmx-connection-handler`

Default {unit}: JMX Connection Handler

Enabled by default: true

See JMX Connection Handler for the properties of this Connection Handler type.

`ldap-connection-handler`

Default {unit}: LDAP Connection Handler

Enabled by default: true

See LDAP Connection Handler for the properties of this Connection Handler type.

`ldif-connection-handler`

Default {unit}: LDIF Connection Handler

Enabled by default: true

See LDIF Connection Handler for the properties of this Connection Handler type.

`snmp-connection-handler`

Default {unit}: SNMP Connection Handler

Enabled by default: true

See SNMP Connection Handler for the properties of this Connection Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Connection Handler properties depend on the Connection Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

`http-connection-handler`

Default {unit}: HTTP Connection Handler

Enabled by default: true

See HTTP Connection Handler for the properties of this Connection Handler type.

`jmx-connection-handler`

Default {unit}: JMX Connection Handler

Enabled by default: true

See JMX Connection Handler for the properties of this Connection Handler type.

`ldap-connection-handler`

Default {unit}: LDAP Connection Handler

Enabled by default: true

See LDAP Connection Handler for the properties of this Connection Handler type.

`ldif-connection-handler`

Default {unit}: LDIF Connection Handler

Enabled by default: true

See LDIF Connection Handler for the properties of this Connection Handler type.

`snmp-connection-handler`

Default {unit}: SNMP Connection Handler

Enabled by default: true

See SNMP Connection Handler for the properties of this Connection Handler type.

HTTP Connection Handler

Connection Handlers of type http-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the HTTP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the HTTP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer HTTP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Connection Handler implementation.

Default Value

org.opends.server.protocols.http.HTTPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the HTTP Connection Handler should keep statistics. If enabled, the HTTP Connection Handler maintains statistics about the number and types of operations requested over HTTP and the amount of data sent and received.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this HTTP Connection Handler should listen for connections from HTTP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the HTTP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the HTTP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to HTTP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-concurrent-ops-per-connection

Description

Specifies the maximum number of internal operations that each HTTP client connection can execute concurrently. This property allow to limit the impact that each HTTP request can have on the whole server by limiting the number of internal operations that each HTTP request can execute concurrently. A value of 0 means that no limit is enforced.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest HTTP request message that will be allowed by the HTTP Connection Handler. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The HTTP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the HTTP Connection Handler should use when performing SSL communication. The property can be used

multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the HTTP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL/TLS-based

sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the HTTP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the HTTP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the HTTP Connection Handler should use SSL. If enabled, the HTTP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the HTTP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the HTTP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

JMX Connection Handler

Connection Handlers of type jmx-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Connection Handler implementation.

Default Value

org.opends.server.protocols.jmx.JmxConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this JMX Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the JMX Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address on which this JMX Connection Handler should listen for connections from JMX clients. If no value is provided, then the JMX Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the JMX Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

rmi-port

Description

Specifies the port number on which the JMX RMI service will listen for connections from clients. A value of 0 indicates the service to choose a port of its own. If the value provided is different than 0, the value will be used as the RMI port. Otherwise, the RMI service will choose a port of its own.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the JMX Connection Handler should use when performing SSL communication. The property can be used multiple

times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the JMX Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the JMX Connection Handler should use SSL. If enabled, the JMX Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

LDAP Connection Handler

Connection Handlers of type ldap-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-ldap-v2

Description

Indicates whether connections from LDAPv2 clients are allowed. If LDAPv2 clients are allowed, then only a minimal degree of special support are provided for them to ensure that LDAPv3-specific protocol elements (for example, Configuration Guide 25 controls, extended response messages, intermediate response messages, referrals) are not sent to an LDAPv2 client.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-start-tls

Description

Indicates whether clients are allowed to use StartTLS. If enabled, the LDAP Connection Handler allows clients to use the StartTLS extended operation to initiate secure communication over an otherwise insecure channel. Note that this is only allowed if the LDAP Connection Handler is not configured to use SSL, and if the server is configured with a valid key manager provider and a valid trust manager provider.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the LDAP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the LDAP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer LDAP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDAP Connection Handler implementation.

Default Value

org.opends.server.protocols.ldap.LDAPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the LDAP Connection Handler should keep statistics. If enabled, the LDAP Connection Handler maintains statistics about the number and types of operations requested

over LDAP and the amount of data sent and received.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this LDAP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this LDAP Connection Handler should listen for connections from LDAP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the LDAP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the LDAP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to LDAP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest LDAP request message that will be allowed by this LDAP Connection handler. This property is analogous to the maxBERSize configuration attribute of the Sun Java System Directory Server. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large

amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The LDAP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-rejection-notice

Description

Indicates whether the LDAP Connection Handler should send a notice of disconnection extended response message to the client if a new connection is rejected for some reason. The extended response message may provide an explanation indicating the reason that the connection was rejected.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the LDAP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the LDAP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the LDAP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the LDAP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Connection Handler should use SSL. If enabled, the LDAP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the LDAP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the LDAP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

LDIF Connection Handler

Connection Handlers of type ldif-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDIF Connection Handler implementation.

Default Value

org.opends.server.protocols.LDIFConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-directory

Description

Specifies the path to the directory in which the LDIF files should be placed.

Default Value

config/auto-process-ldif

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

poll-interval

Description

Specifies how frequently the LDIF connection handler should check the LDIF directory to determine whether a new LDIF file has been added.

Default Value

5 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

SNMP Connection Handler

Connection Handlers of type snmp-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

allowed-manager

Description

Specifies the hosts of the managers to be granted the access rights. This property is required for SNMP v1 and v2 security configuration. An asterisk (*) opens access to all managers.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

allowed-user

Description

Specifies the users to be granted the access rights. This property is required for SNMP v3 security

configuration. An asterisk (*) opens access to all users.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

community

Description

Specifies the v1,v2 community or the v3 context name allowed to access the MIB 2605 monitoring information or the USM MIB. The mapping between "community" and "context name" is set.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SNMP Connection Handler implementation.

Default Value

org.opends.server.snmp.SNMPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this SNMP Connection Handler should listen for connections from SNMP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the SNMP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

Yes

listen-port

Description

Specifies the port number on which the SNMP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

opendmk-jarfile

Description

Indicates the OpenDMK runtime jar file location

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

registered-mbean

Description

Indicates whether the SNMP objects have to be registered in the directory server MBeanServer or not allowing to access SNMP Objects with RMI connector if enabled.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-agent-file

Description

Specifies the USM security configuration to receive authenticated only SNMP requests.

Default Value

config/snmp/security/opendj-snmp.security

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-level

Description

Specifies the type of security level : NoAuthNoPriv : No security mechanisms activated, AuthNoPriv : Authentication activated with no privacy, AuthPriv : Authentication with privacy activated. This property is required for SNMP V3 security configuration.

Default Value

authnopriv

Allowed Values

authnopriv

Authentication activated with no privacy.

authpriv

Authentication with privacy activated.

noauthnopriv

No security mechanisms activated.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trap-port

Description

Specifies the port to use to send SNMP Traps.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take

effect

Advanced Property

No

Read-only

No

traps-community

Description

Specifies the community string that must be included in the traps sent to define managers (trap-destinations). This property is used in the context of SNMP v1, v2 and v3.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-destination

Description

Specifies the hosts to which V1 traps will be sent. V1 Traps are sent to every host listed. If this list is empty, V1 traps are sent to "localhost". Each host in the list must be identifed by its name or complete IP Addess.

Default Value

If the list is empty, V1 traps are sent to "localhost".

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig get-crypto-manager-prop(1)

Name

dsconfig get-crypto-manager-prop - Shows Crypto Manager properties

Synopsis

`dsconfig get-crypto-manager-prop` {options}

Description

Shows Crypto Manager properties.

Options

The `dsconfig get-crypto-manager-prop` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Crypto Manager properties depend on the Crypto Manager type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Crypto Manager types:

`crypto-manager`

Default {property}: Crypto Manager

Enabled by default: false

See Crypto Manager for the properties of this Crypto Manager type.

`-E | --record`

Modifies the display output to show one property value per line.

Crypto Manager properties depend on the Crypto Manager type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Crypto Manager types:

`crypto-manager`

Default null: Crypto Manager

Enabled by default: false

See Crypto Manager for the properties of this Crypto Manager type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Crypto Manager properties depend on the Crypto Manager type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Crypto Manager types:

`crypto-manager`

Default {unit}: Crypto Manager

Enabled by default: false

See Crypto Manager for the properties of this Crypto Manager type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Crypto Manager properties depend on the Crypto Manager type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Crypto Manager types:

`crypto-manager`

Default {unit}: Crypto Manager

Enabled by default: false

See Crypto Manager for the properties of this Crypto Manager type.

Crypto Manager

Crypto Managers of type crypto-manager have the following properties:

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server using the syntax algorithm/mode/padding. The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

digest-algorithm

Description

Specifies the preferred message digest algorithm for the directory server.

Default Value

SHA-256

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-wrapping-transformation

Description

The preferred key wrapping transformation for the directory server. This value must be the same for all server instances in a replication topology.

Default Value

RSA/ECB/OAEPWITHSHA-1ANDMGF1PADDING

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect immediately but will only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

mac-algorithm

Description

Specifies the preferred MAC algorithm for the directory server.

Default Value

HmacSHA256

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

mac-key-length

Description

Specifies the key length in bits for the preferred MAC algorithm.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Crypto Manager should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Crypto Manager is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Crypto Manager must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL or TLS communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-encryption

Description

Specifies whether SSL/TLS is used to provide encrypted communication between two OpenDJ server components.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or TLS communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

dsconfig get-debug-target-prop(1)

Name

dsconfig get-debug-target-prop - Shows Debug Target properties

Synopsis

`dsconfig get-debug-target-prop` {options}

Description

Shows Debug Target properties.

Options

The `dsconfig get-debug-target-prop` command takes the following options:

`--publisher-name {name}`

The name of the Debug Log Publisher.

Debug Target properties depend on the Debug Target type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default {name}: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

`--target-name {name}`

The name of the Debug Target.

Debug Target properties depend on the Debug Target type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default {name}: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

`--property {property}`

The name of a property to be displayed.

Debug Target properties depend on the Debug Target type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default {property}: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

`-E | --record`

Modifies the display output to show one property value per line.

Debug Target properties depend on the Debug Target type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default null: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Debug Target properties depend on the Debug Target type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default {unit}: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Debug Target properties depend on the Debug Target type, which depends on the {unit} you

provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default {unit}: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

Debug Target

Debug Targets of type debug-target have the following properties:

debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

debug-scope

Description

Specifies the fully-qualified OpenDJ Java package, class, or method affected by the settings in this target definition. Use the number character (#) to separate the class name and the method name (that is, org.opends.server.core.DirectoryServer#startUp).

Default Value

None

Allowed Values

The fully-qualified OpenDJ Java package, class, or method name.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the Debug Target is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

include-throwable-cause

Description

Specifies the property to indicate whether to include the cause of exceptions in exception thrown and caught messages.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-entry-arguments

Description

Specifies the property to indicate whether to include method arguments in debug messages.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-return-value

Description

Specifies the property to indicate whether to include the return value in debug messages.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

throwable-stack-frames

Description

Specifies the property to indicate the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

0

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-entry-cache-prop(1)

Name

dsconfig get-entry-cache-prop - Shows Entry Cache properties

Synopsis

`dsconfig get-entry-cache-prop` {options}

Description

Shows Entry Cache properties.

Options

The `dsconfig get-entry-cache-prop` command takes the following options:

`--cache-name {name}`

The name of the Entry Cache.

Entry Cache properties depend on the Entry Cache type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

`fifo-entry-cache`

Default {name}: FIFO Entry Cache

Enabled by default: true

See FIFO Entry Cache for the properties of this Entry Cache type.

`soft-reference-entry-cache`

Default {name}: Soft Reference Entry Cache

Enabled by default: true

See Soft Reference Entry Cache for the properties of this Entry Cache type.

`--property {property}`

The name of a property to be displayed.

Entry Cache properties depend on the Entry Cache type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

`fifo-entry-cache`

Default {property}: FIFO Entry Cache

Enabled by default: true

See FIFO Entry Cache for the properties of this Entry Cache type.

`soft-reference-entry-cache`

Default {property}: Soft Reference Entry Cache

Enabled by default: true

See Soft Reference Entry Cache for the properties of this Entry Cache type.

`-E | --record`

Modifies the display output to show one property value per line.

Entry Cache properties depend on the Entry Cache type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

`fifo-entry-cache`

Default null: FIFO Entry Cache

Enabled by default: true

See FIFO Entry Cache for the properties of this Entry Cache type.

`soft-reference-entry-cache`

Default null: Soft Reference Entry Cache

Enabled by default: true

See Soft Reference Entry Cache for the properties of this Entry Cache type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Entry Cache properties depend on the Entry Cache type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

`fifo-entry-cache`

Default {unit}: FIFO Entry Cache

Enabled by default: true

See FIFO Entry Cache for the properties of this Entry Cache type.

`soft-reference-entry-cache`

Default {unit}: Soft Reference Entry Cache

Enabled by default: true

See Soft Reference Entry Cache for the properties of this Entry Cache type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Entry Cache properties depend on the Entry Cache type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

`fifo-entry-cache`

Default {unit}: FIFO Entry Cache

Enabled by default: true

See FIFO Entry Cache for the properties of this Entry Cache type.

`soft-reference-entry-cache`

Default {unit}: Soft Reference Entry Cache

Enabled by default: true

See Soft Reference Entry Cache for the properties of this Entry Cache type.

FIFO Entry Cache

Entry Caches of type fifo-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the FIFO Entry Cache implementation.

Default Value

org.opends.server.extensions.FIFOEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time to wait while attempting to acquire a read or write lock.

Default Value

2000.0ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-entries

Description

Specifies the maximum number of entries that we will allow in the cache.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-memory-percent

Description

Specifies the maximum percentage of JVM memory used by the server before the entry caches stops caching and begins purging itself. Very low settings such as 10 or 20 (percent) can prevent this entry cache from having enough space to hold any of the entries to cache, making it appear that the server is ignoring or skipping the entry cache entirely.

Default Value

90

Allowed Values

An integer value. Lower value is 1. Upper value is 100.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Soft Reference Entry Cache

Entry Caches of type soft-reference-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Soft Reference Entry Cache implementation.

Default Value

org.opends.server.extensions.SoftReferenceEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time in milliseconds to wait while attempting to acquire a read or write lock.

Default Value

3000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-extended-operation-handler-prop(1)

Name

dsconfig get-extended-operation-handler-prop - Shows Extended Operation Handler properties

Synopsis

`dsconfig get-extended-operation-handler-prop` {options}

Description

Shows Extended Operation Handler properties.

Options

The `dsconfig get-extended-operation-handler-prop` command takes the following options:

`--handler-name {name}`

The name of the Extended Operation Handler.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

`cancel-extended-operation-handler`

Default {name}: Cancel Extended Operation Handler

Enabled by default: true

See Cancel Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-connection-id-extended-operation-handler`

Default {name}: Get Connection Id Extended Operation Handler

Enabled by default: true

See Get Connection Id Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-symmetric-key-extended-operation-handler`

Default {name}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See Get Symmetric Key Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-modify-extended-operation-handler`

Default {name}: Password Modify Extended Operation Handler

Enabled by default: true

See Password Modify Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-policy-state-extended-operation-handler`

Default {name}: Password Policy State Extended Operation Handler

Enabled by default: true

See Password Policy State Extended Operation Handler for the properties of this Extended Operation Handler type.

`start-tls-extended-operation-handler`

Default {name}: Start TLS Extended Operation Handler

Enabled by default: true

See Start TLS Extended Operation Handler for the properties of this Extended Operation Handler type.

`who-am-i-extended-operation-handler`

Default {name}: Who Am I Extended Operation Handler

Enabled by default: true

See Who Am I Extended Operation Handler for the properties of this Extended Operation Handler type.

`--property {property}`

The name of a property to be displayed.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

`cancel-extended-operation-handler`

Default {property}: Cancel Extended Operation Handler

Enabled by default: true

See Cancel Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-connection-id-extended-operation-handler`

Default {property}: Get Connection Id Extended Operation Handler

Enabled by default: true

See Get Connection Id Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-symmetric-key-extended-operation-handler`

Default {property}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See Get Symmetric Key Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-modify-extended-operation-handler`

Default {property}: Password Modify Extended Operation Handler

Enabled by default: true

See Password Modify Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-policy-state-extended-operation-handler`

Default {property}: Password Policy State Extended Operation Handler

Enabled by default: true

See Password Policy State Extended Operation Handler for the properties of this Extended Operation Handler type.

`start-tls-extended-operation-handler`

Default {property}: Start TLS Extended Operation Handler

Enabled by default: true

See Start TLS Extended Operation Handler for the properties of this Extended Operation Handler type.

`who-am-i-extended-operation-handler`

Default {property}: Who Am I Extended Operation Handler

Enabled by default: true

See Who Am I Extended Operation Handler for the properties of this Extended Operation Handler type.

`-E | --record`

Modifies the display output to show one property value per line.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

`cancel-extended-operation-handler`

Default null: Cancel Extended Operation Handler

Enabled by default: true

See Cancel Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-connection-id-extended-operation-handler`

Default null: Get Connection Id Extended Operation Handler

Enabled by default: true

See Get Connection Id Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-symmetric-key-extended-operation-handler`

Default null: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See Get Symmetric Key Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-modify-extended-operation-handler`

Default null: Password Modify Extended Operation Handler

Enabled by default: true

See Password Modify Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-policy-state-extended-operation-handler`

Default null: Password Policy State Extended Operation Handler

Enabled by default: true

See Password Policy State Extended Operation Handler for the properties of this Extended Operation Handler type.

`start-tls-extended-operation-handler`

Default null: Start TLS Extended Operation Handler

Enabled by default: true

See Start TLS Extended Operation Handler for the properties of this Extended Operation

Handler type.

`who-am-i-extended-operation-handler`

Default null: Who Am I Extended Operation Handler

Enabled by default: true

See Who Am I Extended Operation Handler for the properties of this Extended Operation Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

`cancel-extended-operation-handler`

Default {unit}: Cancel Extended Operation Handler

Enabled by default: true

See Cancel Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-connection-id-extended-operation-handler`

Default {unit}: Get Connection Id Extended Operation Handler

Enabled by default: true

See Get Connection Id Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-symmetric-key-extended-operation-handler`

Default {unit}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See Get Symmetric Key Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-modify-extended-operation-handler`

Default {unit}: Password Modify Extended Operation Handler

Enabled by default: true

See Password Modify Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-policy-state-extended-operation-handler`

Default {unit}: Password Policy State Extended Operation Handler

Enabled by default: true

See Password Policy State Extended Operation Handler for the properties of this Extended Operation Handler type.

`start-tls-extended-operation-handler`

Default {unit}: Start TLS Extended Operation Handler

Enabled by default: true

See Start TLS Extended Operation Handler for the properties of this Extended Operation Handler type.

`who-am-i-extended-operation-handler`

Default {unit}: Who Am I Extended Operation Handler

Enabled by default: true

See Who Am I Extended Operation Handler for the properties of this Extended Operation Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

`cancel-extended-operation-handler`

Default {unit}: Cancel Extended Operation Handler

Enabled by default: true

See Cancel Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-connection-id-extended-operation-handler`

Default {unit}: Get Connection Id Extended Operation Handler

Enabled by default: true

See Get Connection Id Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-symmetric-key-extended-operation-handler`

Default {unit}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See Get Symmetric Key Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-modify-extended-operation-handler`

Default {unit}: Password Modify Extended Operation Handler

Enabled by default: true

See Password Modify Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-policy-state-extended-operation-handler`

Default {unit}: Password Policy State Extended Operation Handler

Enabled by default: true

See Password Policy State Extended Operation Handler for the properties of this Extended Operation Handler type.

`start-tls-extended-operation-handler`

Default {unit}: Start TLS Extended Operation Handler

Enabled by default: true

See Start TLS Extended Operation Handler for the properties of this Extended Operation Handler type.

`who-am-i-extended-operation-handler`

Default {unit}: Who Am I Extended Operation Handler

Enabled by default: true

See Who Am I Extended Operation Handler for the properties of this Extended Operation Handler type.

Cancel Extended Operation Handler

Extended Operation Handlers of type cancel-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Cancel Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.CancelExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Get Connection Id Extended Operation Handler

Extended Operation Handlers of type get-connection-id-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Connection Id Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.GetConnectionIDExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Get Symmetric Key Extended Operation Handler

Extended Operation Handlers of type get-symmetric-key-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Symmetric Key Extended Operation Handler implementation.

Default Value

org.opends.server.crypto.GetSymmetricKeyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Modify Extended Operation Handler

Extended Operation Handlers of type password-modify-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that should be used in conjunction with the password modify extended operation. This property is used to identify a user based on an authorization ID in the 'u:' form. Changes to this property take effect immediately.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Password Modify Extended Operation Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Modify Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordModifyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Policy State Extended Operation Handler

Extended Operation Handlers of type password-policy-state-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Policy State Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordPolicyStateExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Start TLS Extended Operation Handler

Extended Operation Handlers of type start-tls-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Start TLS Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.StartTLSExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Who Am I Extended Operation Handler

Extended Operation Handlers of type who-am-i-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Who Am I Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.WhoAmIExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-external-changelog-domain-prop(1)

Name

dsconfig get-external-changelog-domain-prop - Shows External Changelog Domain properties

Synopsis

`dsconfig get-external-changelog-domain-prop` {options}

Description

Shows External Changelog Domain properties.

Options

The `dsconfig get-external-changelog-domain-prop` command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following External Changelog Domain types:

`external-changelog-domain`

Default {name}: External Changelog Domain

Enabled by default: true

See External Changelog Domain for the properties of this External Changelog Domain type.

`--domain-name {name}`

The name of the Replication Domain.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following External Changelog Domain types:

`external-changelog-domain`

Default {name}: External Changelog Domain

Enabled by default: true

See External Changelog Domain for the properties of this External Changelog Domain type.

`--property {property}`

The name of a property to be displayed.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following External Changelog Domain types:

`external-changelog-domain`

Default {property}: External Changelog Domain

Enabled by default: true

See External Changelog Domain for the properties of this External Changelog Domain type.

`-E | --record`

Modifies the display output to show one property value per line.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the null you provide.

By default, OpenDJ directory server supports the following External Changelog Domain types:

`external-changelog-domain`

Default null: External Changelog Domain

Enabled by default: true

See External Changelog Domain for the properties of this External Changelog Domain type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following External Changelog Domain types:

`external-changelog-domain`

Default {unit}: External Changelog Domain

Enabled by default: true

See External Changelog Domain for the properties of this External Changelog Domain type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following External Changelog Domain types:

`external-changelog-domain`

Default {unit}: External Changelog Domain

Enabled by default: true

See External Changelog Domain for the properties of this External Changelog Domain type.

External Changelog Domain

External Changelog Domains of type external-changelog-domain have the following properties:

ecl-include

Description

Specifies a list of attributes which should be published with every change log entry, regardless of whether the attribute itself has changed. The list of attributes may include wild cards such as "*" and "+" as well as object class references prefixed with an ampersand, for example "@person". The included attributes will be published using the "includedAttributes" operational attribute as a single LDIF value rather like the "changes" attribute. For modify and modifyDN operations the included attributes will be taken from the entry before any changes were applied.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ecl-include-for-deletes

Description

Specifies a list of attributes which should be published with every delete operation change log entry, in addition to those specified by the "ecl-include" property. This property provides a means for applications to archive entries after they have been deleted. See the description of the "ecl-include" property for further information about how the included attributes are published.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the External Changelog Domain is enabled. To enable computing the change numbers, set the Replication Server's "ds-cfg-compute-change-number" property to true.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-global-configuration-prop(1)

Name

dsconfig get-global-configuration-prop - Shows Global Configuration properties

Synopsis

`dsconfig get-global-configuration-prop` {options}

Description

Shows Global Configuration properties.

Options

The `dsconfig get-global-configuration-prop` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Global Configuration properties depend on the Global Configuration type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Global Configuration types:

`global`

Default {property}: Global Configuration

Enabled by default: false

See Global Configuration for the properties of this Global Configuration type.

`-E | --record`

Modifies the display output to show one property value per line.

Global Configuration properties depend on the Global Configuration type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Global Configuration types:

`global`

Default null: Global Configuration

Enabled by default: false

See Global Configuration for the properties of this Global Configuration type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Global Configuration properties depend on the Global Configuration type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Global Configuration types:

`global`

Default {unit}: Global Configuration

Enabled by default: false

See Global Configuration for the properties of this Global Configuration type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Global Configuration properties depend on the Global Configuration type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Global Configuration types:

`global`

Default {unit}: Global Configuration

Enabled by default: false

See Global Configuration for the properties of this Global Configuration type.

Global Configuration

Global Configurations of type global have the following properties:

add-missing-rdn-attributes

Description

Indicates whether the directory server should automatically add any attribute values contained in the entry's RDN into that entry when processing an add request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-attribute-name-exceptions

Description

Indicates whether the directory server should allow underscores in attribute names and allow attribute names to begin with numeric digits (both of which are violations of the LDAP standards).

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-task

Description

Specifies the fully-qualified name of a Java class that may be invoked in the server. Any attempt to invoke a task not included in the list of allowed tasks is rejected.

Default Value

If no values are defined, then the server does not allow any tasks to be invoked.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

bind-with-dn-requires-password

Description

Indicates whether the directory server should reject any simple bind request that contains a DN but no password. Although such bind requests are technically allowed by the LDAPv3 specification (and should be treated as anonymous simple authentication), they may introduce security problems in applications that do not verify that the client actually provided a password.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-schema

Description

Indicates whether schema enforcement is active. When schema enforcement is activated, the directory server ensures that all operations result in entries are valid according to the defined server schema. It is strongly recommended that this option be left enabled to prevent the inadvertent addition of invalid data into the server.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-password-policy

Description

Specifies the name of the password policy that is in effect for users whose entries do not specify an alternate password policy (either via a real or virtual attribute). In addition, the default password policy will be used for providing default parameters for sub-entry based password policies when not provided or supported by the sub-entry itself. This property must reference a password policy and no other type of authentication policy.

Default Value

None

Allowed Values

The DN of any Password Policy.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

disabled-privilege

Description

Specifies the name of a privilege that should not be evaluated by the server. If a privilege is disabled, then it is assumed that all clients (including unauthenticated clients) have that privilege.

Default Value

If no values are defined, then the server enforces all privileges.

Allowed Values

backend-backup

Allows the user to request that the server process backup tasks.

backend-restore

Allows the user to request that the server process restore tasks.

bypass-acl

Allows the associated user to bypass access control checks performed by the server.

bypass-lockdown

Allows the associated user to bypass server lockdown mode.

cancel-request

Allows the user to cancel operations in progress on other client connections.

changelog-read

The privilege that provides the ability to perform read operations on the changelog

config-read

Allows the associated user to read the server configuration.

config-write

Allows the associated user to update the server configuration. The config-read privilege is also required.

data-sync

Allows the user to participate in data synchronization.

disconnect-client

Allows the user to terminate other client connections.

jmx-notify

Allows the associated user to subscribe to receive JMX notifications.

jmx-read

Allows the associated user to perform JMX read operations.

jmx-write

Allows the associated user to perform JMX write operations.

ldif-export

Allows the user to request that the server process LDIF export tasks.

ldif-import

Allows the user to request that the server process LDIF import tasks.

modify-acl

Allows the associated user to modify the server's access control configuration.

password-reset

Allows the user to reset user passwords.

privilege-change

Allows the user to make changes to the set of defined root privileges, as well as to grant and revoke privileges for users.

proxied-auth

Allows the user to use the proxied authorization control, or to perform a bind that specifies an alternate authorization identity.

server-lockdown

Allows the user to place and bring the server of lockdown mode.

server-restart

Allows the user to request that the server perform an in-core restart.

server-shutdown

Allows the user to request that the server shut down.

subentry-write

Allows the associated user to perform LDAP subentry write operations.

unindexed-search

Allows the user to request that the server process a search that cannot be optimized using server indexes.

update-schema

Allows the user to make changes to the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

etime-resolution

Description

Specifies the resolution to use for operation elapsed processing time (etime) measurements.

Default Value

milliseconds

Allowed Values

milliseconds

Use millisecond resolution.

nanoseconds

Use nanosecond resolution.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

idle-time-limit

Description

Specifies the maximum length of time that a client connection may remain established since its last completed operation. A value of "0 seconds" indicates that no idle time limit is enforced.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

invalid-attribute-syntax-behavior

Description

Specifies how the directory server should handle operations whenever an attribute value violates the associated attribute syntax.

Default Value

reject

Allowed Values

accept

The directory server silently accepts attribute values that are invalid according to their associated syntax. Matching operations targeting those values may not behave as expected.

reject

The directory server rejects attribute values that are invalid according to their associated syntax.

warn

The directory server accepts attribute values that are invalid according to their associated syntax, but also logs a warning message to the error log. Matching operations targeting those values may not behave as expected.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lookthrough-limit

Description

Specifies the maximum number of entries that the directory server should "look through" in the course of processing a search request. This includes any entry that the server must examine in the course of processing the request, regardless of whether it actually matches the search criteria. A value of 0 indicates that no lookthrough limit is enforced. Note that this is the default server-wide limit, but it may be overridden on a per-user basis using the ds-rlim-lookthrough-limit operational attribute.

Default Value

5000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-allowed-client-connections

Description

Specifies the maximum number of client connections that may be established at any given time A value of 0 indicates that unlimited client connection is allowed.

Default Value

0

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-internal-buffer-size

Description

The threshold capacity beyond which internal cached buffers used for encoding and decoding entries and protocol messages will be trimmed after use. Individual buffers may grow very large when encoding and decoding large entries and protocol messages and should be reduced in size when they are no longer needed. This setting specifies the threshold at which a buffer is determined to have grown too big and should be trimmed down after use.

Default Value

32 KB

Allowed Values

Lower value is 512.Upper value is 1000000000.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-psearches

Description

Defines the maximum number of concurrent persistent searches that can be performed on directory server The persistent search mechanism provides an active channel through which entries that change, and information about the changes that occur, can be communicated. Because each persistent search operation consumes resources, limiting the number of simultaneous persistent searches keeps the performance impact minimal. A value of -1 indicates that there is no limit on the persistent searches.

Default Value

-1

Allowed Values

An integer value. Lower value is 0. A value of "-1" or "unlimited" for no limit.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

notify-abandoned-operations

Description

Indicates whether the directory server should send a response to any operation that is interrupted via an abandon request. The LDAP specification states that abandoned operations should not receive any response, but this may cause problems with client applications that always expect to receive a response to each request.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

proxied-authorization-identity-mapper

Description

Specifies the name of the identity mapper to map authorization ID values (using the "u:" form) provided in the proxied authorization control to the corresponding user entry.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

reject-unauthenticated-requests

Description

Indicates whether the directory server should reject any request (other than bind or StartTLS requests) received from a client that has not yet been authenticated, whose last authentication attempt was unsuccessful, or whose last authentication attempt used anonymous authentication.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

return-bind-error-messages

Description

Indicates whether responses for failed bind operations should include a message string providing the reason for the authentication failure. Note that these messages may include information that could potentially be used by an attacker. If this option is disabled, then these messages appears only in the server's access log.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

save-config-on-successful-startup

Description

Indicates whether the directory server should save a copy of its configuration whenever the startup process completes successfully. This ensures that the server provides a "last known good" configuration, which can be used as a reference (or copied into the active config) if the server fails to start with the current "active" configuration.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-error-result-code

Description

Specifies the numeric value of the result code when request processing fails due to an internal server error.

Default Value

80

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

single-structural-objectclass-behavior

Description

Specifies how the directory server should handle operations an entry does not contain a structural object class or contains multiple structural classes.

Default Value

reject

Allowed Values

accept

The directory server silently accepts entries that do not contain exactly one structural object class. Certain schema features that depend on the entry's structural class may not behave as expected.

reject

The directory server rejects entries that do not contain exactly one structural object class.

warn

The directory server accepts entries that do not contain exactly one structural object class, but also logs a warning message to the error log. Certain schema features that depend on the entry's structural class may not behave as expected.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

size-limit

Description

Specifies the maximum number of entries that can be returned to the client during a single search operation. A value of 0 indicates that no size limit is enforced. Note that this is the default server-wide limit, but it may be overridden on a per-user basis using the ds-rlim-size-limit operational attribute.

Default Value

1000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

smtp-server

Description

Specifies the address (and optional port number) for a mail server that can be used to send email messages via SMTP. It may be an IP address or resolvable hostname, optionally followed by a colon and a port number.

Default Value

If no values are defined, then the server cannot send email via SMTP.

Allowed Values

A hostname, optionally followed by a ":" followed by a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

subordinate-base-dn

Description

Specifies the set of base DNs used for singleLevel, wholeSubtree, and subordinateSubtree searches based at the root DSE.

Default Value

The set of all user-defined suffixes is used.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-limit

Description

Specifies the maximum length of time that should be spent processing a single search operation. A value of 0 seconds indicates that no time limit is enforced. Note that this is the default server-wide time limit, but it may be overridden on a per-user basis using the ds-rlim-time-limit

operational attribute.

Default Value

60 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-transaction-ids

Description

Indicates whether the directory server should trust the transaction ids that may be received from requests, either through a LDAP control or through a HTTP header.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the kinds of write operations the directory server can process.

Default Value

enabled

Allowed Values

disabled

The directory server rejects all write operations that are requested of it, regardless of their origin.

enabled

The directory server attempts to process all write operations that are requested of it, regardless of their origin.

internal-only

The directory server attempts to process write operations requested as internal operations or through synchronization, but rejects any such operations requested from external clients.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-group-implementation-prop(1)

Name

dsconfig get-group-implementation-prop - Shows Group Implementation properties

Synopsis

`dsconfig get-group-implementation-prop` {options}

Description

Shows Group Implementation properties.

Options

The `dsconfig get-group-implementation-prop` command takes the following options:

`--implementation-name {name}`

The name of the Group Implementation.

Group Implementation properties depend on the Group Implementation type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

`dynamic-group-implementation`

Default {name}: Dynamic Group Implementation

Enabled by default: true

See Dynamic Group Implementation for the properties of this Group Implementation type.

`static-group-implementation`

Default {name}: Static Group Implementation

Enabled by default: true

See Static Group Implementation for the properties of this Group Implementation type.

`virtual-static-group-implementation`

Default {name}: Virtual Static Group Implementation

Enabled by default: true

See Virtual Static Group Implementation for the properties of this Group Implementation type.

`--property {property}`

The name of a property to be displayed.

Group Implementation properties depend on the Group Implementation type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

`dynamic-group-implementation`

Default {property}: Dynamic Group Implementation

Enabled by default: true

See Dynamic Group Implementation for the properties of this Group Implementation type.

`static-group-implementation`

Default {property}: Static Group Implementation

Enabled by default: true

See Static Group Implementation for the properties of this Group Implementation type.

`virtual-static-group-implementation`

Default {property}: Virtual Static Group Implementation

Enabled by default: true

See Virtual Static Group Implementation for the properties of this Group Implementation type.

`-E | --record`

Modifies the display output to show one property value per line.

Group Implementation properties depend on the Group Implementation type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

`dynamic-group-implementation`

Default null: Dynamic Group Implementation

Enabled by default: true

See Dynamic Group Implementation for the properties of this Group Implementation type.

`static-group-implementation`

Default null: Static Group Implementation

Enabled by default: true

See Static Group Implementation for the properties of this Group Implementation type.

`virtual-static-group-implementation`

Default null: Virtual Static Group Implementation

Enabled by default: true

See Virtual Static Group Implementation for the properties of this Group Implementation type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Group Implementation properties depend on the Group Implementation type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

`dynamic-group-implementation`

Default {unit}: Dynamic Group Implementation

Enabled by default: true

See Dynamic Group Implementation for the properties of this Group Implementation type.

`static-group-implementation`

Default {unit}: Static Group Implementation

Enabled by default: true

See Static Group Implementation for the properties of this Group Implementation type.

`virtual-static-group-implementation`

Default {unit}: Virtual Static Group Implementation

Enabled by default: true

See Virtual Static Group Implementation for the properties of this Group Implementation type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Group Implementation properties depend on the Group Implementation type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

`dynamic-group-implementation`

Default {unit}: Dynamic Group Implementation

Enabled by default: true

See Dynamic Group Implementation for the properties of this Group Implementation type.

`static-group-implementation`

Default {unit}: Static Group Implementation

Enabled by default: true

See Static Group Implementation for the properties of this Group Implementation type.

`virtual-static-group-implementation`

Default {unit}: Virtual Static Group Implementation

Enabled by default: true

See Virtual Static Group Implementation for the properties of this Group Implementation type.

Dynamic Group Implementation

Group Implementations of type dynamic-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Dynamic Group Implementation implementation.

Default Value

org.opends.server.extensions.DynamicGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Static Group Implementation

Group Implementations of type static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Group Implementation implementation.

Default Value

org.opends.server.extensions.StaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Virtual Static Group Implementation

Group Implementations of type virtual-static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Virtual Static Group Implementation implementation.

Default Value

org.opends.server.extensions.VirtualStaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-http-authorization-mechanism-prop(1)

Name

dsconfig get-http-authorization-mechanism-prop - Shows HTTP Authorization Mechanism properties

Synopsis

`dsconfig get-http-authorization-mechanism-prop` {options}

Description

Shows HTTP Authorization Mechanism properties.

Options

The `dsconfig get-http-authorization-mechanism-prop` command takes the following options:

`--mechanism-name {name}`

The name of the HTTP Authorization Mechanism.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

`http-anonymous-authorization-mechanism`

Default {name}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See HTTP Anonymous Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-basic-authorization-mechanism`

Default {name}: HTTP Basic Authorization Mechanism

Enabled by default: true

See HTTP Basic Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-cts-authorization-mechanism`

Default {name}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Cts Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-file-authorization-mechanism`

Default {name}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 File Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-openam-authorization-mechanism`

Default {name}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Openam Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-token-introspection-authorization-mechanism`

Default {name}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Token Introspection Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`--property {property}`

The name of a property to be displayed.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

`http-anonymous-authorization-mechanism`

Default {property}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See HTTP Anonymous Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-basic-authorization-mechanism`

Default {property}: HTTP Basic Authorization Mechanism

Enabled by default: true

See HTTP Basic Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-cts-authorization-mechanism`

Default {property}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Cts Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-file-authorization-mechanism`

Default {property}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 File Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-openam-authorization-mechanism`

Default {property}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Openam Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-token-introspection-authorization-mechanism`

Default {property}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Token Introspection Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`-E | --record`

Modifies the display output to show one property value per line.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the null you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

`http-anonymous-authorization-mechanism`

Default null: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See HTTP Anonymous Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-basic-authorization-mechanism`

Default null: HTTP Basic Authorization Mechanism

Enabled by default: true

See HTTP Basic Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-cts-authorization-mechanism`

Default null: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Cts Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-file-authorization-mechanism`

Default null: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 File Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-openam-authorization-mechanism`

Default null: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Openam Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-token-introspection-authorization-mechanism`

Default null: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Token Introspection Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

`http-anonymous-authorization-mechanism`

Default {unit}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See HTTP Anonymous Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-basic-authorization-mechanism`

Default {unit}: HTTP Basic Authorization Mechanism

Enabled by default: true

See HTTP Basic Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-cts-authorization-mechanism`

Default {unit}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Cts Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-file-authorization-mechanism`

Default {unit}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 File Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-openam-authorization-mechanism`

Default {unit}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Openam Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-token-introspection-authorization-mechanism`

Default {unit}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Token Introspection Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

`http-anonymous-authorization-mechanism`

Default {unit}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See HTTP Anonymous Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-basic-authorization-mechanism`

Default {unit}: HTTP Basic Authorization Mechanism

Enabled by default: true

See HTTP Basic Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-cts-authorization-mechanism`

Default {unit}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Cts Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-file-authorization-mechanism`

Default {unit}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 File Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-openam-authorization-mechanism`

Default {unit}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Openam Authorization Mechanism for the properties of this HTTP

Authorization Mechanism type.

`http-oauth2-token-introspection-authorization-mechanism`

Default {unit}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Token Introspection Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

HTTP Anonymous Authorization Mechanism

HTTP Authorization Mechanisms of type http-anonymous-authorization-mechanism have the following properties:

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Anonymous Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpAnonymousAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-dn

Description

The authorization DN which will be used for performing anonymous operations.

Default Value

By default, operations will be performed using an anonymously bound connection.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

HTTP Basic Authorization Mechanism

HTTP Authorization Mechanisms of type http-basic-authorization-mechanism have the following

properties:

alt-authentication-enabled

Description

Specifies whether user credentials may be provided using alternative headers to the standard 'Authorize' header.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-password-header

Description

Alternate HTTP headers to get the user's password from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-username-header

Description

Alternate HTTP headers to get the user's name from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper used to get the user's entry corresponding to the user-id provided in the HTTP authentication header.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Basic Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Basic Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpBasicAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es):

org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

HTTP Oauth2 Cts Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-cts-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

The base DN of the Core Token Service where access token are stored. (example: ou=famrecords,ou=openam-session,ou=tokens,dc=example,dc=com)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Cts Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2CtsAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

HTTP Oauth2 File Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-file-authorization-mechanism have the

following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-directory

Description

Directory containing token files. File names must be equal to the token strings. The file content must a JSON object with the following attributes: 'scope', 'expireTime' and all the field(s) needed to resolve the authzIdTemplate.

Default Value

oauth2-demo/

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 File Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2FileAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

HTTP Oauth2 Openam Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-openam-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Openam Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2OpenAmAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Openam Authorization Mechanism .

Default Value

By default the system key manager(s) will be used.

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-info-url

Description

Defines the OpenAM endpoint URL where the access-token resolution request should be sent.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

HTTP Oauth2 Token Introspection Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-token-introspection-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-id

Description

Client's ID to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-secret

Description

Client's secret to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Token Introspection Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2TokenIntrospectionAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Token Introspection Authorization Mechanism .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-introspection-url

Description

Defines the token introspection endpoint URL where the access-token resolution request should be sent. (example: http://example.com/introspect)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

dsconfig get-http-endpoint-prop(1)

Name

dsconfig get-http-endpoint-prop - Shows HTTP Endpoint properties

Synopsis

`dsconfig get-http-endpoint-prop` {options}

Description

Shows HTTP Endpoint properties.

Options

The `dsconfig get-http-endpoint-prop` command takes the following options:

`--endpoint-name {name}`

The name of the HTTP Endpoint.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

`admin-endpoint`

Default {name}: Admin Endpoint

Enabled by default: true

See Admin Endpoint for the properties of this HTTP Endpoint type.

`rest2ldap-endpoint`

Default {name}: Rest2ldap Endpoint

Enabled by default: true

See Rest2ldap Endpoint for the properties of this HTTP Endpoint type.

`--property {property}`

The name of a property to be displayed.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

`admin-endpoint`

Default {property}: Admin Endpoint

Enabled by default: true

See Admin Endpoint for the properties of this HTTP Endpoint type.

`rest2ldap-endpoint`

Default {property}: Rest2ldap Endpoint

Enabled by default: true

See Rest2ldap Endpoint for the properties of this HTTP Endpoint type.

`-E | --record`

Modifies the display output to show one property value per line.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the null you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

`admin-endpoint`

Default null: Admin Endpoint

Enabled by default: true

See Admin Endpoint for the properties of this HTTP Endpoint type.

`rest2ldap-endpoint`

Default null: Rest2ldap Endpoint

Enabled by default: true

See Rest2ldap Endpoint for the properties of this HTTP Endpoint type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

`admin-endpoint`

Default {unit}: Admin Endpoint

Enabled by default: true

See Admin Endpoint for the properties of this HTTP Endpoint type.

`rest2ldap-endpoint`

Default {unit}: Rest2ldap Endpoint

Enabled by default: true

See Rest2ldap Endpoint for the properties of this HTTP Endpoint type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

`admin-endpoint`

Default {unit}: Admin Endpoint

Enabled by default: true

See Admin Endpoint for the properties of this HTTP Endpoint type.

`rest2ldap-endpoint`

Default {unit}: Rest2ldap Endpoint

Enabled by default: true

See Rest2ldap Endpoint for the properties of this HTTP Endpoint type.

Admin Endpoint

HTTP Endpoints of type admin-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Admin Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.AdminEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Rest2ldap Endpoint

HTTP Endpoints of type rest2ldap-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

config-directory

Description

The directory containing the Rest2Ldap configuration file(s) for this specific endpoint. The directory must be readable by the server and may contain multiple configuration files, one for each supported version of the REST endpoint. If a relative path is used then it will be resolved against the server's instance directory.

Default Value

None

Allowed Values

A directory that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Rest2ldap Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.Rest2LdapEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-identity-mapper-prop(1)

Name

dsconfig get-identity-mapper-prop - Shows Identity Mapper properties

Synopsis

`dsconfig get-identity-mapper-prop` {options}

Description

Shows Identity Mapper properties.

Options

The `dsconfig get-identity-mapper-prop` command takes the following options:

`--mapper-name {name}`

The name of the Identity Mapper.

Identity Mapper properties depend on the Identity Mapper type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

`exact-match-identity-mapper`

Default {name}: Exact Match Identity Mapper

Enabled by default: true

See Exact Match Identity Mapper for the properties of this Identity Mapper type.

`regular-expression-identity-mapper`

Default {name}: Regular Expression Identity Mapper

Enabled by default: true

See Regular Expression Identity Mapper for the properties of this Identity Mapper type.

`--property {property}`

The name of a property to be displayed.

Identity Mapper properties depend on the Identity Mapper type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

`exact-match-identity-mapper`

Default {property}: Exact Match Identity Mapper

Enabled by default: true

See Exact Match Identity Mapper for the properties of this Identity Mapper type.

`regular-expression-identity-mapper`

Default {property}: Regular Expression Identity Mapper

Enabled by default: true

See Regular Expression Identity Mapper for the properties of this Identity Mapper type.

`-E | --record`

Modifies the display output to show one property value per line.

Identity Mapper properties depend on the Identity Mapper type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

`exact-match-identity-mapper`

Default null: Exact Match Identity Mapper

Enabled by default: true

See Exact Match Identity Mapper for the properties of this Identity Mapper type.

`regular-expression-identity-mapper`

Default null: Regular Expression Identity Mapper

Enabled by default: true

See Regular Expression Identity Mapper for the properties of this Identity Mapper type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Identity Mapper properties depend on the Identity Mapper type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

`exact-match-identity-mapper`

Default {unit}: Exact Match Identity Mapper

Enabled by default: true

See Exact Match Identity Mapper for the properties of this Identity Mapper type.

`regular-expression-identity-mapper`

Default {unit}: Regular Expression Identity Mapper

Enabled by default: true

See Regular Expression Identity Mapper for the properties of this Identity Mapper type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Identity Mapper properties depend on the Identity Mapper type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

`exact-match-identity-mapper`

Default {unit}: Exact Match Identity Mapper

Enabled by default: true

See Exact Match Identity Mapper for the properties of this Identity Mapper type.

`regular-expression-identity-mapper`

Default {unit}: Regular Expression Identity Mapper

Enabled by default: true

See Regular Expression Identity Mapper for the properties of this Identity Mapper type.

Exact Match Identity Mapper

Identity Mappers of type exact-match-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Exact Match Identity Mapper implementation.

Default Value

org.opends.server.extensions.ExactMatchIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the attribute whose value should exactly match the ID string provided to this identity mapper. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry. The internal search performed includes a logical OR across all of these values.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs will be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Regular Expression Identity Mapper

Identity Mappers of type regular-expression-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Regular Expression Identity Mapper implementation.

Default Value

org.opends.server.extensions.RegularExpressionIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name or OID of the attribute whose value should match the provided identifier string after it has been processed by the associated regular expression. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the base DN(s) that should be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all the specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

match-pattern

Description

Specifies the regular expression pattern that is used to identify portions of the ID string that will be replaced. Any portion of the ID string that matches this pattern is replaced in accordance with the provided replace pattern (or is removed if no replace pattern is specified). If multiple substrings within the given ID string match this pattern, all occurrences are replaced. If no part of the given ID string matches this pattern, the ID string is not altered. Exactly one match pattern value must be provided, and it must be a valid regular expression as described in the API documentation for the java.util.regex.Pattern class, including support for capturing groups.

Default Value

None

Allowed Values

Any valid regular expression pattern which is supported by the javax.util.regex.Pattern class (see http://download.oracle.com/docs/cd/E17409_01/javase/6/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 6).

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replace-pattern

Description

Specifies the replacement pattern that should be used for substrings in the ID string that match the provided regular expression pattern. If no replacement pattern is provided, then any matching portions of the ID string will be removed (i.e., replaced with an empty string). The replacement pattern may include a string from a capturing group by using a dollar sign ($) followed by an integer value that indicates which capturing group should be used.

Default Value

The replace pattern will be the empty string.

Allowed Values

Any valid replacement string that is allowed by the javax.util.regex.Matcher class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-key-manager-provider-prop(1)

Name

dsconfig get-key-manager-provider-prop - Shows Key Manager Provider properties

Synopsis

`dsconfig get-key-manager-provider-prop` {options}

Description

Shows Key Manager Provider properties.

Options

The `dsconfig get-key-manager-provider-prop` command takes the following options:

`--provider-name {name}`

The name of the Key Manager Provider.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

`file-based-key-manager-provider`

Default {name}: File Based Key Manager Provider

Enabled by default: true

See File Based Key Manager Provider for the properties of this Key Manager Provider type.

`ldap-key-manager-provider`

Default {name}: LDAP Key Manager Provider

Enabled by default: true

See LDAP Key Manager Provider for the properties of this Key Manager Provider type.

`pkcs11-key-manager-provider`

Default {name}: PKCS11 Key Manager Provider

Enabled by default: true

See PKCS11 Key Manager Provider for the properties of this Key Manager Provider type.

`--property {property}`

The name of a property to be displayed.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

`file-based-key-manager-provider`

Default {property}: File Based Key Manager Provider

Enabled by default: true

See File Based Key Manager Provider for the properties of this Key Manager Provider type.

`ldap-key-manager-provider`

Default {property}: LDAP Key Manager Provider

Enabled by default: true

See LDAP Key Manager Provider for the properties of this Key Manager Provider type.

`pkcs11-key-manager-provider`

Default {property}: PKCS11 Key Manager Provider

Enabled by default: true

See PKCS11 Key Manager Provider for the properties of this Key Manager Provider type.

`-E | --record`

Modifies the display output to show one property value per line.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

`file-based-key-manager-provider`

Default null: File Based Key Manager Provider

Enabled by default: true

See File Based Key Manager Provider for the properties of this Key Manager Provider type.

`ldap-key-manager-provider`

Default null: LDAP Key Manager Provider

Enabled by default: true

See LDAP Key Manager Provider for the properties of this Key Manager Provider type.

`pkcs11-key-manager-provider`

Default null: PKCS11 Key Manager Provider

Enabled by default: true

See PKCS11 Key Manager Provider for the properties of this Key Manager Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

`file-based-key-manager-provider`

Default {unit}: File Based Key Manager Provider

Enabled by default: true

See File Based Key Manager Provider for the properties of this Key Manager Provider type.

`ldap-key-manager-provider`

Default {unit}: LDAP Key Manager Provider

Enabled by default: true

See LDAP Key Manager Provider for the properties of this Key Manager Provider type.

`pkcs11-key-manager-provider`

Default {unit}: PKCS11 Key Manager Provider

Enabled by default: true

See PKCS11 Key Manager Provider for the properties of this Key Manager Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

`file-based-key-manager-provider`

Default {unit}: File Based Key Manager Provider

Enabled by default: true

See File Based Key Manager Provider for the properties of this Key Manager Provider type.

`ldap-key-manager-provider`

Default {unit}: LDAP Key Manager Provider

Enabled by default: true

See LDAP Key Manager Provider for the properties of this Key Manager Provider type.

`pkcs11-key-manager-provider`

Default {unit}: PKCS11 Key Manager Provider

Enabled by default: true

See PKCS11 Key Manager Provider for the properties of this Key Manager Provider type.

File Based Key Manager Provider

Key Manager Providers of type file-based-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Key Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well. If no value is provided, the JVM-default value is used. Changes to this configuration attribute will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

LDAP Key Manager Provider

Key Manager Providers of type ldap-key-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Key Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider

is accessed.

Advanced Property

No

Read-only

No

PKCS11 Key Manager Provider

Key Manager Providers of type pkcs11-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Key Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11KeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig get-log-publisher-prop(1)

Name

dsconfig get-log-publisher-prop - Shows Log Publisher properties

Synopsis

`dsconfig get-log-publisher-prop` {options}

Description

Shows Log Publisher properties.

Options

The `dsconfig get-log-publisher-prop` command takes the following options:

`--publisher-name {name}`

The name of the Log Publisher.

Log Publisher properties depend on the Log Publisher type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

`csv-file-access-log-publisher`

Default {name}: Csv File Access Log Publisher

Enabled by default: true

See Csv File Access Log Publisher for the properties of this Log Publisher type.

`csv-file-http-access-log-publisher`

Default {name}: Csv File HTTP Access Log Publisher

Enabled by default: true

See Csv File HTTP Access Log Publisher for the properties of this Log Publisher type.

`external-access-log-publisher`

Default {name}: External Access Log Publisher

Enabled by default: true

See External Access Log Publisher for the properties of this Log Publisher type.

`external-http-access-log-publisher`

Default {name}: External HTTP Access Log Publisher

Enabled by default: true

See External HTTP Access Log Publisher for the properties of this Log Publisher type.

`file-based-access-log-publisher`

Default {name}: File Based Access Log Publisher

Enabled by default: true

See File Based Access Log Publisher for the properties of this Log Publisher type.

`file-based-audit-log-publisher`

Default {name}: File Based Audit Log Publisher

Enabled by default: true

See File Based Audit Log Publisher for the properties of this Log Publisher type.

`file-based-debug-log-publisher`

Default {name}: File Based Debug Log Publisher

Enabled by default: true

See File Based Debug Log Publisher for the properties of this Log Publisher type.

`file-based-error-log-publisher`

Default {name}: File Based Error Log Publisher

Enabled by default: true

See File Based Error Log Publisher for the properties of this Log Publisher type.

`file-based-http-access-log-publisher`

Default {name}: File Based HTTP Access Log Publisher

Enabled by default: true

See File Based HTTP Access Log Publisher for the properties of this Log Publisher type.

`json-file-access-log-publisher`

Default {name}: Json File Access Log Publisher

Enabled by default: true

See Json File Access Log Publisher for the properties of this Log Publisher type.

`json-file-http-access-log-publisher`

Default {name}: Json File HTTP Access Log Publisher

Enabled by default: true

See Json File HTTP Access Log Publisher for the properties of this Log Publisher type.

`--property {property}`

The name of a property to be displayed.

Log Publisher properties depend on the Log Publisher type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

`csv-file-access-log-publisher`

Default {property}: Csv File Access Log Publisher

Enabled by default: true

See Csv File Access Log Publisher for the properties of this Log Publisher type.

`csv-file-http-access-log-publisher`

Default {property}: Csv File HTTP Access Log Publisher

Enabled by default: true

See Csv File HTTP Access Log Publisher for the properties of this Log Publisher type.

`external-access-log-publisher`

Default {property}: External Access Log Publisher

Enabled by default: true

See External Access Log Publisher for the properties of this Log Publisher type.

`external-http-access-log-publisher`

Default {property}: External HTTP Access Log Publisher

Enabled by default: true

See External HTTP Access Log Publisher for the properties of this Log Publisher type.

`file-based-access-log-publisher`

Default {property}: File Based Access Log Publisher

Enabled by default: true

See File Based Access Log Publisher for the properties of this Log Publisher type.

`file-based-audit-log-publisher`

Default {property}: File Based Audit Log Publisher

Enabled by default: true

See File Based Audit Log Publisher for the properties of this Log Publisher type.

`file-based-debug-log-publisher`

Default {property}: File Based Debug Log Publisher

Enabled by default: true

See File Based Debug Log Publisher for the properties of this Log Publisher type.

`file-based-error-log-publisher`

Default {property}: File Based Error Log Publisher

Enabled by default: true

See File Based Error Log Publisher for the properties of this Log Publisher type.

`file-based-http-access-log-publisher`

Default {property}: File Based HTTP Access Log Publisher

Enabled by default: true

See File Based HTTP Access Log Publisher for the properties of this Log Publisher type.

`json-file-access-log-publisher`

Default {property}: Json File Access Log Publisher

Enabled by default: true

See Json File Access Log Publisher for the properties of this Log Publisher type.

`json-file-http-access-log-publisher`

Default {property}: Json File HTTP Access Log Publisher

Enabled by default: true

See Json File HTTP Access Log Publisher for the properties of this Log Publisher type.

`-E | --record`

Modifies the display output to show one property value per line.

Log Publisher properties depend on the Log Publisher type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

`csv-file-access-log-publisher`

Default null: Csv File Access Log Publisher

Enabled by default: true

See Csv File Access Log Publisher for the properties of this Log Publisher type.

`csv-file-http-access-log-publisher`

Default null: Csv File HTTP Access Log Publisher

Enabled by default: true

See Csv File HTTP Access Log Publisher for the properties of this Log Publisher type.

`external-access-log-publisher`

Default null: External Access Log Publisher

Enabled by default: true

See External Access Log Publisher for the properties of this Log Publisher type.

`external-http-access-log-publisher`

Default null: External HTTP Access Log Publisher

Enabled by default: true

See External HTTP Access Log Publisher for the properties of this Log Publisher type.

`file-based-access-log-publisher`

Default null: File Based Access Log Publisher

Enabled by default: true

See File Based Access Log Publisher for the properties of this Log Publisher type.

`file-based-audit-log-publisher`

Default null: File Based Audit Log Publisher

Enabled by default: true

See File Based Audit Log Publisher for the properties of this Log Publisher type.

`file-based-debug-log-publisher`

Default null: File Based Debug Log Publisher

Enabled by default: true

See File Based Debug Log Publisher for the properties of this Log Publisher type.

`file-based-error-log-publisher`

Default null: File Based Error Log Publisher

Enabled by default: true

See File Based Error Log Publisher for the properties of this Log Publisher type.

`file-based-http-access-log-publisher`

Default null: File Based HTTP Access Log Publisher

Enabled by default: true

See File Based HTTP Access Log Publisher for the properties of this Log Publisher type.

`json-file-access-log-publisher`

Default null: Json File Access Log Publisher

Enabled by default: true

See Json File Access Log Publisher for the properties of this Log Publisher type.

`json-file-http-access-log-publisher`

Default null: Json File HTTP Access Log Publisher

Enabled by default: true

See Json File HTTP Access Log Publisher for the properties of this Log Publisher type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Log Publisher properties depend on the Log Publisher type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

`csv-file-access-log-publisher`

Default {unit}: Csv File Access Log Publisher

Enabled by default: true

See Csv File Access Log Publisher for the properties of this Log Publisher type.

`csv-file-http-access-log-publisher`

Default {unit}: Csv File HTTP Access Log Publisher

Enabled by default: true

See Csv File HTTP Access Log Publisher for the properties of this Log Publisher type.

`external-access-log-publisher`

Default {unit}: External Access Log Publisher

Enabled by default: true

See External Access Log Publisher for the properties of this Log Publisher type.

`external-http-access-log-publisher`

Default {unit}: External HTTP Access Log Publisher

Enabled by default: true

See External HTTP Access Log Publisher for the properties of this Log Publisher type.

`file-based-access-log-publisher`

Default {unit}: File Based Access Log Publisher

Enabled by default: true

See File Based Access Log Publisher for the properties of this Log Publisher type.

`file-based-audit-log-publisher`

Default {unit}: File Based Audit Log Publisher

Enabled by default: true

See File Based Audit Log Publisher for the properties of this Log Publisher type.

`file-based-debug-log-publisher`

Default {unit}: File Based Debug Log Publisher

Enabled by default: true

See File Based Debug Log Publisher for the properties of this Log Publisher type.

`file-based-error-log-publisher`

Default {unit}: File Based Error Log Publisher

Enabled by default: true

See File Based Error Log Publisher for the properties of this Log Publisher type.

`file-based-http-access-log-publisher`

Default {unit}: File Based HTTP Access Log Publisher

Enabled by default: true

See File Based HTTP Access Log Publisher for the properties of this Log Publisher type.

`json-file-access-log-publisher`

Default {unit}: Json File Access Log Publisher

Enabled by default: true

See Json File Access Log Publisher for the properties of this Log Publisher type.

`json-file-http-access-log-publisher`

Default {unit}: Json File HTTP Access Log Publisher

Enabled by default: true

See Json File HTTP Access Log Publisher for the properties of this Log Publisher type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Log Publisher properties depend on the Log Publisher type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

`csv-file-access-log-publisher`

Default {unit}: Csv File Access Log Publisher

Enabled by default: true

See Csv File Access Log Publisher for the properties of this Log Publisher type.

`csv-file-http-access-log-publisher`

Default {unit}: Csv File HTTP Access Log Publisher

Enabled by default: true

See Csv File HTTP Access Log Publisher for the properties of this Log Publisher type.

`external-access-log-publisher`

Default {unit}: External Access Log Publisher

Enabled by default: true

See External Access Log Publisher for the properties of this Log Publisher type.

`external-http-access-log-publisher`

Default {unit}: External HTTP Access Log Publisher

Enabled by default: true

See External HTTP Access Log Publisher for the properties of this Log Publisher type.

`file-based-access-log-publisher`

Default {unit}: File Based Access Log Publisher

Enabled by default: true

See File Based Access Log Publisher for the properties of this Log Publisher type.

`file-based-audit-log-publisher`

Default {unit}: File Based Audit Log Publisher

Enabled by default: true

See File Based Audit Log Publisher for the properties of this Log Publisher type.

`file-based-debug-log-publisher`

Default {unit}: File Based Debug Log Publisher

Enabled by default: true

See File Based Debug Log Publisher for the properties of this Log Publisher type.

`file-based-error-log-publisher`

Default {unit}: File Based Error Log Publisher

Enabled by default: true

See File Based Error Log Publisher for the properties of this Log Publisher type.

`file-based-http-access-log-publisher`

Default {unit}: File Based HTTP Access Log Publisher

Enabled by default: true

See File Based HTTP Access Log Publisher for the properties of this Log Publisher type.

`json-file-access-log-publisher`

Default {unit}: Json File Access Log Publisher

Enabled by default: true

See Json File Access Log Publisher for the properties of this Log Publisher type.

`json-file-http-access-log-publisher`

Default {unit}: Json File HTTP Access Log Publisher

Enabled by default: true

See Json File HTTP Access Log Publisher for the properties of this Log Publisher type.

Csv File Access Log Publisher

Log Publishers of type csv-file-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writting in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CsvFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Csv File Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when the tamper-evident option is enabled.

Default Value

3s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Csv File HTTP Access Log Publisher

Log Publishers of type csv-file-http-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File HTTP Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Csv File HTTP Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when secure option is enabled.

Default Value

3s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

External Access Log Publisher

Log Publishers of type external-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External Access Log Publisher. The content of the

JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External Access Log Publisher implementation.

Default Value

org.opends.server.loggers.ExternalAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

External HTTP Access Log Publisher

Log Publishers of type external-http-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External HTTP Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Access Log Publisher

Log Publishers of type file-based-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the access log.

Default Value

multi-line

Allowed Values

combined

Combine log records for operation requests and responses into a single record. This format should be used when log records are to be filtered based on response criteria (e.g. result code).

multi-line

Outputs separate log records for operation requests and responses.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Audit Log Publisher

Log Publishers of type file-based-audit-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Audit Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Audit Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAuditLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Audit Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Audit Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Audit Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Audit Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Debug Log Publisher

Log Publishers of type file-based-debug-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Debug Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-include-throwable-cause

Description

Indicates whether to include the cause of exceptions in exception thrown and caught messages logged by default.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-entry-arguments

Description

Indicates whether to include method arguments in debug messages logged by default.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-return-value

Description

Indicates whether to include the return value in debug messages logged by default.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-throwable-stack-frames

Description

Indicates the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Debug Log Publisher implementation.

Default Value

org.opends.server.loggers.TextDebugLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Debug Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Debug Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Debug Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Debug Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Error Log Publisher

Log Publishers of type file-based-error-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Error Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer will be flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-severity

Description

Specifies the default severity levels for the logger.

Default Value

error warning

Allowed Values

all

Messages of all severity levels are logged.

debug

The error log severity that is used for messages that provide debugging information triggered during processing.

error

The error log severity that is used for messages that provide information about errors which may force the server to shut down or operate in a significantly degraded state.

info

The error log severity that is used for messages that provide information about significant events within the server that are not warnings or errors.

none

No messages of any severity are logged by default. This value is intended to be used in conjunction with the override-severity property to define an error logger that will publish no error message beside the errors of a given category.

notice

The error log severity that is used for the most important informational messages (i.e., information that should almost always be logged but is not associated with a warning or error condition).

warning

The error log severity that is used for messages that provide information about warnings triggered during processing.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Error Log Publisher implementation.

Default Value

org.opends.server.loggers.TextErrorLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Error Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Error Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

override-severity

Description

Specifies the override severity levels for the logger based on the category of the messages. Each override severity level should include the category and the severity levels to log for that category, for example, core=error,info,warning. Valid categories are: core, extensions, protocol, config, log, util, schema, plugin, jeb, backend, tools, task, access-control, admin, sync, version, quicksetup, admin-tool, dsconfig, user-defined. Valid severities are: all, error, info, warning, notice, debug.

Default Value

All messages with the default severity levels are logged.

Allowed Values

A string in the form category=severity1,severity2...

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Error Log Publisher . When multiple policies are used, log files will be cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files will never be cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Error Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based HTTP Access Log Publisher

Log Publishers of type file-based-http-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based HTTP Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based HTTP Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the HTTP access log.

Default Value

cs-host c-ip cs-username x-datetime cs-method cs-uri-stem cs-uri-query cs-version sc-status cs(User-Agent) x-connection-id x-etime x-transaction-id

Allowed Values

A space separated list of fields describing the extended log format to be used for logging HTTP accesses. Available values are listed on the W3C working draft http://www.w3.org/TR/WD-logfile.html and Microsoft website http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/676400bc-8969-4aa7-851a-9319490a9bbb.mspx?mfr=true
OpenDJ supports the following standard fields: "c-ip", "c-port", "cs-host", "cs-method", "cs-uri", "cs-uri-stem", "cs-uri-query", "cs(User-Agent)", "cs-username", "cs-version", "s-computername", "s-ip", "s-port", "sc-status". OpenDJ supports the following application specific field extensions: "x-connection-id" displays the internal connection ID assigned to the HTTP client connection, "x-datetime" displays the completion date and time for the logged HTTP request and its ouput is controlled by the "ds-cfg-log-record-time-format" property, "x-etime" displays the total execution time for the logged HTTP request, "x-transaction-id" displays the transaction id associated to a request

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Json File Access Log Publisher

Log Publishers of type json-file-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.JsonFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Json File HTTP Access Log Publisher

Log Publishers of type json-file-http-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-log-retention-policy-prop(1)

Name

dsconfig get-log-retention-policy-prop - Shows Log Retention Policy properties

Synopsis

`dsconfig get-log-retention-policy-prop` {options}

Description

Shows Log Retention Policy properties.

Options

The `dsconfig get-log-retention-policy-prop` command takes the following options:

`--policy-name {name}`

The name of the Log Retention Policy.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

`file-count-log-retention-policy`

Default {name}: File Count Log Retention Policy

Enabled by default: false

See File Count Log Retention Policy for the properties of this Log Retention Policy type.

`free-disk-space-log-retention-policy`

Default {name}: Free Disk Space Log Retention Policy

Enabled by default: false

See Free Disk Space Log Retention Policy for the properties of this Log Retention Policy type.

`size-limit-log-retention-policy`

Default {name}: Size Limit Log Retention Policy

Enabled by default: false

See Size Limit Log Retention Policy for the properties of this Log Retention Policy type.

`--property {property}`

The name of a property to be displayed.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

`file-count-log-retention-policy`

Default {property}: File Count Log Retention Policy

Enabled by default: false

See File Count Log Retention Policy for the properties of this Log Retention Policy type.

`free-disk-space-log-retention-policy`

Default {property}: Free Disk Space Log Retention Policy

Enabled by default: false

See Free Disk Space Log Retention Policy for the properties of this Log Retention Policy type.

`size-limit-log-retention-policy`

Default {property}: Size Limit Log Retention Policy

Enabled by default: false

See Size Limit Log Retention Policy for the properties of this Log Retention Policy type.

`-E | --record`

Modifies the display output to show one property value per line.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

`file-count-log-retention-policy`

Default null: File Count Log Retention Policy

Enabled by default: false

See File Count Log Retention Policy for the properties of this Log Retention Policy type.

`free-disk-space-log-retention-policy`

Default null: Free Disk Space Log Retention Policy

Enabled by default: false

See Free Disk Space Log Retention Policy for the properties of this Log Retention Policy type.

`size-limit-log-retention-policy`

Default null: Size Limit Log Retention Policy

Enabled by default: false

See Size Limit Log Retention Policy for the properties of this Log Retention Policy type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

`file-count-log-retention-policy`

Default {unit}: File Count Log Retention Policy

Enabled by default: false

See File Count Log Retention Policy for the properties of this Log Retention Policy type.

`free-disk-space-log-retention-policy`

Default {unit}: Free Disk Space Log Retention Policy

Enabled by default: false

See Free Disk Space Log Retention Policy for the properties of this Log Retention Policy type.

`size-limit-log-retention-policy`

Default {unit}: Size Limit Log Retention Policy

Enabled by default: false

See Size Limit Log Retention Policy for the properties of this Log Retention Policy type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

`file-count-log-retention-policy`

Default {unit}: File Count Log Retention Policy

Enabled by default: false

See File Count Log Retention Policy for the properties of this Log Retention Policy type.

`free-disk-space-log-retention-policy`

Default {unit}: Free Disk Space Log Retention Policy

Enabled by default: false

See Free Disk Space Log Retention Policy for the properties of this Log Retention Policy type.

`size-limit-log-retention-policy`

Default {unit}: Size Limit Log Retention Policy

Enabled by default: false

See Size Limit Log Retention Policy for the properties of this Log Retention Policy type.

File Count Log Retention Policy

Log Retention Policies of type file-count-log-retention-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the File Count Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FileNumberRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

number-of-files

Description

Specifies the number of archived log files to retain before the oldest ones are cleaned.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Free Disk Space Log Retention Policy

Log Retention Policies of type free-disk-space-log-retention-policy have the following properties:

free-disk-space

Description

Specifies the minimum amount of free disk space that should be available on the file system on which the archived log files are stored.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Free Disk Space Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FreeDiskSpaceRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Size Limit Log Retention Policy

Log Retention Policies of type size-limit-log-retention-policy have the following properties:

disk-space-used

Description

Specifies the maximum total disk space used by the log files.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Retention Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-log-rotation-policy-prop(1)

Name

dsconfig get-log-rotation-policy-prop - Shows Log Rotation Policy properties

Synopsis

`dsconfig get-log-rotation-policy-prop` {options}

Description

Shows Log Rotation Policy properties.

Options

The `dsconfig get-log-rotation-policy-prop` command takes the following options:

`--policy-name {name}`

The name of the Log Rotation Policy.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

`fixed-time-log-rotation-policy`

Default {name}: Fixed Time Log Rotation Policy

Enabled by default: false

See Fixed Time Log Rotation Policy for the properties of this Log Rotation Policy type.

`size-limit-log-rotation-policy`

Default {name}: Size Limit Log Rotation Policy

Enabled by default: false

See Size Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`time-limit-log-rotation-policy`

Default {name}: Time Limit Log Rotation Policy

Enabled by default: false

See Time Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`--property {property}`

The name of a property to be displayed.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

`fixed-time-log-rotation-policy`

Default {property}: Fixed Time Log Rotation Policy

Enabled by default: false

See Fixed Time Log Rotation Policy for the properties of this Log Rotation Policy type.

`size-limit-log-rotation-policy`

Default {property}: Size Limit Log Rotation Policy

Enabled by default: false

See Size Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`time-limit-log-rotation-policy`

Default {property}: Time Limit Log Rotation Policy

Enabled by default: false

See Time Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`-E | --record`

Modifies the display output to show one property value per line.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

`fixed-time-log-rotation-policy`

Default null: Fixed Time Log Rotation Policy

Enabled by default: false

See Fixed Time Log Rotation Policy for the properties of this Log Rotation Policy type.

`size-limit-log-rotation-policy`

Default null: Size Limit Log Rotation Policy

Enabled by default: false

See Size Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`time-limit-log-rotation-policy`

Default null: Time Limit Log Rotation Policy

Enabled by default: false

See Time Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

`fixed-time-log-rotation-policy`

Default {unit}: Fixed Time Log Rotation Policy

Enabled by default: false

See Fixed Time Log Rotation Policy for the properties of this Log Rotation Policy type.

`size-limit-log-rotation-policy`

Default {unit}: Size Limit Log Rotation Policy

Enabled by default: false

See Size Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`time-limit-log-rotation-policy`

Default {unit}: Time Limit Log Rotation Policy

Enabled by default: false

See Time Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

`fixed-time-log-rotation-policy`

Default {unit}: Fixed Time Log Rotation Policy

Enabled by default: false

See Fixed Time Log Rotation Policy for the properties of this Log Rotation Policy type.

`size-limit-log-rotation-policy`

Default {unit}: Size Limit Log Rotation Policy

Enabled by default: false

See Size Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`time-limit-log-rotation-policy`

Default {unit}: Time Limit Log Rotation Policy

Enabled by default: false

See Time Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

Fixed Time Log Rotation Policy

Log Rotation Policies of type fixed-time-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fixed Time Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.FixedTimeRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-of-day

Description

Specifies the time of day at which log rotation should occur.

Default Value

None

Allowed Values

24 hour time of day in HHmm format.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Size Limit Log Rotation Policy

Log Rotation Policies of type size-limit-log-rotation-policy have the following properties:

file-size-limit

Description

Specifies the maximum size that a log file can reach before it is rotated.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Time Limit Log Rotation Policy

Log Rotation Policies of type time-limit-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Time Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.TimeLimitRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

rotation-interval

Description

Specifies the time interval between rotations.

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-monitor-provider-prop(1)

Name

dsconfig get-monitor-provider-prop - Shows Monitor Provider properties

Synopsis

`dsconfig get-monitor-provider-prop` {options}

Description

Shows Monitor Provider properties.

Options

The `dsconfig get-monitor-provider-prop` command takes the following options:

`--provider-name {name}`

The name of the Monitor Provider.

Monitor Provider properties depend on the Monitor Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

`client-connection-monitor-provider`

Default {name}: Client Connection Monitor Provider

Enabled by default: true

See Client Connection Monitor Provider for the properties of this Monitor Provider type.

`entry-cache-monitor-provider`

Default {name}: Entry Cache Monitor Provider

Enabled by default: true

See Entry Cache Monitor Provider for the properties of this Monitor Provider type.

`memory-usage-monitor-provider`

Default {name}: Memory Usage Monitor Provider

Enabled by default: true

See Memory Usage Monitor Provider for the properties of this Monitor Provider type.

`stack-trace-monitor-provider`

Default {name}: Stack Trace Monitor Provider

Enabled by default: true

See Stack Trace Monitor Provider for the properties of this Monitor Provider type.

`system-info-monitor-provider`

Default {name}: System Info Monitor Provider

Enabled by default: true

See System Info Monitor Provider for the properties of this Monitor Provider type.

`version-monitor-provider`

Default {name}: Version Monitor Provider

Enabled by default: true

See Version Monitor Provider for the properties of this Monitor Provider type.

`--property {property}`

The name of a property to be displayed.

Monitor Provider properties depend on the Monitor Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

`client-connection-monitor-provider`

Default {property}: Client Connection Monitor Provider

Enabled by default: true

See Client Connection Monitor Provider for the properties of this Monitor Provider type.

`entry-cache-monitor-provider`

Default {property}: Entry Cache Monitor Provider

Enabled by default: true

See Entry Cache Monitor Provider for the properties of this Monitor Provider type.

`memory-usage-monitor-provider`

Default {property}: Memory Usage Monitor Provider

Enabled by default: true

See Memory Usage Monitor Provider for the properties of this Monitor Provider type.

`stack-trace-monitor-provider`

Default {property}: Stack Trace Monitor Provider

Enabled by default: true

See Stack Trace Monitor Provider for the properties of this Monitor Provider type.

`system-info-monitor-provider`

Default {property}: System Info Monitor Provider

Enabled by default: true

See System Info Monitor Provider for the properties of this Monitor Provider type.

`version-monitor-provider`

Default {property}: Version Monitor Provider

Enabled by default: true

See Version Monitor Provider for the properties of this Monitor Provider type.

`-E | --record`

Modifies the display output to show one property value per line.

Monitor Provider properties depend on the Monitor Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

`client-connection-monitor-provider`

Default null: Client Connection Monitor Provider

Enabled by default: true

See Client Connection Monitor Provider for the properties of this Monitor Provider type.

`entry-cache-monitor-provider`

Default null: Entry Cache Monitor Provider

Enabled by default: true

See Entry Cache Monitor Provider for the properties of this Monitor Provider type.

`memory-usage-monitor-provider`

Default null: Memory Usage Monitor Provider

Enabled by default: true

See Memory Usage Monitor Provider for the properties of this Monitor Provider type.

`stack-trace-monitor-provider`

Default null: Stack Trace Monitor Provider

Enabled by default: true

See Stack Trace Monitor Provider for the properties of this Monitor Provider type.

`system-info-monitor-provider`

Default null: System Info Monitor Provider

Enabled by default: true

See System Info Monitor Provider for the properties of this Monitor Provider type.

`version-monitor-provider`

Default null: Version Monitor Provider

Enabled by default: true

See Version Monitor Provider for the properties of this Monitor Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Monitor Provider properties depend on the Monitor Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

`client-connection-monitor-provider`

Default {unit}: Client Connection Monitor Provider

Enabled by default: true

See Client Connection Monitor Provider for the properties of this Monitor Provider type.

`entry-cache-monitor-provider`

Default {unit}: Entry Cache Monitor Provider

Enabled by default: true

See Entry Cache Monitor Provider for the properties of this Monitor Provider type.

`memory-usage-monitor-provider`

Default {unit}: Memory Usage Monitor Provider

Enabled by default: true

See Memory Usage Monitor Provider for the properties of this Monitor Provider type.

`stack-trace-monitor-provider`

Default {unit}: Stack Trace Monitor Provider

Enabled by default: true

See Stack Trace Monitor Provider for the properties of this Monitor Provider type.

`system-info-monitor-provider`

Default {unit}: System Info Monitor Provider

Enabled by default: true

See System Info Monitor Provider for the properties of this Monitor Provider type.

`version-monitor-provider`

Default {unit}: Version Monitor Provider

Enabled by default: true

See Version Monitor Provider for the properties of this Monitor Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Monitor Provider properties depend on the Monitor Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

`client-connection-monitor-provider`

Default {unit}: Client Connection Monitor Provider

Enabled by default: true

See Client Connection Monitor Provider for the properties of this Monitor Provider type.

`entry-cache-monitor-provider`

Default {unit}: Entry Cache Monitor Provider

Enabled by default: true

See Entry Cache Monitor Provider for the properties of this Monitor Provider type.

`memory-usage-monitor-provider`

Default {unit}: Memory Usage Monitor Provider

Enabled by default: true

See Memory Usage Monitor Provider for the properties of this Monitor Provider type.

`stack-trace-monitor-provider`

Default {unit}: Stack Trace Monitor Provider

Enabled by default: true

See Stack Trace Monitor Provider for the properties of this Monitor Provider type.

`system-info-monitor-provider`

Default {unit}: System Info Monitor Provider

Enabled by default: true

See System Info Monitor Provider for the properties of this Monitor Provider type.

`version-monitor-provider`

Default {unit}: Version Monitor Provider

Enabled by default: true

See Version Monitor Provider for the properties of this Monitor Provider type.

Client Connection Monitor Provider

Monitor Providers of type client-connection-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Client Connection Monitor Provider implementation.

Default Value

org.opends.server.monitors.ClientConnectionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Entry Cache Monitor Provider

Monitor Providers of type entry-cache-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Entry Cache Monitor Provider implementation.

Default Value

org.opends.server.monitors.EntryCacheMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Memory Usage Monitor Provider

Monitor Providers of type memory-usage-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Memory Usage Monitor Provider implementation.

Default Value

org.opends.server.monitors.MemoryUsageMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Stack Trace Monitor Provider

Monitor Providers of type stack-trace-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Stack Trace Monitor Provider implementation.

Default Value

org.opends.server.monitors.StackTraceMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

System Info Monitor Provider

Monitor Providers of type system-info-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the System Info Monitor Provider implementation.

Default Value

org.opends.server.monitors.SystemInfoMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Version Monitor Provider

Monitor Providers of type version-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Version Monitor Provider implementation.

Default Value

org.opends.server.monitors.VersionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-password-generator-prop(1)

Name

dsconfig get-password-generator-prop - Shows Password Generator properties

Synopsis

`dsconfig get-password-generator-prop` {options}

Description

Shows Password Generator properties.

Options

The `dsconfig get-password-generator-prop` command takes the following options:

`--generator-name {name}`

The name of the Password Generator.

Password Generator properties depend on the Password Generator type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

`random-password-generator`

Default {name}: Random Password Generator

Enabled by default: true

See Random Password Generator for the properties of this Password Generator type.

`--property {property}`

The name of a property to be displayed.

Password Generator properties depend on the Password Generator type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

`random-password-generator`

Default {property}: Random Password Generator

Enabled by default: true

See Random Password Generator for the properties of this Password Generator type.

`-E | --record`

Modifies the display output to show one property value per line.

Password Generator properties depend on the Password Generator type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Password Generator types:

`random-password-generator`

Default null: Random Password Generator

Enabled by default: true

See Random Password Generator for the properties of this Password Generator type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Password Generator properties depend on the Password Generator type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

`random-password-generator`

Default {unit}: Random Password Generator

Enabled by default: true

See Random Password Generator for the properties of this Password Generator type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Password Generator properties depend on the Password Generator type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

`random-password-generator`

Default {unit}: Random Password Generator

Enabled by default: true

See Random Password Generator for the properties of this Password Generator type.

Random Password Generator

Password Generators of type random-password-generator have the following properties:

enabled

Description

Indicates whether the Password Generator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Random Password Generator implementation.

Default Value

org.opends.server.extensions.RandomPasswordGenerator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordGenerator

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

password-character-set

Description

Specifies one or more named character sets. This is a multi-valued property, with each value defining a different character set. The format of the character set is the name of the set followed by a colon and the characters that are in that set. For example, the value "alpha:abcdefghijklmnopqrstuvwxyz" defines a character set named "alpha" containing all of the lower-case ASCII alphabetic characters.

Default Value

None

Allowed Values

A character set name (consisting of ASCII letters) followed by a colon and the set of characters that are included in that character set.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-format

Description

Specifies the format to use for the generated password. The value is a comma-delimited list of elements in which each of those elements is comprised of the name of a character set defined in the password-character-set property, a colon, and the number of characters to include from that set. For example, a value of "alpha:3,numeric:2,alpha:3" generates an 8-character password in which the first three characters are from the "alpha" set, the next two are from the "numeric" set, and the final three are from the "alpha" set.

Default Value

None

Allowed Values

A comma-delimited list whose elements comprise a valid character set name, a colon, and a positive integer indicating the number of characters from that set to be included.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-password-policy-prop(1)

Name

dsconfig get-password-policy-prop - Shows Authentication Policy properties

Synopsis

`dsconfig get-password-policy-prop` {options}

Description

Shows Authentication Policy properties.

Options

The `dsconfig get-password-policy-prop` command takes the following options:

`--policy-name {name}`

The name of the Authentication Policy.

Authentication Policy properties depend on the Authentication Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

`ldap-pass-through-authentication-policy`

Default {name}: LDAP Pass Through Authentication Policy

Enabled by default: false

See LDAP Pass Through Authentication Policy for the properties of this Authentication Policy type.

`password-policy`

Default {name}: Password Policy

Enabled by default: false

See Password Policy for the properties of this Authentication Policy type.

`--property {property}`

The name of a property to be displayed.

Authentication Policy properties depend on the Authentication Policy type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

`ldap-pass-through-authentication-policy`

Default {property}: LDAP Pass Through Authentication Policy

Enabled by default: false

See LDAP Pass Through Authentication Policy for the properties of this Authentication Policy type.

`password-policy`

Default {property}: Password Policy

Enabled by default: false

See Password Policy for the properties of this Authentication Policy type.

`-E | --record`

Modifies the display output to show one property value per line.

Authentication Policy properties depend on the Authentication Policy type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

`ldap-pass-through-authentication-policy`

Default null: LDAP Pass Through Authentication Policy

Enabled by default: false

See LDAP Pass Through Authentication Policy for the properties of this Authentication Policy type.

`password-policy`

Default null: Password Policy

Enabled by default: false

See Password Policy for the properties of this Authentication Policy type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Authentication Policy properties depend on the Authentication Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

`ldap-pass-through-authentication-policy`

Default {unit}: LDAP Pass Through Authentication Policy

Enabled by default: false

See LDAP Pass Through Authentication Policy for the properties of this Authentication Policy type.

`password-policy`

Default {unit}: Password Policy

Enabled by default: false

See Password Policy for the properties of this Authentication Policy type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Authentication Policy properties depend on the Authentication Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

`ldap-pass-through-authentication-policy`

Default {unit}: LDAP Pass Through Authentication Policy

Enabled by default: false

See LDAP Pass Through Authentication Policy for the properties of this Authentication Policy type.

`password-policy`

Default {unit}: Password Policy

Enabled by default: false

See Password Policy for the properties of this Authentication Policy type.

LDAP Pass Through Authentication Policy

Authentication Policies of type ldap-pass-through-authentication-policy have the following properties:

cached-password-storage-scheme

Description

Specifies the name of a password storage scheme which should be used for encoding cached passwords. Changing the password storage scheme will cause all existing cached passwords to be discarded.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cached-password-ttl

Description

Specifies the maximum length of time that a locally cached password may be used for authentication before it is refreshed from the remote LDAP service. This property represents a cache timeout. Increasing the timeout period decreases the frequency that bind operations are delegated to the remote LDAP service, but increases the risk of users authenticating using stale passwords. Note that authentication attempts which fail because the provided password does not match the locally cached password will always be retried against the remote LDAP service.

Default Value

8 hours

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-timeout

Description

Specifies the timeout used when connecting to remote LDAP directory servers, performing SSL negotiation, and for individual search and bind requests. If the timeout expires then the current operation will be aborted and retried against another LDAP server if one is available.

Default Value

3 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the LDAP Pass Through Authentication Policy implementation.

Default Value

org.opends.server.extensions.LDAPPassThroughAuthenticationPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

mapped-attribute

Description

Specifies one or more attributes in the user's entry whose value(s) will determine the bind DN used when authenticating to the remote LDAP directory service. This property is mandatory when using the "mapped-bind" or "mapped-search" mapping policies. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. At least one of the named attributes must exist in a user's local entry in order for authentication to proceed. When multiple attributes or values are found in the user's entry then the behavior is determined by the mapping policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-base-dn

Description

Specifies the set of base DNs below which to search for users in the remote LDAP directory service. This property is mandatory when using the "mapped-search" mapping policy. If multiple values are given, searches are performed below all specified base DNs.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-dn

Description

Specifies the bind DN which should be used to perform user searches in the remote LDAP directory service.

Default Value

Searches will be performed anonymously.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password

Description

Specifies the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-environment-variable

Description

Specifies the name of an environment variable containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-file

Description

Specifies the name of a file containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-property

Description

Specifies the name of a Java property containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-filter-template

Description

If defined, overrides the filter used when searching for the user, substituting %s with the value of the local entry's "mapped-attribute". The filter-template may include ZERO or ONE %s substitutions. If multiple mapped-attributes are configured, multiple renditions of this template will be aggregated into one larger filter using an OR (|) operator. An example use-case for this property would be to use a different attribute type on the mapped search. For example, mapped-attribute could be set to "uid" and filter-template to "(samAccountName=%s)". You can also use the filter to restrict search results. For example: "(&(uid=%s)(objectclass=student))"

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapping-policy

Description

Specifies the mapping algorithm for obtaining the bind DN from the user's entry.

Default Value

unmapped

Allowed Values

mapped-bind

Bind to the remote LDAP directory service using a DN obtained from an attribute in the user's entry. This policy will check each attribute named in the "mapped-attribute" property. If more than one attribute or value is present then the first one will be used.

mapped-search

Bind to the remote LDAP directory service using the DN of an entry obtained using a search against the remote LDAP directory service. The search filter will comprise of an equality matching filter whose attribute type is the "mapped-attribute" property, and whose assertion value is the attribute value obtained from the user's entry. If more than one attribute or value is present then the filter will be composed of multiple equality filters combined using a logical OR (union).

unmapped

Bind to the remote LDAP directory service using the DN of the user's entry in this directory server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

primary-remote-ldap-server

Description

Specifies the primary list of remote LDAP servers which should be used for pass through

authentication. If more than one LDAP server is specified then operations may be distributed across them. If all of the primary LDAP servers are unavailable then operations will fail-over to the set of secondary LDAP servers, if defined.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-remote-ldap-server

Description

Specifies the secondary list of remote LDAP servers which should be used for pass through authentication in the event that the primary LDAP servers are unavailable. If more than one LDAP server is specified then operations may be distributed across them. Operations will be rerouted to the primary LDAP servers as soon as they are determined to be available.

Default Value

No secondary LDAP servers.

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols which are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with remote LDAP directory servers.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

use-password-caching

Description

Indicates whether passwords should be cached locally within the user's entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Pass Through Authentication Policy should use SSL. If enabled, the LDAP Pass Through Authentication Policy will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether LDAP connections should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether LDAP connections should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Policy

Authentication Policies of type password-policy have the following properties:

account-status-notification-handler

Description

Specifies the names of the account status notification handlers that are used with the associated password storage scheme.

Default Value

None

Allowed Values

The DN of any Account Status Notification Handler. The referenced account status notification handlers must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-expired-password-changes

Description

Indicates whether a user whose password is expired is still allowed to change that password using the password modify extended operation.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-multiple-password-values

Description

Indicates whether user entries can have multiple distinct values for the password attribute. This is potentially dangerous because many mechanisms used to change the password do not work well with such a configuration. If multiple password values are allowed, then any of them can be used to authenticate, and they are all subject to the same policy constraints.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-pre-encoded-passwords

Description

Indicates whether users can change their passwords by providing a pre-encoded value. This can cause a security risk because the clear-text version of the password is not known and therefore validation checks cannot be applied to it.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-user-password-changes

Description

Indicates whether users can change their own passwords. This check is made in addition to access control evaluation. Both must allow the password change for it to occur.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-password-storage-scheme

Description

Specifies the names of the password storage schemes that are used to encode clear-text passwords for this password policy.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

deprecated-password-storage-scheme

Description

Specifies the names of the password storage schemes that are considered deprecated for this password policy. If a user with this password policy authenticates to the server and his/her password is encoded with a deprecated scheme, those values are removed and replaced with values encoded using the default password storage scheme(s).

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

expire-passwords-without-warning

Description

Indicates whether the directory server allows a user's password to expire even if that user has never seen an expiration warning notification. If this property is true, accounts always expire when the expiration time arrives. If this property is false or disabled, the user always receives at least one warning notification, and the password expiration is set to the warning time plus the warning interval.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-add

Description

Indicates whether users are forced to change their passwords upon first authenticating to the directory server after their account has been created.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-reset

Description

Indicates whether users are forced to change their passwords if they are reset by an administrator. For this purpose, anyone with permission to change a given user's password other than that user is considered an administrator.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

grace-login-count

Description

Specifies the number of grace logins that a user is allowed after the account has expired to allow that user to choose a new password. A value of 0 indicates that no grace logins are allowed.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

idle-lockout-interval

Description

Specifies the maximum length of time that an account may remain idle (that is, the associated user does not authenticate to the server) before that user is locked out. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that idle accounts are not automatically locked out. This feature is available only if the last login time is maintained.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the Password Policy implementation.

Default Value

org.opends.server.core.PasswordPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

last-login-time-attribute

Description

Specifies the name or OID of the attribute type that is used to hold the last login time for users with the associated password policy. This attribute type must be defined in the directory server schema and must either be defined as an operational attribute or must be allowed by the set of objectClasses for all users with the associated password policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

last-login-time-format

Description

Specifies the format string that is used to generate the last login time value for users with the associated password policy. This format string conforms to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-duration

Description

Specifies the length of time that an account is locked after too many authentication failures. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the account must remain locked until an administrator resets the password.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-count

Description

Specifies the maximum number of authentication failures that a user is allowed before the account is locked out. A value of 0 indicates that accounts are never locked out due to failed attempts.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-expiration-interval

Description

Specifies the length of time before an authentication failure is no longer counted against a user for the purposes of account lockout. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the authentication failures must never expire. The failure count is always cleared upon a successful authentication.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-age

Description

Specifies the maximum length of time that a user can continue using the same password before it must be changed (that is, the password expiration interval). The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables password expiration.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-reset-age

Description

Specifies the maximum length of time that users have to change passwords after they have been reset by an administrator before they become locked. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables this feature.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-age

Description

Specifies the minimum length of time after a password change before the user is allowed to change the password again. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. This setting can be used to prevent users from changing their passwords repeatedly over a short period of time to flush an old password from the history so that it can be re-used.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-attribute

Description

Specifies the attribute type used to hold user passwords. This attribute type must be defined in the server schema, and it must have either the user password or auth password syntax.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-change-requires-current-password

Description

Indicates whether user password changes must use the password modify extended operation and must include the user's current password before the change is allowed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-expiration-warning-interval

Description

Specifies the maximum length of time before a user's password actually expires that the server begins to include warning notifications in bind responses for that user. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables the warning interval.

Default Value

5 days

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-generator

Description

Specifies the name of the password generator that is used with the associated password policy. This is used in conjunction with the password modify extended operation to generate a new password for a user when none was provided in the request.

Default Value

None

Allowed Values

The DN of any Password Generator. The referenced password generator must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-count

Description

Specifies the maximum number of former passwords to maintain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero indicates that either no password history is to be maintained (if the password history duration has a value of zero seconds), or that there is no maximum number of passwords to maintain in the history (if the password history duration has a value greater than zero seconds).

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-duration

Description

Specifies the maximum length of time that passwords remain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero seconds indicates that either no password history is to be maintained (if the password history count has a value of zero), or that there is no maximum duration for passwords in the history (if the password history count has a value greater than zero).

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-validator

Description

Specifies the names of the password validators that are used with the associated password storage scheme. The password validators are invoked when a user attempts to provide a new password, to determine whether the new password is acceptable.

Default Value

None

Allowed Values

The DN of any Password Validator. The referenced password validators must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

previous-last-login-time-format

Description

Specifies the format string(s) that might have been used with the last login time at any point in the past for users associated with the password policy. These values are used to make it possible

to parse previous values, but are not used to set new values. The format strings conform to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-change-by-time

Description

Specifies the time by which all users with the associated password policy must change their passwords. The value is expressed in a generalized time format. If this time is equal to the current time or is in the past, then all users are required to change their passwords immediately. The behavior of the server in this mode is identical to the behavior observed when users are forced to change their passwords after an administrative reset.

Default Value

None

Allowed Values

A valid timestamp in generalized time form (for example, a value of "20070409185811Z" indicates a value of April 9, 2007 at 6:58:11 pm GMT).

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-authentication

Description

Indicates whether users with the associated password policy are required to authenticate in a secure manner. This might mean either using a secure communication channel between the client and the server, or using a SASL mechanism that does not expose the credentials.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-password-changes

Description

Indicates whether users with the associated password policy are required to change their password in a secure manner that does not expose the credentials.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

skip-validation-for-administrators

Description

Indicates whether passwords set by administrators are allowed to bypass the password validation process that is required for user password changes.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

state-update-failure-policy

Description

Specifies how the server deals with the inability to update password policy state information during an authentication attempt. In particular, this property can be used to control whether an otherwise successful bind operation fails if a failure occurs while attempting to update password policy state information (for example, to clear a record of previous authentication failures or to update the last login time). It can also be used to control whether to reject a bind request if it is known ahead of time that it will not be possible to update the authentication failure times in the

event of an unsuccessful bind attempt (for example, if the backend writability mode is disabled).

Default Value

reactive

Allowed Values

ignore

If a bind attempt would otherwise be successful, then do not reject it if a problem occurs while attempting to update the password policy state information for the user.

proactive

Proactively reject any bind attempt if it is known ahead of time that it would not be possible to update the user's password policy state information.

reactive

Even if a bind attempt would otherwise be successful, reject it if a problem occurs while attempting to update the password policy state information for the user.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-password-storage-scheme-prop(1)

Name

dsconfig get-password-storage-scheme-prop - Shows Password Storage Scheme properties

Synopsis

`dsconfig get-password-storage-scheme-prop` {options}

Description

Shows Password Storage Scheme properties.

Options

The `dsconfig get-password-storage-scheme-prop` command takes the following options:

`--scheme-name {name}`

The name of the Password Storage Scheme.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

`aes-password-storage-scheme`

Default {name}: AES Password Storage Scheme

Enabled by default: true

See AES Password Storage Scheme for the properties of this Password Storage Scheme type.

`base64-password-storage-scheme`

Default {name}: Base64 Password Storage Scheme

Enabled by default: true

See Base64 Password Storage Scheme for the properties of this Password Storage Scheme type.

`bcrypt-password-storage-scheme`

Default {name}: Bcrypt Password Storage Scheme

Enabled by default: true

See Bcrypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`blowfish-password-storage-scheme`

Default {name}: Blowfish Password Storage Scheme

Enabled by default: true

See Blowfish Password Storage Scheme for the properties of this Password Storage Scheme type.

`clear-password-storage-scheme`

Default {name}: Clear Password Storage Scheme

Enabled by default: true

See Clear Password Storage Scheme for the properties of this Password Storage Scheme type.

`crypt-password-storage-scheme`

Default {name}: Crypt Password Storage Scheme

Enabled by default: true

See Crypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`md5-password-storage-scheme`

Default {name}: MD5 Password Storage Scheme

Enabled by default: true

See MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha256-password-storage-scheme`

Default {name}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha512-password-storage-scheme`

Default {name}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pkcs5s2-password-storage-scheme`

Default {name}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See PKCS5S2 Password Storage Scheme for the properties of this Password Storage Scheme type.

`rc4-password-storage-scheme`

Default {name}: RC4 Password Storage Scheme

Enabled by default: true

See RC4 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-md5-password-storage-scheme`

Default {name}: Salted MD5 Password Storage Scheme

Enabled by default: true

See Salted MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha1-password-storage-scheme`

Default {name}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See Salted SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha256-password-storage-scheme`

Default {name}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See Salted SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha384-password-storage-scheme`

Default {name}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See Salted SHA384 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha512-password-storage-scheme`

Default {name}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See Salted SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`sha1-password-storage-scheme`

Default {name}: SHA1 Password Storage Scheme

Enabled by default: true

See SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`triple-des-password-storage-scheme`

Default {name}: Triple DES Password Storage Scheme

Enabled by default: true

See Triple DES Password Storage Scheme for the properties of this Password Storage Scheme type.

`--property {property}`

The name of a property to be displayed.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

`aes-password-storage-scheme`

Default {property}: AES Password Storage Scheme

Enabled by default: true

See AES Password Storage Scheme for the properties of this Password Storage Scheme type.

`base64-password-storage-scheme`

Default {property}: Base64 Password Storage Scheme

Enabled by default: true

See Base64 Password Storage Scheme for the properties of this Password Storage Scheme type.

`bcrypt-password-storage-scheme`

Default {property}: Bcrypt Password Storage Scheme

Enabled by default: true

See Bcrypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`blowfish-password-storage-scheme`

Default {property}: Blowfish Password Storage Scheme

Enabled by default: true

See Blowfish Password Storage Scheme for the properties of this Password Storage Scheme type.

`clear-password-storage-scheme`

Default {property}: Clear Password Storage Scheme

Enabled by default: true

See Clear Password Storage Scheme for the properties of this Password Storage Scheme type.

`crypt-password-storage-scheme`

Default {property}: Crypt Password Storage Scheme

Enabled by default: true

See Crypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`md5-password-storage-scheme`

Default {property}: MD5 Password Storage Scheme

Enabled by default: true

See MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha256-password-storage-scheme`

Default {property}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha512-password-storage-scheme`

Default {property}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pkcs5s2-password-storage-scheme`

Default {property}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See PKCS5S2 Password Storage Scheme for the properties of this Password Storage Scheme type.

`rc4-password-storage-scheme`

Default {property}: RC4 Password Storage Scheme

Enabled by default: true

See RC4 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-md5-password-storage-scheme`

Default {property}: Salted MD5 Password Storage Scheme

Enabled by default: true

See Salted MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha1-password-storage-scheme`

Default {property}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See Salted SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha256-password-storage-scheme`

Default {property}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See Salted SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha384-password-storage-scheme`

Default {property}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See Salted SHA384 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha512-password-storage-scheme`

Default {property}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See Salted SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`sha1-password-storage-scheme`

Default {property}: SHA1 Password Storage Scheme

Enabled by default: true

See SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`triple-des-password-storage-scheme`

Default {property}: Triple DES Password Storage Scheme

Enabled by default: true

See Triple DES Password Storage Scheme for the properties of this Password Storage Scheme type.

`-E | --record`

Modifies the display output to show one property value per line.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

`aes-password-storage-scheme`

Default null: AES Password Storage Scheme

Enabled by default: true

See AES Password Storage Scheme for the properties of this Password Storage Scheme type.

`base64-password-storage-scheme`

Default null: Base64 Password Storage Scheme

Enabled by default: true

See Base64 Password Storage Scheme for the properties of this Password Storage Scheme type.

`bcrypt-password-storage-scheme`

Default null: Bcrypt Password Storage Scheme

Enabled by default: true

See Bcrypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`blowfish-password-storage-scheme`

Default null: Blowfish Password Storage Scheme

Enabled by default: true

See Blowfish Password Storage Scheme for the properties of this Password Storage Scheme type.

`clear-password-storage-scheme`

Default null: Clear Password Storage Scheme

Enabled by default: true

See Clear Password Storage Scheme for the properties of this Password Storage Scheme type.

`crypt-password-storage-scheme`

Default null: Crypt Password Storage Scheme

Enabled by default: true

See Crypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`md5-password-storage-scheme`

Default null: MD5 Password Storage Scheme

Enabled by default: true

See MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha256-password-storage-scheme`

Default null: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha512-password-storage-scheme`

Default null: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pkcs5s2-password-storage-scheme`

Default null: PKCS5S2 Password Storage Scheme

Enabled by default: true

See PKCS5S2 Password Storage Scheme for the properties of this Password Storage Scheme type.

`rc4-password-storage-scheme`

Default null: RC4 Password Storage Scheme

Enabled by default: true

See RC4 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-md5-password-storage-scheme`

Default null: Salted MD5 Password Storage Scheme

Enabled by default: true

See Salted MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha1-password-storage-scheme`

Default null: Salted SHA1 Password Storage Scheme

Enabled by default: true

See Salted SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha256-password-storage-scheme`

Default null: Salted SHA256 Password Storage Scheme

Enabled by default: true

See Salted SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha384-password-storage-scheme`

Default null: Salted SHA384 Password Storage Scheme

Enabled by default: true

See Salted SHA384 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha512-password-storage-scheme`

Default null: Salted SHA512 Password Storage Scheme

Enabled by default: true

See Salted SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`sha1-password-storage-scheme`

Default null: SHA1 Password Storage Scheme

Enabled by default: true

See SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`triple-des-password-storage-scheme`

Default null: Triple DES Password Storage Scheme

Enabled by default: true

See Triple DES Password Storage Scheme for the properties of this Password Storage Scheme type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

`aes-password-storage-scheme`

Default {unit}: AES Password Storage Scheme

Enabled by default: true

See AES Password Storage Scheme for the properties of this Password Storage Scheme type.

`base64-password-storage-scheme`

Default {unit}: Base64 Password Storage Scheme

Enabled by default: true

See Base64 Password Storage Scheme for the properties of this Password Storage Scheme type.

`bcrypt-password-storage-scheme`

Default {unit}: Bcrypt Password Storage Scheme

Enabled by default: true

See Bcrypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`blowfish-password-storage-scheme`

Default {unit}: Blowfish Password Storage Scheme

Enabled by default: true

See Blowfish Password Storage Scheme for the properties of this Password Storage Scheme type.

`clear-password-storage-scheme`

Default {unit}: Clear Password Storage Scheme

Enabled by default: true

See Clear Password Storage Scheme for the properties of this Password Storage Scheme type.

`crypt-password-storage-scheme`

Default {unit}: Crypt Password Storage Scheme

Enabled by default: true

See Crypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`md5-password-storage-scheme`

Default {unit}: MD5 Password Storage Scheme

Enabled by default: true

See MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha256-password-storage-scheme`

Default {unit}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha512-password-storage-scheme`

Default {unit}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pkcs5s2-password-storage-scheme`

Default {unit}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See PKCS5S2 Password Storage Scheme for the properties of this Password Storage Scheme type.

`rc4-password-storage-scheme`

Default {unit}: RC4 Password Storage Scheme

Enabled by default: true

See RC4 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-md5-password-storage-scheme`

Default {unit}: Salted MD5 Password Storage Scheme

Enabled by default: true

See Salted MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha1-password-storage-scheme`

Default {unit}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See Salted SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha256-password-storage-scheme`

Default {unit}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See Salted SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha384-password-storage-scheme`

Default {unit}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See Salted SHA384 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha512-password-storage-scheme`

Default {unit}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See Salted SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`sha1-password-storage-scheme`

Default {unit}: SHA1 Password Storage Scheme

Enabled by default: true

See SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`triple-des-password-storage-scheme`

Default {unit}: Triple DES Password Storage Scheme

Enabled by default: true

See Triple DES Password Storage Scheme for the properties of this Password Storage Scheme type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

`aes-password-storage-scheme`

Default {unit}: AES Password Storage Scheme

Enabled by default: true

See AES Password Storage Scheme for the properties of this Password Storage Scheme type.

`base64-password-storage-scheme`

Default {unit}: Base64 Password Storage Scheme

Enabled by default: true

See Base64 Password Storage Scheme for the properties of this Password Storage Scheme type.

`bcrypt-password-storage-scheme`

Default {unit}: Bcrypt Password Storage Scheme

Enabled by default: true

See Bcrypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`blowfish-password-storage-scheme`

Default {unit}: Blowfish Password Storage Scheme

Enabled by default: true

See Blowfish Password Storage Scheme for the properties of this Password Storage Scheme type.

`clear-password-storage-scheme`

Default {unit}: Clear Password Storage Scheme

Enabled by default: true

See Clear Password Storage Scheme for the properties of this Password Storage Scheme type.

`crypt-password-storage-scheme`

Default {unit}: Crypt Password Storage Scheme

Enabled by default: true

See Crypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`md5-password-storage-scheme`

Default {unit}: MD5 Password Storage Scheme

Enabled by default: true

See MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha256-password-storage-scheme`

Default {unit}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha512-password-storage-scheme`

Default {unit}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pkcs5s2-password-storage-scheme`

Default {unit}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See PKCS5S2 Password Storage Scheme for the properties of this Password Storage Scheme type.

`rc4-password-storage-scheme`

Default {unit}: RC4 Password Storage Scheme

Enabled by default: true

See RC4 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-md5-password-storage-scheme`

Default {unit}: Salted MD5 Password Storage Scheme

Enabled by default: true

See Salted MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha1-password-storage-scheme`

Default {unit}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See Salted SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha256-password-storage-scheme`

Default {unit}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See Salted SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha384-password-storage-scheme`

Default {unit}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See Salted SHA384 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha512-password-storage-scheme`

Default {unit}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See Salted SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`sha1-password-storage-scheme`

Default {unit}: SHA1 Password Storage Scheme

Enabled by default: true

See SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`triple-des-password-storage-scheme`

Default {unit}: Triple DES Password Storage Scheme

Enabled by default: true

See Triple DES Password Storage Scheme for the properties of this Password Storage Scheme type.

AES Password Storage Scheme

Password Storage Schemes of type aes-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the AES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.AESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Base64 Password Storage Scheme

Password Storage Schemes of type base64-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Base64 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.Base64PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Bcrypt Password Storage Scheme

Password Storage Schemes of type bcrypt-password-storage-scheme have the following properties:

bcrypt-cost

Description

The cost parameter specifies a key expansion iteration count as a power of two. A default value of 12 (2^12 iterations) is considered in 2016 as a reasonable balance between responsiveness and security for regular users.

Default Value

12

Allowed Values

An integer value. Lower value is 1. Upper value is 30.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Bcrypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BcryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Blowfish Password Storage Scheme

Password Storage Schemes of type blowfish-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Blowfish Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BlowfishPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Clear Password Storage Scheme

Password Storage Schemes of type clear-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Clear Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.ClearPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Crypt Password Storage Scheme

Password Storage Schemes of type crypt-password-storage-scheme have the following properties:

crypt-password-storage-encryption-algorithm

Description

Specifies the algorithm to use to encrypt new passwords. Select the crypt algorithm to use to encrypt new passwords. The value can either be "unix", which means the password is encrypted with the weak Unix crypt algorithm, or "md5" which means the password is encrypted with the BSD MD5 algorithm and has a 1 prefix, or "sha256" which means the password is encrypted with the SHA256 algorithm and has a 5 prefix, or "sha512" which means the password is encrypted with the SHA512 algorithm and has a 6 prefix.

Default Value

unix

Allowed Values

md5

New passwords are encrypted with the BSD MD5 algorithm.

sha256

New passwords are encrypted with the Unix crypt SHA256 algorithm.

sha512

New passwords are encrypted with the Unix crypt SHA512 algorithm.

unix

New passwords are encrypted with the Unix crypt algorithm. Passwords are truncated at 8 characters and the top bit of each character is ignored.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Crypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.CryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

MD5 Password Storage Scheme

Password Storage Schemes of type md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.MD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

PBKDF2 Hmac SHA256 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

PBKDF2 Hmac SHA512 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

PKCS5S2 Password Storage Scheme

Password Storage Schemes of type pkcs5s2-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PKCS5S2 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PKCS5S2PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

RC4 Password Storage Scheme

Password Storage Schemes of type rc4-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the RC4 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.RC4PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted MD5 Password Storage Scheme

Password Storage Schemes of type salted-md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedMD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA1 Password Storage Scheme

Password Storage Schemes of type salted-sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA256 Password Storage Scheme

Password Storage Schemes of type salted-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA384 Password Storage Scheme

Password Storage Schemes of type salted-sha384-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA384 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA384PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA512 Password Storage Scheme

Password Storage Schemes of type salted-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

SHA1 Password Storage Scheme

Password Storage Schemes of type sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Triple DES Password Storage Scheme

Password Storage Schemes of type triple-des-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Triple DES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.TripleDESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-password-validator-prop(1)

Name

dsconfig get-password-validator-prop - Shows Password Validator properties

Synopsis

`dsconfig get-password-validator-prop` {options}

Description

Shows Password Validator properties.

Options

The `dsconfig get-password-validator-prop` command takes the following options:

`--validator-name {name}`

The name of the Password Validator.

Password Validator properties depend on the Password Validator type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

`attribute-value-password-validator`

Default {name}: Attribute Value Password Validator

Enabled by default: true

See Attribute Value Password Validator for the properties of this Password Validator type.

`character-set-password-validator`

Default {name}: Character Set Password Validator

Enabled by default: true

See Character Set Password Validator for the properties of this Password Validator type.

`dictionary-password-validator`

Default {name}: Dictionary Password Validator

Enabled by default: true

See Dictionary Password Validator for the properties of this Password Validator type.

`length-based-password-validator`

Default {name}: Length Based Password Validator

Enabled by default: true

See Length Based Password Validator for the properties of this Password Validator type.

`repeated-characters-password-validator`

Default {name}: Repeated Characters Password Validator

Enabled by default: true

See Repeated Characters Password Validator for the properties of this Password Validator type.

`similarity-based-password-validator`

Default {name}: Similarity Based Password Validator

Enabled by default: true

See Similarity Based Password Validator for the properties of this Password Validator type.

`unique-characters-password-validator`

Default {name}: Unique Characters Password Validator

Enabled by default: true

See Unique Characters Password Validator for the properties of this Password Validator type.

`--property {property}`

The name of a property to be displayed.

Password Validator properties depend on the Password Validator type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

`attribute-value-password-validator`

Default {property}: Attribute Value Password Validator

Enabled by default: true

See Attribute Value Password Validator for the properties of this Password Validator type.

`character-set-password-validator`

Default {property}: Character Set Password Validator

Enabled by default: true

See Character Set Password Validator for the properties of this Password Validator type.

`dictionary-password-validator`

Default {property}: Dictionary Password Validator

Enabled by default: true

See Dictionary Password Validator for the properties of this Password Validator type.

`length-based-password-validator`

Default {property}: Length Based Password Validator

Enabled by default: true

See Length Based Password Validator for the properties of this Password Validator type.

`repeated-characters-password-validator`

Default {property}: Repeated Characters Password Validator

Enabled by default: true

See Repeated Characters Password Validator for the properties of this Password Validator type.

`similarity-based-password-validator`

Default {property}: Similarity Based Password Validator

Enabled by default: true

See Similarity Based Password Validator for the properties of this Password Validator type.

`unique-characters-password-validator`

Default {property}: Unique Characters Password Validator

Enabled by default: true

See Unique Characters Password Validator for the properties of this Password Validator type.

`-E | --record`

Modifies the display output to show one property value per line.

Password Validator properties depend on the Password Validator type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Password Validator types:

`attribute-value-password-validator`

Default null: Attribute Value Password Validator

Enabled by default: true

See Attribute Value Password Validator for the properties of this Password Validator type.

`character-set-password-validator`

Default null: Character Set Password Validator

Enabled by default: true

See Character Set Password Validator for the properties of this Password Validator type.

`dictionary-password-validator`

Default null: Dictionary Password Validator

Enabled by default: true

See Dictionary Password Validator for the properties of this Password Validator type.

`length-based-password-validator`

Default null: Length Based Password Validator

Enabled by default: true

See Length Based Password Validator for the properties of this Password Validator type.

`repeated-characters-password-validator`

Default null: Repeated Characters Password Validator

Enabled by default: true

See Repeated Characters Password Validator for the properties of this Password Validator type.

`similarity-based-password-validator`

Default null: Similarity Based Password Validator

Enabled by default: true

See Similarity Based Password Validator for the properties of this Password Validator type.

`unique-characters-password-validator`

Default null: Unique Characters Password Validator

Enabled by default: true

See Unique Characters Password Validator for the properties of this Password Validator type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Password Validator properties depend on the Password Validator type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

`attribute-value-password-validator`

Default {unit}: Attribute Value Password Validator

Enabled by default: true

See Attribute Value Password Validator for the properties of this Password Validator type.

`character-set-password-validator`

Default {unit}: Character Set Password Validator

Enabled by default: true

See Character Set Password Validator for the properties of this Password Validator type.

`dictionary-password-validator`

Default {unit}: Dictionary Password Validator

Enabled by default: true

See Dictionary Password Validator for the properties of this Password Validator type.

`length-based-password-validator`

Default {unit}: Length Based Password Validator

Enabled by default: true

See Length Based Password Validator for the properties of this Password Validator type.

`repeated-characters-password-validator`

Default {unit}: Repeated Characters Password Validator

Enabled by default: true

See Repeated Characters Password Validator for the properties of this Password Validator type.

`similarity-based-password-validator`

Default {unit}: Similarity Based Password Validator

Enabled by default: true

See Similarity Based Password Validator for the properties of this Password Validator type.

`unique-characters-password-validator`

Default {unit}: Unique Characters Password Validator

Enabled by default: true

See Unique Characters Password Validator for the properties of this Password Validator type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Password Validator properties depend on the Password Validator type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

`attribute-value-password-validator`

Default {unit}: Attribute Value Password Validator

Enabled by default: true

See Attribute Value Password Validator for the properties of this Password Validator type.

`character-set-password-validator`

Default {unit}: Character Set Password Validator

Enabled by default: true

See Character Set Password Validator for the properties of this Password Validator type.

`dictionary-password-validator`

Default {unit}: Dictionary Password Validator

Enabled by default: true

See Dictionary Password Validator for the properties of this Password Validator type.

`length-based-password-validator`

Default {unit}: Length Based Password Validator

Enabled by default: true

See Length Based Password Validator for the properties of this Password Validator type.

`repeated-characters-password-validator`

Default {unit}: Repeated Characters Password Validator

Enabled by default: true

See Repeated Characters Password Validator for the properties of this Password Validator type.

`similarity-based-password-validator`

Default {unit}: Similarity Based Password Validator

Enabled by default: true

See Similarity Based Password Validator for the properties of this Password Validator type.

`unique-characters-password-validator`

Default {unit}: Unique Characters Password Validator

Enabled by default: true

See Unique Characters Password Validator for the properties of this Password Validator type.

Attribute Value Password Validator

Password Validators of type attribute-value-password-validator have the following properties:

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against attribute values. If "false" then only match the entire password against attribute values otherwise ("true") check whether the password contains attribute values.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.AttributeValuePasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name(s) of the attribute(s) whose values should be checked to determine whether they match the provided password. If no values are provided, then the server checks if the proposed password matches the value of any attribute in the user's entry.

Default Value

All attributes in the user entry will be checked.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator should test the reversed value of the provided password as well as the order in which it was given.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Character Set Password Validator

Password Validators of type character-set-password-validator have the following properties:

allow-unclassified-characters

Description

Indicates whether this password validator allows passwords to contain characters outside of any of the user-defined character sets and ranges. If this is "false", then only those characters in the user-defined character sets and ranges may be used in passwords. Any password containing a character not included in any character set or range will be rejected.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set

Description

Specifies a character set containing characters that a password may contain and a value indicating the minimum number of characters required from that set. Each value must be an integer (indicating the minimum required characters from the set which may be zero, indicating that the character set is optional) followed by a colon and the characters to include in that set (for example, "3:abcdefghijklmnopqrstuvwxyz" indicates that a user password must contain at least three characters from the set of lowercase ASCII letters). Multiple character sets can be defined in separate values, although no character can appear in more than one character set.

Default Value

If no sets are specified, the validator only uses the defined character ranges.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set-ranges

Description

Specifies a character range containing characters that a password may contain and a value indicating the minimum number of characters required from that range. Each value must be an integer (indicating the minimum required characters from the range which may be zero, indicating that the character range is optional) followed by a colon and one or more range specifications. A range specification is 3 characters: the first character allowed, a minus, and the last character allowed. For example, "3:A-Za-z0-9". The ranges in each value should not overlap, and the characters in each range specification should be ordered.

Default Value

If no ranges are specified, the validator only uses the defined character sets.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.CharacterSetPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-character-sets

Description

Specifies the minimum number of character sets and ranges that a password must contain. This property should only be used in conjunction with optional character sets and ranges (those requiring zero characters). Its value must include any mandatory character sets and ranges (those requiring greater than zero characters). This is useful in situations where a password must contain characters from mandatory character sets and ranges, and characters from at least N optional character sets and ranges. For example, it is quite common to require that a password contains at least one non-alphanumeric character as well as characters from two alphanumeric character sets (lower-case, upper-case, digits). In this case, this property should be set to 3.

Default Value

The password must contain characters from each of the mandatory character sets and ranges and, if there are optional character sets and ranges, at least one character from one of the optional character sets and ranges.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Dictionary Password Validator

Password Validators of type dictionary-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator is to treat password characters in a case-sensitive manner. If it is set to true, then the validator rejects a password only if it appears in the dictionary with exactly the same capitalization as provided by the user.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against dictionary words. If "false" then only match the entire password against words otherwise ("true") check whether the password contains words.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dictionary-file

Description

Specifies the path to the file containing a list of words that cannot be used as passwords. It should be formatted with one word per line. The value can be an absolute path or a path that is relative to the OpenDJ instance root.

Default Value

For Unix and Linux systems: config/wordlist.txt. For Windows systems: config\wordlist.txt

Allowed Values

The path to any text file contained on the system that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.DictionaryPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator is to test the reversed value of the provided password as well as the order in which it was given. For example, if the user provides a new password of "password" and this configuration attribute is set to true, then the value "drowssap" is also tested against attribute values in the user's entry.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Length Based Password Validator

Password Validators of type length-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.LengthBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-password-length

Description

Specifies the maximum number of characters that can be included in a proposed password. A value of zero indicates that there will be no upper bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the

maximum length.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-length

Description

Specifies the minimum number of characters that must be included in a proposed password. A value of zero indicates that there will be no lower bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

6

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Repeated Characters Password Validator

Password Validators of type repeated-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. If the value of this property is false, the validator ignores any differences in capitalization when looking for consecutive characters in the password. If the value is true, the validator considers a character to be repeating only if all consecutive occurrences use the same capitalization.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.RepeatedCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-consecutive-length

Description

Specifies the maximum number of times that any character can appear consecutively in a password value. A value of zero indicates that no maximum limit is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Similarity Based Password Validator

Password Validators of type similarity-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.SimilarityBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-password-difference

Description

Specifies the minimum difference of new and old password. A value of zero indicates that no difference between passwords is acceptable.

Default Value

None

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Unique Characters Password Validator

Password Validators of type unique-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. A value of true indicates that the validator does not consider a capital letter to be the same as its lower-case counterpart. A value of false indicates that the validator ignores differences in capitalization when looking at the number of unique characters in the password.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.UniqueCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-unique-characters

Description

Specifies the minimum number of unique characters that a password will be allowed to contain. A value of zero indicates that no minimum value is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-plugin-prop(1)

Name

dsconfig get-plugin-prop - Shows Plugin properties

Synopsis

`dsconfig get-plugin-prop` {options}

Description

Shows Plugin properties.

Options

The `dsconfig get-plugin-prop` command takes the following options:

`--plugin-name {name}`
: The name of the Plugin.

  Plugin properties depend on the Plugin type, which depends on the {name} you provide.

  By default, OpenDJ directory server supports the following Plugin types:

  `attribute-cleanup-plugin`
  : Default {name}: Attribute Cleanup Plugin

    Enabled by default: true

    See Attribute Cleanup Plugin for the properties of this Plugin type.

  `change-number-control-plugin`
  : Default {name}: Change Number Control Plugin

    Enabled by default: true

    See Change Number Control Plugin for the properties of this Plugin type.

  `entry-uuid-plugin`
  : Default {name}: Entry UUID Plugin

    Enabled by default: true

    See Entry UUID Plugin for the properties of this Plugin type.

  `fractional-ldif-import-plugin`
  : Default {name}: Fractional LDIF Import Plugin

Enabled by default: true

See Fractional LDIF Import Plugin for the properties of this Plugin type.

`last-mod-plugin`

Default {name}: Last Mod Plugin

Enabled by default: true

See Last Mod Plugin for the properties of this Plugin type.

`ldap-attribute-description-list-plugin`

Default {name}: LDAP Attribute Description List Plugin

Enabled by default: true

See LDAP Attribute Description List Plugin for the properties of this Plugin type.

`password-policy-import-plugin`

Default {name}: Password Policy Import Plugin

Enabled by default: true

See Password Policy Import Plugin for the properties of this Plugin type.

`profiler-plugin`

Default {name}: Profiler Plugin

Enabled by default: true

See Profiler Plugin for the properties of this Plugin type.

`referential-integrity-plugin`

Default {name}: Referential Integrity Plugin

Enabled by default: true

See Referential Integrity Plugin for the properties of this Plugin type.

`samba-password-plugin`

Default {name}: Samba Password Plugin

Enabled by default: true

See Samba Password Plugin for the properties of this Plugin type.

`seven-bit-clean-plugin`

Default {name}: Seven Bit Clean Plugin

Enabled by default: true

See Seven Bit Clean Plugin for the properties of this Plugin type.

`unique-attribute-plugin`

Default {name}: Unique Attribute Plugin

Enabled by default: true

See Unique Attribute Plugin for the properties of this Plugin type.

`--property {property}`

The name of a property to be displayed.

Plugin properties depend on the Plugin type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Plugin types:

`attribute-cleanup-plugin`

Default {property}: Attribute Cleanup Plugin

Enabled by default: true

See Attribute Cleanup Plugin for the properties of this Plugin type.

`change-number-control-plugin`

Default {property}: Change Number Control Plugin

Enabled by default: true

See Change Number Control Plugin for the properties of this Plugin type.

`entry-uuid-plugin`

Default {property}: Entry UUID Plugin

Enabled by default: true

See Entry UUID Plugin for the properties of this Plugin type.

`fractional-ldif-import-plugin`

Default {property}: Fractional LDIF Import Plugin

Enabled by default: true

See Fractional LDIF Import Plugin for the properties of this Plugin type.

`last-mod-plugin`

Default {property}: Last Mod Plugin

Enabled by default: true

See Last Mod Plugin for the properties of this Plugin type.

`ldap-attribute-description-list-plugin`

Default {property}: LDAP Attribute Description List Plugin

Enabled by default: true

See LDAP Attribute Description List Plugin for the properties of this Plugin type.

`password-policy-import-plugin`

Default {property}: Password Policy Import Plugin

Enabled by default: true

See Password Policy Import Plugin for the properties of this Plugin type.

`profiler-plugin`

Default {property}: Profiler Plugin

Enabled by default: true

See Profiler Plugin for the properties of this Plugin type.

`referential-integrity-plugin`

Default {property}: Referential Integrity Plugin

Enabled by default: true

See Referential Integrity Plugin for the properties of this Plugin type.

`samba-password-plugin`

Default {property}: Samba Password Plugin

Enabled by default: true

See Samba Password Plugin for the properties of this Plugin type.

`seven-bit-clean-plugin`

Default {property}: Seven Bit Clean Plugin

Enabled by default: true

See Seven Bit Clean Plugin for the properties of this Plugin type.

`unique-attribute-plugin`

Default {property}: Unique Attribute Plugin

Enabled by default: true

See Unique Attribute Plugin for the properties of this Plugin type.

`-E | --record`

Modifies the display output to show one property value per line.

Plugin properties depend on the Plugin type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Plugin types:

`attribute-cleanup-plugin`

Default null: Attribute Cleanup Plugin

Enabled by default: true

See Attribute Cleanup Plugin for the properties of this Plugin type.

`change-number-control-plugin`

Default null: Change Number Control Plugin

Enabled by default: true

See Change Number Control Plugin for the properties of this Plugin type.

`entry-uuid-plugin`

Default null: Entry UUID Plugin

Enabled by default: true

See Entry UUID Plugin for the properties of this Plugin type.

`fractional-ldif-import-plugin`

Default null: Fractional LDIF Import Plugin

Enabled by default: true

See Fractional LDIF Import Plugin for the properties of this Plugin type.

`last-mod-plugin`

Default null: Last Mod Plugin

Enabled by default: true

See Last Mod Plugin for the properties of this Plugin type.

`ldap-attribute-description-list-plugin`

Default null: LDAP Attribute Description List Plugin

Enabled by default: true

See LDAP Attribute Description List Plugin for the properties of this Plugin type.

`password-policy-import-plugin`

Default null: Password Policy Import Plugin

Enabled by default: true

See Password Policy Import Plugin for the properties of this Plugin type.

`profiler-plugin`

Default null: Profiler Plugin

Enabled by default: true

See Profiler Plugin for the properties of this Plugin type.

`referential-integrity-plugin`

Default null: Referential Integrity Plugin

Enabled by default: true

See Referential Integrity Plugin for the properties of this Plugin type.

`samba-password-plugin`

Default null: Samba Password Plugin

Enabled by default: true

See Samba Password Plugin for the properties of this Plugin type.

`seven-bit-clean-plugin`

Default null: Seven Bit Clean Plugin

Enabled by default: true

See Seven Bit Clean Plugin for the properties of this Plugin type.

`unique-attribute-plugin`

Default null: Unique Attribute Plugin

Enabled by default: true

See Unique Attribute Plugin for the properties of this Plugin type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Plugin properties depend on the Plugin type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Plugin types:

`attribute-cleanup-plugin`

Default {unit}: Attribute Cleanup Plugin

Enabled by default: true

See Attribute Cleanup Plugin for the properties of this Plugin type.

`change-number-control-plugin`

Default {unit}: Change Number Control Plugin

Enabled by default: true

See Change Number Control Plugin for the properties of this Plugin type.

`entry-uuid-plugin`

Default {unit}: Entry UUID Plugin

Enabled by default: true

See Entry UUID Plugin for the properties of this Plugin type.

`fractional-ldif-import-plugin`

Default {unit}: Fractional LDIF Import Plugin

Enabled by default: true

See Fractional LDIF Import Plugin for the properties of this Plugin type.

`last-mod-plugin`

Default {unit}: Last Mod Plugin

Enabled by default: true

See Last Mod Plugin for the properties of this Plugin type.

`ldap-attribute-description-list-plugin`

Default {unit}: LDAP Attribute Description List Plugin

Enabled by default: true

See LDAP Attribute Description List Plugin for the properties of this Plugin type.

`password-policy-import-plugin`

Default {unit}: Password Policy Import Plugin

Enabled by default: true

See Password Policy Import Plugin for the properties of this Plugin type.

`profiler-plugin`

Default {unit}: Profiler Plugin

Enabled by default: true

See Profiler Plugin for the properties of this Plugin type.

`referential-integrity-plugin`

Default {unit}: Referential Integrity Plugin

Enabled by default: true

See Referential Integrity Plugin for the properties of this Plugin type.

`samba-password-plugin`

Default {unit}: Samba Password Plugin

Enabled by default: true

See Samba Password Plugin for the properties of this Plugin type.

`seven-bit-clean-plugin`

Default {unit}: Seven Bit Clean Plugin

Enabled by default: true

See Seven Bit Clean Plugin for the properties of this Plugin type.

`unique-attribute-plugin`

Default {unit}: Unique Attribute Plugin

Enabled by default: true

See Unique Attribute Plugin for the properties of this Plugin type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Plugin properties depend on the Plugin type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Plugin types:

`attribute-cleanup-plugin`

Default {unit}: Attribute Cleanup Plugin

Enabled by default: true

See Attribute Cleanup Plugin for the properties of this Plugin type.

`change-number-control-plugin`

Default {unit}: Change Number Control Plugin

Enabled by default: true

See Change Number Control Plugin for the properties of this Plugin type.

`entry-uuid-plugin`

Default {unit}: Entry UUID Plugin

Enabled by default: true

See Entry UUID Plugin for the properties of this Plugin type.

`fractional-ldif-import-plugin`

Default {unit}: Fractional LDIF Import Plugin

Enabled by default: true

See Fractional LDIF Import Plugin for the properties of this Plugin type.

`last-mod-plugin`

Default {unit}: Last Mod Plugin

Enabled by default: true

See Last Mod Plugin for the properties of this Plugin type.

`ldap-attribute-description-list-plugin`

Default {unit}: LDAP Attribute Description List Plugin

Enabled by default: true

See LDAP Attribute Description List Plugin for the properties of this Plugin type.

`password-policy-import-plugin`

Default {unit}: Password Policy Import Plugin

Enabled by default: true

See Password Policy Import Plugin for the properties of this Plugin type.

`profiler-plugin`

Default {unit}: Profiler Plugin

Enabled by default: true

See Profiler Plugin for the properties of this Plugin type.

`referential-integrity-plugin`

Default {unit}: Referential Integrity Plugin

Enabled by default: true

See Referential Integrity Plugin for the properties of this Plugin type.

`samba-password-plugin`

Default {unit}: Samba Password Plugin

Enabled by default: true

See Samba Password Plugin for the properties of this Plugin type.

`seven-bit-clean-plugin`

Default {unit}: Seven Bit Clean Plugin

Enabled by default: true

See Seven Bit Clean Plugin for the properties of this Plugin type.

`unique-attribute-plugin`

Default {unit}: Unique Attribute Plugin

Enabled by default: true

See Unique Attribute Plugin for the properties of this Plugin type.

Attribute Cleanup Plugin

Plugins of type attribute-cleanup-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.AttributeCleanupPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparseadd preparsemodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

remove-inbound-attributes

Description

A list of attributes which should be removed from incoming add or modify requests.

Default Value

No attributes will be removed

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rename-inbound-attributes

Description

A list of attributes which should be renamed in incoming add or modify requests.

Default Value

No attributes will be renamed

Allowed Values

An attribute name mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Change Number Control Plugin

Plugins of type change-number-control-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ChangeNumberControlPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postOperationAdd postOperationDelete postOperationModify postOperationModifyDN

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Entry UUID Plugin

Plugins of type entry-uuid-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.EntryUUIDPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport preoperationadd

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Fractional LDIF Import Plugin

Plugins of type fractional-ldif-import-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

None

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

None

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

Last Mod Plugin

Plugins of type last-mod-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LastModPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd preoperationmodify preoperationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the

client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

LDAP Attribute Description List Plugin

Plugins of type ldap-attribute-description-list-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LDAPADListPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparsesearch

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Policy Import Plugin

Plugins of type password-policy-import-plugin have the following properties:

default-auth-password-storage-scheme

Description

Specifies the names of password storage schemes that to be used for encoding passwords contained in attributes with the auth password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy should be used to govern them.

Default Value

If the default password policy uses an attribute with the auth password syntax, then the server

uses the default password storage schemes for that password policy. Otherwise, it encodes auth password values using the "SHA1" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import plug-in is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-user-password-storage-scheme

Description

Specifies the names of the password storage schemes to be used for encoding passwords contained in attributes with the user password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy is to be used to govern them.

Default Value

If the default password policy uses the attribute with the user password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes user password values using the "SSHA" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import Plugin is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.PasswordPolicyImportPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Profiler Plugin

Plugins of type profiler-plugin have the following properties:

enable-profiling-on-startup

Description

Indicates whether the profiler plug-in is to start collecting data automatically when the directory

server is started. This property is read only when the server is started, and any changes take effect on the next restart. This property is typically set to "false" unless startup profiling is required, because otherwise the volume of data that can be collected can cause the server to run out of memory if it is not turned off in a timely manner.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.profiler.ProfilerPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

startup

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

profile-action

Description

Specifies the action that should be taken by the profiler. A value of "start" causes the profiler thread to start collecting data if it is not already active. A value of "stop" causes the profiler thread to stop collecting data and write it to disk, and a value of "cancel" causes the profiler thread to stop collecting data and discard anything that has been captured. These operations occur immediately.

Default Value

none

Allowed Values

cancel

Stop collecting profile data and discard what has been captured.

none

Do not take any action.

start

Start collecting profile data.

stop

Stop collecting profile data and write what has been captured to a file in the profile directory.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-directory

Description

Specifies the path to the directory where profile information is to be written. This path may be either an absolute path or a path that is relative to the root of the OpenDJ directory server instance. The directory must exist and the directory server must have permission to create new files in it.

Default Value

None

Allowed Values

The path to any directory that exists on the filesystem and that can be read and written by the server user.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-sample-interval

Description

Specifies the sample interval in milliseconds to be used when capturing profiling information in the server. When capturing data, the profiler thread sleeps for this length of time between calls to obtain traces for all threads running in the JVM.

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

NoneChanges to this configuration attribute take effect the next time the profiler is started.

Advanced Property

No

Read-only

No

Referential Integrity Plugin

Plugins of type referential-integrity-plugin have the following properties:

attribute-type

Description

Specifies the attribute types for which referential integrity is to be maintained. At least one attribute type must be specified, and the syntax of any attributes must be either a distinguished name (1.3.6.1.4.1.1466.115.121.1.12) or name and optional UID (1.3.6.1.4.1.1466.115.121.1.34).

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN that limits the scope within which referential integrity is maintained.

Default Value

Referential integrity is maintained in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references

Description

Specifies whether reference attributes must refer to existing entries. When this property is set to true, this plugin will ensure that any new references added as part of an add or modify operation point to existing entries, and that the referenced entries match the filter criteria for the referencing attribute, if specified.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-filter-criteria

Description

Specifies additional filter criteria which will be enforced when checking references. If a reference attribute has filter criteria defined then this plugin will ensure that any new references added as part of an add or modify operation refer to an existing entry which matches the specified filter.

Default Value

None

Allowed Values

An attribute-filter mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-scope-criteria

Description

Specifies whether referenced entries must reside within the same naming context as the entry containing the reference. The reference scope will only be enforced when reference checking is enabled.

Default Value

global

Allowed Values

global

References may refer to existing entries located anywhere in the Directory.

naming-context

References must refer to existing entries located within the same naming context.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ReferentialIntegrityPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

Specifies the log file location where the update records are written when the plug-in is in background-mode processing. The default location is the logs directory of the server instance, using the file name "referint".

Default Value

logs/referint

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postoperationdelete postoperationmodifydn subordinatemodifydn subordinatedelete preoperationadd preoperationmodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

update-interval

Description

Specifies the interval in seconds when referential integrity updates are made. If this value is 0, then the updates are made synchronously in the foreground.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Samba Password Plugin

Plugins of type samba-password-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SambaPasswordPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationmodify postoperationextended

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pwd-sync-policy

Description

Specifies which Samba passwords should be kept synchronized.

Default Value

sync-nt-password

Allowed Values

sync-lm-password

Synchronize the LanMan password attribute "sambaLMPassword"

sync-nt-password

Synchronize the NT password attribute "sambaNTPassword"

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

samba-administrator-dn

Description

Specifies the distinguished name of the user which Samba uses to perform Password Modify extended operations against this directory server in order to synchronize the userPassword attribute after the LanMan or NT passwords have been updated. The user must have the 'password-reset' privilege and should not be a root user. This user name can be used in order to identify Samba connections and avoid double re-synchronization of the same password. If this property is left undefined, then no password updates will be skipped.

Default Value

Synchronize all updates to user passwords

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Seven Bit Clean Plugin

Plugins of type seven-bit-clean-plugin have the following properties:

attribute-type

Description

Specifies the name or OID of an attribute type for which values should be checked to ensure that they are 7-bit clean.

Default Value

uid mail userPassword

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN below which the checking is performed. Any attempt to update a value for one of the configured attributes below this base DN must be 7-bit clean for the operation to be allowed.

Default Value

All entries below all public naming contexts will be checked.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons

that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SevenBitCleanPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport preparseadd preparsemodify preparsemodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Unique Attribute Plugin

Plugins of type unique-attribute-plugin have the following properties:

base-dn

Description

Specifies a base DN within which the attribute must be unique.

Default Value

The plug-in uses the server's public naming contexts in the searches.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.UniqueAttributePlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd preoperationmodify preoperationmodifydn postoperationadd postoperationmodify postoperationmodifydn postsynchronizationadd postsynchronizationmodify postsynchronizationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

type

Description

Specifies the type of attributes to check for value uniqueness.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-plugin-root-prop(1)

Name

dsconfig get-plugin-root-prop - Shows Plugin Root properties

Synopsis

`dsconfig get-plugin-root-prop` {options}

Description

Shows Plugin Root properties.

Options

The `dsconfig get-plugin-root-prop` command takes the following options:

`--property {property}`
: The name of a property to be displayed.

  Plugin Root properties depend on the Plugin Root type, which depends on the {property} you provide.

  By default, OpenDJ directory server supports the following Plugin Root types:

  `plugin-root`
  : Default {property}: Plugin Root

    Enabled by default: false

    See Plugin Root for the properties of this Plugin Root type.

`-E | --record`
: Modifies the display output to show one property value per line.

  Plugin Root properties depend on the Plugin Root type, which depends on the null you provide.

  By default, OpenDJ directory server supports the following Plugin Root types:

  `plugin-root`
  : Default null: Plugin Root

    Enabled by default: false

    See Plugin Root for the properties of this Plugin Root type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Plugin Root properties depend on the Plugin Root type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Plugin Root types:

`plugin-root`

Default {unit}: Plugin Root

Enabled by default: false

See Plugin Root for the properties of this Plugin Root type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Plugin Root properties depend on the Plugin Root type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Plugin Root types:

`plugin-root`

Default {unit}: Plugin Root

Enabled by default: false

See Plugin Root for the properties of this Plugin Root type.

Plugin Root

Plugin Roots of type plugin-root have the following properties:

plugin-order-intermediate-response

Description

Specifies the order in which intermediate response plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which intermediate response plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-ldif-export

Description

Specifies the order in which LDIF export plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which LDIF export plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-ldif-import

Description

Specifies the order in which LDIF import plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which LDIF import plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-ldif-import-begin

Description

Specifies the order in which LDIF import begin plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which LDIF import begin plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-ldif-import-end

Description

Specifies the order in which LDIF import end plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which LDIF import end plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-connect

Description

Specifies the order in which post-connect plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-connect plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-disconnect

Description

Specifies the order in which post-disconnect plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-disconnect plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-abandon

Description

Specifies the order in which post-operation abandon plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation abandon plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-add

Description

Specifies the order in which post-operation add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-bind

Description

Specifies the order in which post-operation bind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation bind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-compare

Description

Specifies the order in which post-operation compare plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation compare plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-delete

Description

Specifies the order in which post-operation delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-extended

Description

Specifies the order in which post-operation extended operation plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation extended operation plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-modify

Description

Specifies the order in which post-operation modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-modify-dn

Description

Specifies the order in which post-operation modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-search

Description

Specifies the order in which post-operation search plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation search plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-unbind

Description

Specifies the order in which post-operation unbind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation unbind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-add

Description

Specifies the order in which post-response add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-bind

Description

Specifies the order in which post-response bind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response bind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-compare

Description

Specifies the order in which post-response compare plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response compare plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-delete

Description

Specifies the order in which post-response delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-extended

Description

Specifies the order in which post-response extended operation plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response extended operation plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-modify

Description

Specifies the order in which post-response modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-modify-dn

Description

Specifies the order in which post-response modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the

position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-search

Description

Specifies the order in which post-response search plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response search plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-synchronization-add

Description

Specifies the order in which post-synchronization add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-synchronization add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-synchronization-delete

Description

Specifies the order in which post-synchronization delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-synchronization delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-synchronization-modify

Description

Specifies the order in which post-synchronization modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-synchronization modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-synchronization-modify-dn

Description

Specifies the order in which post-synchronization modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-synchronization modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-add

Description

Specifies the order in which pre-operation add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-bind

Description

Specifies the order in which pre-operation bind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation bind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-compare

Description

Specifies the order in which pre-operation compare plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is

undefined).

Default Value

The order in which pre-operation compare plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-delete

Description

Specifies the order in which pre-operation delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-extended

Description

Specifies the order in which pre-operation extended operation plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation extended operation plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-modify

Description

Specifies the order in which pre-operation modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-modify-dn

Description

Specifies the order in which pre-operation modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-search

Description

Specifies the order in which pre-operation search plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation searc plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-abandon

Description

Specifies the order in which pre-parse abandon plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse abandon plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-add

Description

Specifies the order in which pre-parse add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-bind

Description

Specifies the order in which pre-parse bind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse bind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-compare

Description

Specifies the order in which pre-parse compare plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse compare plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-delete

Description

Specifies the order in which pre-parse delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-extended

Description

Specifies the order in which pre-parse extended operation plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse extended operation plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-modify

Description

Specifies the order in which pre-parse modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-modify-dn

Description

Specifies the order in which pre-parse modify DN plug-ins are to be loaded and invoked. The

value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-search

Description

Specifies the order in which pre-parse search plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse search plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-unbind

Description

Specifies the order in which pre-parse unbind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse unbind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-search-result-entry

Description

Specifies the order in which search result entry plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which search result entry plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-search-result-reference

Description

Specifies the order in which search result reference plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which search result reference plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-shutdown

Description

Specifies the order in which shutdown plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which shutdown plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-startup

Description

Specifies the order in which startup plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which startup plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-subordinate-delete

Description

Specifies the order in which subordinate delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which subordinate delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-subordinate-modify-dn

Description

Specifies the order in which subordinate modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which subordinate modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-replication-domain-prop(1)

Name

dsconfig get-replication-domain-prop - Shows Replication Domain properties

Synopsis

`dsconfig get-replication-domain-prop` {options}

Description

Shows Replication Domain properties.

Options

The `dsconfig get-replication-domain-prop` command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default {name}: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

`--domain-name {name}`

The name of the Replication Domain.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default {name}: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

`--property {property}`

The name of a property to be displayed.

Replication Domain properties depend on the Replication Domain type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default {property}: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

`-E | --record`

Modifies the display output to show one property value per line.

Replication Domain properties depend on the Replication Domain type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default null: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Replication Domain properties depend on the Replication Domain type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default {unit}: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Replication Domain properties depend on the Replication Domain type, which depends on the

{unit} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default {unit}: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

Replication Domain

Replication Domains of type replication-domain have the following properties:

assured-sd-level

Description

The level of acknowledgment for Safe Data assured sub mode. When assured replication is configured in Safe Data mode, this value defines the number of replication servers (with the same group ID of the local server) that should acknowledge the sent update before the LDAP client call can return.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-timeout

Description

The timeout value when waiting for assured replication acknowledgments. Defines the amount of milliseconds the server will wait for assured acknowledgments (in either Safe Data or Safe

Read assured replication modes) before returning anyway the LDAP client call.

Default Value

2000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-type

Description

Defines the assured replication mode of the replicated domain. The assured replication can be disabled or enabled. When enabled, two modes are available: Safe Data or Safe Read modes.

Default Value

not-assured

Allowed Values

not-assured

Assured replication is not enabled. Updates sent for replication (for being replayed on other LDAP servers in the topology) are sent without waiting for any acknowledgment and the LDAP client call returns immediately.

safe-data

Assured replication is enabled in Safe Data mode: updates sent for replication are subject to acknowledgment from the replication servers that have the same group ID as the local server (defined with the group-id property). The number of acknowledgments to expect is defined by the assured-sd-level property. After acknowledgments are received, LDAP client call returns.

safe-read

Assured replication is enabled in Safe Read mode: updates sent for replication are subject to acknowledgments from the LDAP servers in the topology that have the same group ID as the local server (defined with the group-id property). After acknowledgments are received, LDAP

client call returns.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN of the replicated data.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

changetime-heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when sending its local change time to the Replication Server. The directory server sends a regular heart-beat to the Replication within the specified interval. The heart-beat indicates the change time of the directory server to

the Replication Server.

Default Value

1000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

conflicts-historical-purge-delay

Description

This delay indicates the time (in minutes) the domain keeps the historical information necessary to solve conflicts.When a change stored in the historical part of the user entry has a date (from its replication ChangeNumber) older than this delay, it is candidate to be purged. The purge is applied on 2 events: modify of the entry, dedicated purge task.

Default Value

1440m

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 minutes.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-exclude

Description

Allows to exclude some attributes to replicate to this server. If fractional-exclude configuration attribute is used, attributes specified in this attribute will be ignored (not added/modified/deleted) when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-include attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be excluded. The object class may be "*" indicating that the attribute type(s) should be excluded regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-include

Description

Allows to include some attributes to replicate to this server. If fractional-include configuration attribute is used, only attributes specified in this attribute will be added/modified/deleted when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-exclude attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be included. The object class may be "*" indicating that the attribute type(s) should be included regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group ID associated with this replicated domain. This value defines the group ID of the replicated domain. The replication system will preferably connect and send updates to replicate to a replication server with the same group ID as its own one (the local server group ID).

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when communicating with Replication Servers. The directory server expects a regular heart-beat coming from the Replication Server within the specified interval. If a heartbeat is not received within the interval, the Directory Server closes its connection and connects to another Replication Server.

Default Value

10000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 100 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

initialization-window-size

Description

Specifies the window size that this directory server may use when communicating with remote Directory Servers for initialization.

Default Value

100

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

isolation-policy

Description

Specifies the behavior of the directory server if a write operation is attempted on the data within the Replication Domain when none of the configured Replication Servers are available.

Default Value

reject-all-updates

Allowed Values

accept-all-updates

Indicates that updates should be accepted even though it is not possible to send them to any Replication Server. Best effort is made to re-send those updates to a Replication Servers when one of them is available, however those changes are at risk because they are only available from the historical information. This mode can also introduce high replication latency.

reject-all-updates

Indicates that all updates attempted on this Replication Domain are rejected when no Replication Server is available.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-changenumber

Description

Indicates if this server logs the ChangeNumber in access log. This boolean indicates if the

domain should log the ChangeNumber of replicated operations in the access log.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

referrals-url

Description

The URLs other LDAP servers should use to refer to the local server. URLs used by peer servers in the topology to refer to the local server through LDAP referrals. If this attribute is not defined, every URLs available to access this server will be used. If defined, only URLs specified here will be used.

Default Value

None

Allowed Values

A LDAP URL compliant with RFC 2255.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of the Replication Servers within the Replication Domain to which the directory server should try to connect at startup time. Addresses must be specified using the syntax: hostname:port

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

server-id

Description

Specifies a unique identifier for the directory server within the Replication Domain. Each directory server within the same Replication Domain must have a different server ID. A directory server which is a member of multiple Replication Domains may use the same server ID for each of its Replication Domain configurations.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

solve-conflicts

Description

Indicates if this server solves conflict. This boolean indicates if this domain keeps the historical information necessary to solve conflicts. When set to false the server will not maintain historical information and will therefore not be able to solve conflict. This should therefore be done only if the replication is used in a single master type of deployment.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the directory server will use when communicating with Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-replication-server-prop(1)

Name

dsconfig get-replication-server-prop - Shows Replication Server properties

Synopsis

`dsconfig get-replication-server-prop` {options}

Description

Shows Replication Server properties.

Options

The `dsconfig get-replication-server-prop` command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Server properties depend on the Replication Server type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

`replication-server`

Default {name}: Replication Server

Enabled by default: false

See Replication Server for the properties of this Replication Server type.

`--property {property}`

The name of a property to be displayed.

Replication Server properties depend on the Replication Server type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

`replication-server`

Default {property}: Replication Server

Enabled by default: false

See Replication Server for the properties of this Replication Server type.

`-E | --record`

Modifies the display output to show one property value per line.

Replication Server properties depend on the Replication Server type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Replication Server types:

`replication-server`

Default null: Replication Server

Enabled by default: false

See Replication Server for the properties of this Replication Server type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Replication Server properties depend on the Replication Server type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

`replication-server`

Default {unit}: Replication Server

Enabled by default: false

See Replication Server for the properties of this Replication Server type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Replication Server properties depend on the Replication Server type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

`replication-server`

Default {unit}: Replication Server

Enabled by default: false

See Replication Server for the properties of this Replication Server type.

Replication Server

Replication Servers of type replication-server have the following properties:

assured-timeout

Description

The timeout value when waiting for assured mode acknowledgments. Defines the number of milliseconds that the replication server will wait for assured acknowledgments (in either Safe Data or Safe Read assured sub modes) before forgetting them and answer to the entity that sent an update and is waiting for acknowledgment.

Default Value

1000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations

performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compute-change-number

Description

Whether the replication server will compute change numbers. This boolean tells the replication server to compute change numbers for each replicated change by maintaining a change number index database. Changenumbers are computed according to http://tools.ietf.org/html/draft-good-ldap-changelog-04. Note this functionality has an impact on CPU, disk accesses and storage. If changenumbers are not required, it is advisable to set this value to false.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the replication change-log should make records readable only by Directory Server. Throughput and disk space are affected by the more expensive operations taking place. Confidentiality is achieved by encrypting records on all domains managed by this replication server. Encrypting the records prevents unauthorized parties from accessing contents of LDAP operations. For complete protection, consider enabling secure communications between servers. Change number indexing is not affected by the setting.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect operations performed after the change.

Advanced Property

No

Read-only

No

degraded-status-threshold

Description

The number of pending changes as threshold value for putting a directory server in degraded status. This value represents a number of pending changes a replication server has in queue for sending to a directory server. Once this value is crossed, the matching directory server goes in degraded status. When number of pending changes goes back under this value, the directory server is put back in normal status. 0 means status analyzer is disabled and directory servers are never put in degraded status.

Default Value

5000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group id for the replication server. This value defines the group id of the replication server. The replication system of a LDAP server uses the group id of the replicated domain and tries to connect, if possible, to a replication with the same group id.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

monitoring-period

Description

The period between sending of monitoring messages. Defines the duration that the replication server will wait before sending new monitoring messages to its peers (replication servers and directory servers). Larger values increase the length of time it takes for a directory server to detect and switch to a more suitable replication server, whereas smaller values increase the amount of background network traffic.

Default Value

60s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

Specifies the number of changes that are kept in memory for each directory server in the Replication Domain.

Default Value

10000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

replication-db-directory

Description

The path where the Replication Server stores all persistent information.

Default Value

changelogDb

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

replication-port

Description

The port on which this Replication Server waits for connections from other Replication Servers or Directory Servers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-purge-delay

Description

The time (in seconds) after which the Replication Server erases all persistent information.

Default Value

3 days

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of other Replication Servers to which this Replication Server tries to connect at startup time. Addresses must be specified using the syntax: "hostname:port". If IPv6 addresses are used as the hostname, they must be specified using the syntax "[IPv6Address]:port".

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server-id

Description

Specifies a unique identifier for the Replication Server. Each Replication Server must have a different server ID.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

weight

Description

The weight of the replication server. The weight affected to the replication server. Each replication server of the topology has a weight. When combined together, the weights of the replication servers of a same group can be translated to a percentage that determines the quantity of directory servers of the topology that should be connected to a replication server. For instance imagine a topology with 3 replication servers (with the same group id) with the following weights: RS1=1, RS2=1, RS3=2. This means that RS1 should have 25% of the directory servers connected in the topology, RS2 25%, and RS3 50%. This may be useful if the replication servers of the topology have a different power and one wants to spread the load between the replication servers according to their power.

Default Value

1

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the Replication Server uses when communicating with other Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-root-dn-prop(1)

Name

dsconfig get-root-dn-prop - Shows Root DN properties

Synopsis

`dsconfig get-root-dn-prop` {options}

Description

Shows Root DN properties.

Options

The `dsconfig get-root-dn-prop` command takes the following options:

`--property {property}`
: The name of a property to be displayed.

  Root DN properties depend on the Root DN type, which depends on the {property} you provide.

  By default, OpenDJ directory server supports the following Root DN types:

  `root-dn`
  : Default {property}: Root DN

    Enabled by default: false

    See Root DN for the properties of this Root DN type.

`-E | --record`
: Modifies the display output to show one property value per line.

  Root DN properties depend on the Root DN type, which depends on the null you provide.

  By default, OpenDJ directory server supports the following Root DN types:

  `root-dn`
  : Default null: Root DN

    Enabled by default: false

    See Root DN for the properties of this Root DN type.

`-z | --unit-size {unit}`
: Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb

(bytes, kilobytes, megabytes, gigabytes, or terabytes).

Root DN properties depend on the Root DN type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Root DN types:

`root-dn`

Default {unit}: Root DN

Enabled by default: false

See Root DN for the properties of this Root DN type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Root DN properties depend on the Root DN type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Root DN types:

`root-dn`

Default {unit}: Root DN

Enabled by default: false

See Root DN for the properties of this Root DN type.

Root DN

Root Dns of type root-dn have the following properties:

default-root-privilege-name

Description

Specifies the names of the privileges that root users will be granted by default.

Default Value

bypass-lockdown bypass-acl modify-acl config-read config-write ldif-import ldif-export backend-backup backend-restore server-lockdown server-shutdown server-restart disconnect-client cancel-request password-reset update-schema privilege-change unindexed-search subentry-write changelog-read

Allowed Values

backend-backup

Allows the user to request that the server process backup tasks.

backend-restore

Allows the user to request that the server process restore tasks.

bypass-acl

Allows the associated user to bypass access control checks performed by the server.

bypass-lockdown

Allows the associated user to bypass server lockdown mode.

cancel-request

Allows the user to cancel operations in progress on other client connections.

changelog-read

Allows the user to perform read operations on the changelog

config-read

Allows the associated user to read the server configuration.

config-write

Allows the associated user to update the server configuration. The config-read privilege is also required.

data-sync

Allows the user to participate in data synchronization.

disconnect-client

Allows the user to terminate other client connections.

jmx-notify

Allows the associated user to subscribe to receive JMX notifications.

jmx-read

Allows the associated user to perform JMX read operations.

jmx-write

Allows the associated user to perform JMX write operations.

ldif-export

Allows the user to request that the server process LDIF export tasks.

ldif-import

Allows the user to request that the server process LDIF import tasks.

modify-acl

Allows the associated user to modify the server's access control configuration.

password-reset

Allows the user to reset user passwords.

privilege-change

Allows the user to make changes to the set of defined root privileges, as well as to grant and

revoke privileges for users.

proxied-auth

Allows the user to use the proxied authorization control, or to perform a bind that specifies an alternate authorization identity.

server-lockdown

Allows the user to place and bring the server of lockdown mode.

server-restart

Allows the user to request that the server perform an in-core restart.

server-shutdown

Allows the user to request that the server shut down.

subentry-write

Allows the associated user to perform LDAP subentry write operations.

unindexed-search

Allows the user to request that the server process a search that cannot be optimized using server indexes.

update-schema

Allows the user to make changes to the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-root-dse-backend-prop(1)

Name

dsconfig get-root-dse-backend-prop - Shows Root DSE Backend properties

Synopsis

`dsconfig get-root-dse-backend-prop` {options}

Description

Shows Root DSE Backend properties.

Options

The `dsconfig get-root-dse-backend-prop` command takes the following options:

`--property {property}`
: The name of a property to be displayed.

  Root DSE Backend properties depend on the Root DSE Backend type, which depends on the {property} you provide.

  By default, OpenDJ directory server supports the following Root DSE Backend types:

  `root-dse-backend`
  : Default {property}: Root DSE Backend

    Enabled by default: false

    See Root DSE Backend for the properties of this Root DSE Backend type.

`-E | --record`
: Modifies the display output to show one property value per line.

  Root DSE Backend properties depend on the Root DSE Backend type, which depends on the null you provide.

  By default, OpenDJ directory server supports the following Root DSE Backend types:

  `root-dse-backend`
  : Default null: Root DSE Backend

    Enabled by default: false

    See Root DSE Backend for the properties of this Root DSE Backend type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Root DSE Backend properties depend on the Root DSE Backend type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Root DSE Backend types:

`root-dse-backend`

Default {unit}: Root DSE Backend

Enabled by default: false

See Root DSE Backend for the properties of this Root DSE Backend type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Root DSE Backend properties depend on the Root DSE Backend type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Root DSE Backend types:

`root-dse-backend`

Default {unit}: Root DSE Backend

Enabled by default: false

See Root DSE Backend for the properties of this Root DSE Backend type.

Root DSE Backend

Root DSE Backends of type root-dse-backend have the following properties:

show-all-attributes

Description

Indicates whether all attributes in the root DSE are to be treated like user attributes (and therefore returned to clients by default) regardless of the directory server schema configuration.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

show-subordinate-naming-contexts

Description

Indicates whether subordinate naming contexts should be visible in the namingContexts attribute of the RootDSE. By default only top level naming contexts are visible

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-sasl-mechanism-handler-prop(1)

Name

dsconfig get-sasl-mechanism-handler-prop - Shows SASL Mechanism Handler properties

Synopsis

`dsconfig get-sasl-mechanism-handler-prop` {options}

Description

Shows SASL Mechanism Handler properties.

Options

The `dsconfig get-sasl-mechanism-handler-prop` command takes the following options:

`--handler-name {name}`

The name of the SASL Mechanism Handler.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

`anonymous-sasl-mechanism-handler`

Default {name}: Anonymous SASL Mechanism Handler

Enabled by default: true

See Anonymous SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`cram-md5-sasl-mechanism-handler`

Default {name}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See Cram MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`digest-md5-sasl-mechanism-handler`

Default {name}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See Digest MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`external-sasl-mechanism-handler`

Default {name}: External SASL Mechanism Handler

Enabled by default: true

See External SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`gssapi-sasl-mechanism-handler`

Default {name}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See GSSAPI SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`plain-sasl-mechanism-handler`

Default {name}: Plain SASL Mechanism Handler

Enabled by default: true

See Plain SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`--property {property}`

The name of a property to be displayed.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

`anonymous-sasl-mechanism-handler`

Default {property}: Anonymous SASL Mechanism Handler

Enabled by default: true

See Anonymous SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`cram-md5-sasl-mechanism-handler`

Default {property}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See Cram MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`digest-md5-sasl-mechanism-handler`

Default {property}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See Digest MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`external-sasl-mechanism-handler`

Default {property}: External SASL Mechanism Handler

Enabled by default: true

See External SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`gssapi-sasl-mechanism-handler`

Default {property}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See GSSAPI SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`plain-sasl-mechanism-handler`

Default {property}: Plain SASL Mechanism Handler

Enabled by default: true

See Plain SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`-E | --record`

Modifies the display output to show one property value per line.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

`anonymous-sasl-mechanism-handler`

Default null: Anonymous SASL Mechanism Handler

Enabled by default: true

See Anonymous SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`cram-md5-sasl-mechanism-handler`

Default null: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See Cram MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`digest-md5-sasl-mechanism-handler`

Default null: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See Digest MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`external-sasl-mechanism-handler`

Default null: External SASL Mechanism Handler

Enabled by default: true

See External SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`gssapi-sasl-mechanism-handler`

Default null: GSSAPI SASL Mechanism Handler

Enabled by default: true

See GSSAPI SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`plain-sasl-mechanism-handler`

Default null: Plain SASL Mechanism Handler

Enabled by default: true

See Plain SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

`anonymous-sasl-mechanism-handler`

Default {unit}: Anonymous SASL Mechanism Handler

Enabled by default: true

See Anonymous SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`cram-md5-sasl-mechanism-handler`

Default {unit}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See Cram MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`digest-md5-sasl-mechanism-handler`

Default {unit}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See Digest MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`external-sasl-mechanism-handler`

Default {unit}: External SASL Mechanism Handler

Enabled by default: true

See External SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`gssapi-sasl-mechanism-handler`

Default {unit}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See GSSAPI SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`plain-sasl-mechanism-handler`

Default {unit}: Plain SASL Mechanism Handler

Enabled by default: true

See Plain SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

`anonymous-sasl-mechanism-handler`

Default {unit}: Anonymous SASL Mechanism Handler

Enabled by default: true

See Anonymous SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`cram-md5-sasl-mechanism-handler`

Default {unit}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See Cram MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`digest-md5-sasl-mechanism-handler`

Default {unit}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See Digest MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`external-sasl-mechanism-handler`

Default {unit}: External SASL Mechanism Handler

Enabled by default: true

See External SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`gssapi-sasl-mechanism-handler`

Default {unit}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See GSSAPI SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`plain-sasl-mechanism-handler`

Default {unit}: Plain SASL Mechanism Handler

Enabled by default: true

See Plain SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

Anonymous SASL Mechanism Handler

SASL Mechanism Handlers of type anonymous-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.AnonymousSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Cram MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type cram-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper used with this SASL mechanism handler to match the authentication ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the

Cram MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.CRAMMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Digest MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type digest-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Digest MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.DigestMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realms that is to be used by the server for DIGEST-MD5 authentication. If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Default Value

If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Allowed Values

Any realm string that does not contain a comma.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the server that is used when validating the digest-uri parameter during the authentication process. If this configuration attribute is present, then the server expects that clients use a digest-uri equal to "ldap/" followed by the value of this attribute. For example, if the attribute has a value of "directory.example.com", then the server expects clients to use a digest-uri of "ldap/directory.example.com". If no value is provided, then the server does not attempt to validate the digest-uri provided by the client and accepts any value.

Default Value

The server attempts to determine the fully-qualified domain name dynamically.

Allowed Values

The fully-qualified address that is expected for clients to use when connecting to the server and authenticating via DIGEST-MD5.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

External SASL Mechanism Handler

SASL Mechanism Handlers of type external-sasl-mechanism-handler have the following properties:

certificate-attribute

Description

Specifies the name of the attribute to hold user certificates. This property must specify the name of a valid attribute type defined in the server schema.

Default Value

userCertificate

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-mapper

Description

Specifies the name of the certificate mapper that should be used to match client certificates to user entries.

Default Value

None

Allowed Values

The DN of any Certificate Mapper. The referenced certificate mapper must be enabled when the External SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-validation-policy

Description

Indicates whether to attempt to validate the peer certificate against a certificate held in the user's entry.

Default Value

None

Allowed Values

always

Always require the peer certificate to be present in the user’s entry.

ifpresent

If the user’s entry contains one or more certificates, require that one of them match the peer certificate.

never

Do not look for the peer certificate to be present in the user’s entry.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.ExternalSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

GSSAPI SASL Mechanism Handler

SASL Mechanism Handlers of type gssapi-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the Kerberos principal included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the GSSAPI SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.GSSAPISASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

kdc-address

Description

Specifies the address of the KDC that is to be used for Kerberos processing. If provided, this property must be a fully-qualified DNS-resolvable name. If this property is not provided, then the server attempts to determine it from the system-wide Kerberos configuration.

Default Value

The server attempts to determine the KDC address from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

keytab

Description

Specifies the path to the keytab file that should be used for Kerberos processing. If provided, this is either an absolute path or one that is relative to the server instance root.

Default Value

The server attempts to use the system-wide default keytab.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

principal-name

Description

Specifies the principal name. It can either be a simple user name or a service name such as host/example.com. If this property is not provided, then the server attempts to build the principal name by appending the fully qualified domain name to the string "ldap/".

Default Value

The server attempts to determine the principal name from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realm to be used for GSSAPI authentication.

Default Value

The server attempts to determine the realm from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the system.

Default Value

The server attempts to determine the fully-qualified domain name dynamically .

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Plain SASL Mechanism Handler

SASL Mechanism Handlers of type plain-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Plain SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.PlainSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-schema-provider-prop(1)

Name

dsconfig get-schema-provider-prop - Shows Schema Provider properties

Synopsis

`dsconfig get-schema-provider-prop` {options}

Description

Shows Schema Provider properties.

Options

The `dsconfig get-schema-provider-prop` command takes the following options:

`--provider-name {name}`

The name of the Schema Provider.

Schema Provider properties depend on the Schema Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

`core-schema`

Default {name}: Core Schema

Enabled by default: true

See Core Schema for the properties of this Schema Provider type.

`json-schema`

Default {name}: Json Schema

Enabled by default: true

See Json Schema for the properties of this Schema Provider type.

`--property {property}`

The name of a property to be displayed.

Schema Provider properties depend on the Schema Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

`core-schema`

Default {property}: Core Schema

Enabled by default: true

See Core Schema for the properties of this Schema Provider type.

`json-schema`

Default {property}: Json Schema

Enabled by default: true

See Json Schema for the properties of this Schema Provider type.

`-E | --record`

Modifies the display output to show one property value per line.

Schema Provider properties depend on the Schema Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

`core-schema`

Default null: Core Schema

Enabled by default: true

See Core Schema for the properties of this Schema Provider type.

`json-schema`

Default null: Json Schema

Enabled by default: true

See Json Schema for the properties of this Schema Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Schema Provider properties depend on the Schema Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

`core-schema`

Default {unit}: Core Schema

Enabled by default: true

See Core Schema for the properties of this Schema Provider type.

`json-schema`

Default {unit}: Json Schema

Enabled by default: true

See Json Schema for the properties of this Schema Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Schema Provider properties depend on the Schema Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

`core-schema`

Default {unit}: Core Schema

Enabled by default: true

See Core Schema for the properties of this Schema Provider type.

`json-schema`

Default {unit}: Json Schema

Enabled by default: true

See Json Schema for the properties of this Schema Provider type.

Core Schema

Schema Providers of type core-schema have the following properties:

allow-attribute-types-with-no-sup-or-syntax

Description

Indicates whether the schema should allow attribute type definitions that do not declare a superior attribute type or syntax When set to true, invalid attribute type definitions will use the default syntax.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-zero-length-values-directory-string

Description

Indicates whether zero-length (that is, an empty string) values are allowed for directory string. This is technically not allowed by the revised LDAPv3 specification, but some environments may require it for backward compatibility with servers that do allow it.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disabled-matching-rule

Description

The set of disabled matching rules. Matching rules must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled matching rule.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

disabled-syntax

Description

The set of disabled syntaxes. Syntaxes must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled syntax, or NONE

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Core Schema implementation.

Default Value

org.opends.server.schema.CoreSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

json-validation-policy

Description

Specifies the policy that will be used when validating JSON syntax values.

Default Value

strict

Allowed Values

disabled

JSON syntax values will not be validated and, as a result any sequence of bytes will be acceptable.

lenient

JSON syntax values must comply with RFC 7159 except: 1) comments are allowed, 2) single quotes may be used instead of double quotes, and 3) unquoted control characters are allowed in strings.

strict

JSON syntax values must strictly conform to RFC 7159.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-certificates

Description

Indicates whether X.509 Certificate values are required to strictly comply with the standard definition for this syntax. When set to false, certificates will not be validated and, as a result any sequence of bytes will be acceptable.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-country-string

Description

Indicates whether country code values are required to strictly comply with the standard definition for this syntax. When set to false, country codes will not be validated and, as a result any string containing 2 characters will be acceptable.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-jpeg-photos

Description

Indicates whether to require JPEG values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-telephone-numbers

Description

Indicates whether to require telephone number values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strip-syntax-min-upper-bound-attribute-type-description

Description

Indicates whether the suggested minimum upper bound appended to an attribute's syntax OID in it's schema definition Attribute Type Description is stripped off. When retrieving the server's schema, some APIs (JNDI) fail in their syntax lookup methods, because they do not parse this value correctly. This configuration option allows the server to be configured to provide schema definitions these APIs can parse correctly.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Json Schema

Schema Providers of type json-schema have the following properties:

case-sensitive-strings

Description

Indicates whether JSON string comparisons should be case-sensitive.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ignore-white-space

Description

Indicates whether JSON string comparisons should ignore white-space. When enabled all leading and trailing white space will be removed and intermediate white space will be reduced to a single character.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

indexed-field

Description

Specifies which JSON fields should be indexed. A field will be indexed if it matches any of the configured field patterns.

Default Value

All JSON fields will be indexed.

Allowed Values

A JSON pointer which may include wild-cards. A single '**' wild-card matches at most a single path element, whereas a double '*' matches zero or more path elements.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Json Schema implementation.

Default Value

org.opends.server.schema.JsonSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

matching-rule-name

Description

The name of the custom JSON matching rule.

Default Value

The matching rule will not have a name.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

matching-rule-oid

Description

The numeric OID of the custom JSON matching rule.

Default Value

None

Allowed Values

The OID of the matching rule.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-service-discovery-mechanism-prop(1)

Name

dsconfig get-service-discovery-mechanism-prop - Shows Service Discovery Mechanism properties

Synopsis

`dsconfig get-service-discovery-mechanism-prop` {options}

Description

Shows Service Discovery Mechanism properties.

Options

The `dsconfig get-service-discovery-mechanism-prop` command takes the following options:

`--mechanism-name {name}`

The name of the Service Discovery Mechanism.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

`replication-service-discovery-mechanism`

Default {name}: Replication Service Discovery Mechanism

Enabled by default: false

See Replication Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`static-service-discovery-mechanism`

Default {name}: Static Service Discovery Mechanism

Enabled by default: false

See Static Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`--property {property}`

The name of a property to be displayed.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type,

which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

`replication-service-discovery-mechanism`

Default {property}: Replication Service Discovery Mechanism

Enabled by default: false

See Replication Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`static-service-discovery-mechanism`

Default {property}: Static Service Discovery Mechanism

Enabled by default: false

See Static Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`-E | --record`

Modifies the display output to show one property value per line.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

`replication-service-discovery-mechanism`

Default null: Replication Service Discovery Mechanism

Enabled by default: false

See Replication Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`static-service-discovery-mechanism`

Default null: Static Service Discovery Mechanism

Enabled by default: false

See Static Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

`replication-service-discovery-mechanism`

Default {unit}: Replication Service Discovery Mechanism

Enabled by default: false

See Replication Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`static-service-discovery-mechanism`

Default {unit}: Static Service Discovery Mechanism

Enabled by default: false

See Static Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

`replication-service-discovery-mechanism`

Default {unit}: Replication Service Discovery Mechanism

Enabled by default: false

See Replication Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`static-service-discovery-mechanism`

Default {unit}: Static Service Discovery Mechanism

Enabled by default: false

See Static Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

Replication Service Discovery Mechanism

Service Discovery Mechanisms of type replication-service-discovery-mechanism have the following properties:

bind-dn

Description

The bind DN for periodically reading replication server configurations The bind DN must be present on all replication servers and directory servers, it must be able to read the server configuration.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

bind-password

Description

The bind password for periodically reading replication server configurations The bind password must be the same on all replication and directory servers

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

discovery-interval

Description

Interval between two replication server configuration discovery queries. Specifies how frequently to query a replication server configuration in order to discover information about available directory server replicas.

Default Value

60s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.ReplicationServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-group-id

Description

Replication domain group ID of preferred directory server replicas. Directory server replicas with this replication domain group ID will be preferred over other directory server replicas. Secondary server replicas will only be used when all primary server replicas become unavailable.

Default Value

All the server replicas will be treated the same.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the list of replication servers to contact periodically when discovering server replicas.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

Static Service Discovery Mechanism

Service Discovery Mechanisms of type static-service-discovery-mechanism have the following properties:

discovery-interval

Description

Interval between two server configuration discovery executions. Specifies how frequently to read the configuration of the servers in order to discover their new information.

Default Value

60s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.StaticServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-server

Description

Specifies a list of servers that will be used in preference to secondary servers when available.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-server

Description

Specifies a list of servers that will be used in place of primary servers when all primary servers are unavailable.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig get-synchronization-provider-prop(1)

Name

dsconfig get-synchronization-provider-prop - Shows Synchronization Provider properties

Synopsis

`dsconfig get-synchronization-provider-prop` {options}

Description

Shows Synchronization Provider properties.

Options

The `dsconfig get-synchronization-provider-prop` command takes the following options:

`--provider-name {name}`

The name of the Synchronization Provider.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

`replication-synchronization-provider`

Default {name}: Replication Synchronization Provider

Enabled by default: true

See Replication Synchronization Provider for the properties of this Synchronization Provider type.

`--property {property}`

The name of a property to be displayed.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

`replication-synchronization-provider`

Default {property}: Replication Synchronization Provider

Enabled by default: true

See Replication Synchronization Provider for the properties of this Synchronization Provider type.

`-E | --record`

Modifies the display output to show one property value per line.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

`replication-synchronization-provider`

Default null: Replication Synchronization Provider

Enabled by default: true

See Replication Synchronization Provider for the properties of this Synchronization Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

`replication-synchronization-provider`

Default {unit}: Replication Synchronization Provider

Enabled by default: true

See Replication Synchronization Provider for the properties of this Synchronization Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

`replication-synchronization-provider`

Default {unit}: Replication Synchronization Provider

Enabled by default: true

See Replication Synchronization Provider for the properties of this Synchronization Provider

type.

Replication Synchronization Provider

Synchronization Providers of type replication-synchronization-provider have the following properties:

connection-timeout

Description

Specifies the timeout used when connecting to peers and when performing SSL negotiation.

Default Value

5 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Synchronization Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Synchronization Provider implementation.

Default Value

org.opends.server.replication.plugin.MultimasterReplication

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SynchronizationProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-update-replay-threads

Description

Specifies the number of update replay threads. This value is the number of threads created for replaying every updates received for all the replication domains.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-trust-manager-provider-prop(1)

Name

dsconfig get-trust-manager-provider-prop - Shows Trust Manager Provider properties

Synopsis

`dsconfig get-trust-manager-provider-prop` {options}

Description

Shows Trust Manager Provider properties.

Options

The `dsconfig get-trust-manager-provider-prop` command takes the following options:

`--provider-name {name}`

The name of the Trust Manager Provider.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

`blind-trust-manager-provider`

Default {name}: Blind Trust Manager Provider

Enabled by default: true

See Blind Trust Manager Provider for the properties of this Trust Manager Provider type.

`file-based-trust-manager-provider`

Default {name}: File Based Trust Manager Provider

Enabled by default: true

See File Based Trust Manager Provider for the properties of this Trust Manager Provider type.

`ldap-trust-manager-provider`

Default {name}: LDAP Trust Manager Provider

Enabled by default: true

See LDAP Trust Manager Provider for the properties of this Trust Manager Provider type.

`pkcs11-trust-manager-provider`

Default {name}: PKCS11 Trust Manager Provider

Enabled by default: true

See PKCS11 Trust Manager Provider for the properties of this Trust Manager Provider type.

`--property {property}`

The name of a property to be displayed.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

`blind-trust-manager-provider`

Default {property}: Blind Trust Manager Provider

Enabled by default: true

See Blind Trust Manager Provider for the properties of this Trust Manager Provider type.

`file-based-trust-manager-provider`

Default {property}: File Based Trust Manager Provider

Enabled by default: true

See File Based Trust Manager Provider for the properties of this Trust Manager Provider type.

`ldap-trust-manager-provider`

Default {property}: LDAP Trust Manager Provider

Enabled by default: true

See LDAP Trust Manager Provider for the properties of this Trust Manager Provider type.

`pkcs11-trust-manager-provider`

Default {property}: PKCS11 Trust Manager Provider

Enabled by default: true

See PKCS11 Trust Manager Provider for the properties of this Trust Manager Provider type.

`-E | --record`

Modifies the display output to show one property value per line.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

`blind-trust-manager-provider`

Default null: Blind Trust Manager Provider

Enabled by default: true

See Blind Trust Manager Provider for the properties of this Trust Manager Provider type.

`file-based-trust-manager-provider`

Default null: File Based Trust Manager Provider

Enabled by default: true

See File Based Trust Manager Provider for the properties of this Trust Manager Provider type.

`ldap-trust-manager-provider`

Default null: LDAP Trust Manager Provider

Enabled by default: true

See LDAP Trust Manager Provider for the properties of this Trust Manager Provider type.

`pkcs11-trust-manager-provider`

Default null: PKCS11 Trust Manager Provider

Enabled by default: true

See PKCS11 Trust Manager Provider for the properties of this Trust Manager Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

`blind-trust-manager-provider`

Default {unit}: Blind Trust Manager Provider

Enabled by default: true

See Blind Trust Manager Provider for the properties of this Trust Manager Provider type.

`file-based-trust-manager-provider`

Default {unit}: File Based Trust Manager Provider

Enabled by default: true

See File Based Trust Manager Provider for the properties of this Trust Manager Provider type.

`ldap-trust-manager-provider`

Default {unit}: LDAP Trust Manager Provider

Enabled by default: true

See LDAP Trust Manager Provider for the properties of this Trust Manager Provider type.

`pkcs11-trust-manager-provider`

Default {unit}: PKCS11 Trust Manager Provider

Enabled by default: true

See PKCS11 Trust Manager Provider for the properties of this Trust Manager Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

`blind-trust-manager-provider`

Default {unit}: Blind Trust Manager Provider

Enabled by default: true

See Blind Trust Manager Provider for the properties of this Trust Manager Provider type.

`file-based-trust-manager-provider`

Default {unit}: File Based Trust Manager Provider

Enabled by default: true

See File Based Trust Manager Provider for the properties of this Trust Manager Provider type.

`ldap-trust-manager-provider`

Default {unit}: LDAP Trust Manager Provider

Enabled by default: true

See LDAP Trust Manager Provider for the properties of this Trust Manager Provider type.

`pkcs11-trust-manager-provider`

Default {unit}: PKCS11 Trust Manager Provider

Enabled by default: true

See PKCS11 Trust Manager Provider for the properties of this Trust Manager Provider type.

Blind Trust Manager Provider

Trust Manager Providers of type blind-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Blind Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.BlindTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Trust Manager Provider

Trust Manager Providers of type file-based-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file containing the trust information. It can be an absolute path or a path that is relative to the OpenDJ instance root. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

An absolute path or a path that is relative to the OpenDJ directory server instance root.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the trust store file. Valid values always include 'JKS' and 'PKCS12', but different implementations can allow other values as well. If no value is provided, then the JVM default value is used. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment. The "JKS" and "PKCS12" formats are typically available in Java environments.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

LDAP Trust Manager Provider

Trust Manager Providers of type ldap-trust-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

PKCS11 Trust Manager Provider

Trust Manager Providers of type pkcs11-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11TrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the

PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig get-virtual-attribute-prop(1)

Name

dsconfig get-virtual-attribute-prop - Shows Virtual Attribute properties

Synopsis

`dsconfig get-virtual-attribute-prop` {options}

Description

Shows Virtual Attribute properties.

Options

The `dsconfig get-virtual-attribute-prop` command takes the following options:

`--name {name}`

The name of the Virtual Attribute.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

`collective-attribute-subentries-virtual-attribute`

Default {name}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See Collective Attribute Subentries Virtual Attribute for the properties of this Virtual Attribute type.

`entity-tag-virtual-attribute`

Default {name}: Entity Tag Virtual Attribute

Enabled by default: true

See Entity Tag Virtual Attribute for the properties of this Virtual Attribute type.

`entry-dn-virtual-attribute`

Default {name}: Entry DN Virtual Attribute

Enabled by default: true

See Entry DN Virtual Attribute for the properties of this Virtual Attribute type.

`entry-uuid-virtual-attribute`

Default {name}: Entry UUID Virtual Attribute

Enabled by default: true

See Entry UUID Virtual Attribute for the properties of this Virtual Attribute type.

`governing-structure-rule-virtual-attribute`

Default {name}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See Governing Structure Rule Virtual Attribute for the properties of this Virtual Attribute type.

`has-subordinates-virtual-attribute`

Default {name}: Has Subordinates Virtual Attribute

Enabled by default: true

See Has Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`is-member-of-virtual-attribute`

Default {name}: Is Member Of Virtual Attribute

Enabled by default: true

See Is Member Of Virtual Attribute for the properties of this Virtual Attribute type.

`member-virtual-attribute`

Default {name}: Member Virtual Attribute

Enabled by default: true

See Member Virtual Attribute for the properties of this Virtual Attribute type.

`num-subordinates-virtual-attribute`

Default {name}: Num Subordinates Virtual Attribute

Enabled by default: true

See Num Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`password-expiration-time-virtual-attribute`

Default {name}: Password Expiration Time Virtual Attribute

Enabled by default: true

See Password Expiration Time Virtual Attribute for the properties of this Virtual Attribute type.

`password-policy-subentry-virtual-attribute`

Default {name}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See Password Policy Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`structural-object-class-virtual-attribute`

Default {name}: Structural Object Class Virtual Attribute

Enabled by default: true

See Structural Object Class Virtual Attribute for the properties of this Virtual Attribute type.

`subschema-subentry-virtual-attribute`

Default {name}: Subschema Subentry Virtual Attribute

Enabled by default: true

See Subschema Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`user-defined-virtual-attribute`

Default {name}: User Defined Virtual Attribute

Enabled by default: true

See User Defined Virtual Attribute for the properties of this Virtual Attribute type.

`--property {property}`

The name of a property to be displayed.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

`collective-attribute-subentries-virtual-attribute`

Default {property}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See Collective Attribute Subentries Virtual Attribute for the properties of this Virtual Attribute type.

`entity-tag-virtual-attribute`

Default {property}: Entity Tag Virtual Attribute

Enabled by default: true

See Entity Tag Virtual Attribute for the properties of this Virtual Attribute type.

`entry-dn-virtual-attribute`

Default {property}: Entry DN Virtual Attribute

Enabled by default: true

See Entry DN Virtual Attribute for the properties of this Virtual Attribute type.

`entry-uuid-virtual-attribute`

Default {property}: Entry UUID Virtual Attribute

Enabled by default: true

See Entry UUID Virtual Attribute for the properties of this Virtual Attribute type.

`governing-structure-rule-virtual-attribute`

Default {property}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See Governing Structure Rule Virtual Attribute for the properties of this Virtual Attribute type.

`has-subordinates-virtual-attribute`

Default {property}: Has Subordinates Virtual Attribute

Enabled by default: true

See Has Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`is-member-of-virtual-attribute`

Default {property}: Is Member Of Virtual Attribute

Enabled by default: true

See Is Member Of Virtual Attribute for the properties of this Virtual Attribute type.

`member-virtual-attribute`

Default {property}: Member Virtual Attribute

Enabled by default: true

See Member Virtual Attribute for the properties of this Virtual Attribute type.

`num-subordinates-virtual-attribute`

Default {property}: Num Subordinates Virtual Attribute

Enabled by default: true

See Num Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`password-expiration-time-virtual-attribute`

Default {property}: Password Expiration Time Virtual Attribute

Enabled by default: true

See Password Expiration Time Virtual Attribute for the properties of this Virtual Attribute type.

`password-policy-subentry-virtual-attribute`

Default {property}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See Password Policy Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`structural-object-class-virtual-attribute`

Default {property}: Structural Object Class Virtual Attribute

Enabled by default: true

See Structural Object Class Virtual Attribute for the properties of this Virtual Attribute type.

`subschema-subentry-virtual-attribute`

Default {property}: Subschema Subentry Virtual Attribute

Enabled by default: true

See Subschema Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`user-defined-virtual-attribute`

Default {property}: User Defined Virtual Attribute

Enabled by default: true

See User Defined Virtual Attribute for the properties of this Virtual Attribute type.

`-E | --record`

Modifies the display output to show one property value per line.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

`collective-attribute-subentries-virtual-attribute`

Default null: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See Collective Attribute Subentries Virtual Attribute for the properties of this Virtual

Attribute type.

`entity-tag-virtual-attribute`

Default null: Entity Tag Virtual Attribute

Enabled by default: true

See Entity Tag Virtual Attribute for the properties of this Virtual Attribute type.

`entry-dn-virtual-attribute`

Default null: Entry DN Virtual Attribute

Enabled by default: true

See Entry DN Virtual Attribute for the properties of this Virtual Attribute type.

`entry-uuid-virtual-attribute`

Default null: Entry UUID Virtual Attribute

Enabled by default: true

See Entry UUID Virtual Attribute for the properties of this Virtual Attribute type.

`governing-structure-rule-virtual-attribute`

Default null: Governing Structure Rule Virtual Attribute

Enabled by default: true

See Governing Structure Rule Virtual Attribute for the properties of this Virtual Attribute type.

`has-subordinates-virtual-attribute`

Default null: Has Subordinates Virtual Attribute

Enabled by default: true

See Has Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`is-member-of-virtual-attribute`

Default null: Is Member Of Virtual Attribute

Enabled by default: true

See Is Member Of Virtual Attribute for the properties of this Virtual Attribute type.

`member-virtual-attribute`

Default null: Member Virtual Attribute

Enabled by default: true

See Member Virtual Attribute for the properties of this Virtual Attribute type.

`num-subordinates-virtual-attribute`

Default null: Num Subordinates Virtual Attribute

Enabled by default: true

See Num Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`password-expiration-time-virtual-attribute`

Default null: Password Expiration Time Virtual Attribute

Enabled by default: true

See Password Expiration Time Virtual Attribute for the properties of this Virtual Attribute type.

`password-policy-subentry-virtual-attribute`

Default null: Password Policy Subentry Virtual Attribute

Enabled by default: true

See Password Policy Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`structural-object-class-virtual-attribute`

Default null: Structural Object Class Virtual Attribute

Enabled by default: true

See Structural Object Class Virtual Attribute for the properties of this Virtual Attribute type.

`subschema-subentry-virtual-attribute`

Default null: Subschema Subentry Virtual Attribute

Enabled by default: true

See Subschema Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`user-defined-virtual-attribute`

Default null: User Defined Virtual Attribute

Enabled by default: true

See User Defined Virtual Attribute for the properties of this Virtual Attribute type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

`collective-attribute-subentries-virtual-attribute`

Default {unit}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See Collective Attribute Subentries Virtual Attribute for the properties of this Virtual Attribute type.

`entity-tag-virtual-attribute`

Default {unit}: Entity Tag Virtual Attribute

Enabled by default: true

See Entity Tag Virtual Attribute for the properties of this Virtual Attribute type.

`entry-dn-virtual-attribute`

Default {unit}: Entry DN Virtual Attribute

Enabled by default: true

See Entry DN Virtual Attribute for the properties of this Virtual Attribute type.

`entry-uuid-virtual-attribute`

Default {unit}: Entry UUID Virtual Attribute

Enabled by default: true

See Entry UUID Virtual Attribute for the properties of this Virtual Attribute type.

`governing-structure-rule-virtual-attribute`

Default {unit}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See Governing Structure Rule Virtual Attribute for the properties of this Virtual Attribute type.

`has-subordinates-virtual-attribute`

Default {unit}: Has Subordinates Virtual Attribute

Enabled by default: true

See Has Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`is-member-of-virtual-attribute`

Default {unit}: Is Member Of Virtual Attribute

Enabled by default: true

See Is Member Of Virtual Attribute for the properties of this Virtual Attribute type.

`member-virtual-attribute`

Default {unit}: Member Virtual Attribute

Enabled by default: true

See Member Virtual Attribute for the properties of this Virtual Attribute type.

`num-subordinates-virtual-attribute`

Default {unit}: Num Subordinates Virtual Attribute

Enabled by default: true

See Num Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`password-expiration-time-virtual-attribute`

Default {unit}: Password Expiration Time Virtual Attribute

Enabled by default: true

See Password Expiration Time Virtual Attribute for the properties of this Virtual Attribute type.

`password-policy-subentry-virtual-attribute`

Default {unit}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See Password Policy Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`structural-object-class-virtual-attribute`

Default {unit}: Structural Object Class Virtual Attribute

Enabled by default: true

See Structural Object Class Virtual Attribute for the properties of this Virtual Attribute type.

`subschema-subentry-virtual-attribute`

Default {unit}: Subschema Subentry Virtual Attribute

Enabled by default: true

See Subschema Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`user-defined-virtual-attribute`

Default {unit}: User Defined Virtual Attribute

Enabled by default: true

See User Defined Virtual Attribute for the properties of this Virtual Attribute type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

`collective-attribute-subentries-virtual-attribute`

Default {unit}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See Collective Attribute Subentries Virtual Attribute for the properties of this Virtual Attribute type.

`entity-tag-virtual-attribute`

Default {unit}: Entity Tag Virtual Attribute

Enabled by default: true

See Entity Tag Virtual Attribute for the properties of this Virtual Attribute type.

`entry-dn-virtual-attribute`

Default {unit}: Entry DN Virtual Attribute

Enabled by default: true

See Entry DN Virtual Attribute for the properties of this Virtual Attribute type.

`entry-uuid-virtual-attribute`

Default {unit}: Entry UUID Virtual Attribute

Enabled by default: true

See Entry UUID Virtual Attribute for the properties of this Virtual Attribute type.

`governing-structure-rule-virtual-attribute`

Default {unit}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See Governing Structure Rule Virtual Attribute for the properties of this Virtual Attribute type.

`has-subordinates-virtual-attribute`

Default {unit}: Has Subordinates Virtual Attribute

Enabled by default: true

See Has Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`is-member-of-virtual-attribute`

Default {unit}: Is Member Of Virtual Attribute

Enabled by default: true

See Is Member Of Virtual Attribute for the properties of this Virtual Attribute type.

`member-virtual-attribute`

Default {unit}: Member Virtual Attribute

Enabled by default: true

See Member Virtual Attribute for the properties of this Virtual Attribute type.

`num-subordinates-virtual-attribute`

Default {unit}: Num Subordinates Virtual Attribute

Enabled by default: true

See Num Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`password-expiration-time-virtual-attribute`

Default {unit}: Password Expiration Time Virtual Attribute

Enabled by default: true

See Password Expiration Time Virtual Attribute for the properties of this Virtual Attribute type.

`password-policy-subentry-virtual-attribute`

Default {unit}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See Password Policy Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`structural-object-class-virtual-attribute`

Default {unit}: Structural Object Class Virtual Attribute

Enabled by default: true

See Structural Object Class Virtual Attribute for the properties of this Virtual Attribute type.

`subschema-subentry-virtual-attribute`

Default {unit}: Subschema Subentry Virtual Attribute

Enabled by default: true

See Subschema Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`user-defined-virtual-attribute`

Default {unit}: User Defined Virtual Attribute

Enabled by default: true

See User Defined Virtual Attribute for the properties of this Virtual Attribute type.

Collective Attribute Subentries Virtual Attribute

Virtual Attributes of type collective-attribute-subentries-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

collectiveAttributeSubentries

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.CollectiveAttributeSubentriesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Entity Tag Virtual Attribute

Virtual Attributes of type entity-tag-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

etag

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

checksum-algorithm

Description

The algorithm which should be used for calculating the entity tag checksum value.

Default Value

adler-32

Allowed Values

adler-32

The Adler-32 checksum algorithm which is almost as reliable as a CRC-32 but can be computed much faster.

crc-32

The CRC-32 checksum algorithm.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

excluded-attribute

Description

The list of attributes which should be ignored when calculating the entity tag checksum value. Certain attributes like "ds-sync-hist" may vary between replicas due to different purging schedules and should not be included in the checksum.

Default Value

ds-sync-hist

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to

use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntityTagVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Entry DN Virtual Attribute

Virtual Attributes of type entry-dn-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryDN

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no

values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryDNVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Entry UUID Virtual Attribute

Virtual Attributes of type entry-uuid-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryUUID

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryUUIDVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Governing Structure Rule Virtual Attribute

Virtual Attributes of type governing-structure-rule-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

governingStructureRule

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.GoverningSturctureRuleVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Has Subordinates Virtual Attribute

Virtual Attributes of type has-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

hasSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry

and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those

filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.HasSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Is Member Of Virtual Attribute

Virtual Attributes of type is-member-of-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

isMemberOf

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.IsMemberOfVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Member Virtual Attribute

Virtual Attributes of type member-virtual-attribute have the following properties:

allow-retrieving-membership

Description

Indicates whether to handle requests that request all values for the virtual attribute. This operation can be very expensive in some cases and is not consistent with the primary function of virtual static groups, which is to make it possible to use static group idioms to determine whether a given user is a member. If this attribute is set to false, attempts to retrieve the entire set of values receive an empty set, and only attempts to determine whether the attribute has a

specific value or set of values (which is the primary anticipated use for virtual static groups) are handled properly.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.MemberVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Num Subordinates Virtual Attribute

Virtual Attributes of type num-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

numSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to

use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.NumSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Password Expiration Time Virtual Attribute

Virtual Attributes of type password-expiration-time-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

ds-pwp-password-expiration-time

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no

values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordExpirationTimeVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Password Policy Subentry Virtual Attribute

Virtual Attributes of type password-policy-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

pwdPolicySubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordPolicySubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Structural Object Class Virtual Attribute

Virtual Attributes of type structural-object-class-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

structuralObjectClass

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.StructuralObjectClassVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subschema Subentry Virtual Attribute

Virtual Attributes of type subschema-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

subschemaSubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry

and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those

filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.SubschemaSubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

User Defined Virtual Attribute

Virtual Attributes of type user-defined-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.UserDefinedVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

value

Description

Specifies the values to be included in the virtual attribute.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-work-queue-prop(1)

Name

dsconfig get-work-queue-prop - Shows Work Queue properties

Synopsis

`dsconfig get-work-queue-prop` {options}

Description

Shows Work Queue properties.

Options

The `dsconfig get-work-queue-prop` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Work Queue properties depend on the Work Queue type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Work Queue types:

`parallel-work-queue`

Default {property}: Parallel Work Queue

Enabled by default: false

See Parallel Work Queue for the properties of this Work Queue type.

`traditional-work-queue`

Default {property}: Traditional Work Queue

Enabled by default: false

See Traditional Work Queue for the properties of this Work Queue type.

`-E | --record`

Modifies the display output to show one property value per line.

Work Queue properties depend on the Work Queue type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Work Queue types:

`parallel-work-queue`

Default null: Parallel Work Queue

Enabled by default: false

See Parallel Work Queue for the properties of this Work Queue type.

`traditional-work-queue`

Default null: Traditional Work Queue

Enabled by default: false

See Traditional Work Queue for the properties of this Work Queue type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Work Queue properties depend on the Work Queue type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Work Queue types:

`parallel-work-queue`

Default {unit}: Parallel Work Queue

Enabled by default: false

See Parallel Work Queue for the properties of this Work Queue type.

`traditional-work-queue`

Default {unit}: Traditional Work Queue

Enabled by default: false

See Traditional Work Queue for the properties of this Work Queue type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Work Queue properties depend on the Work Queue type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Work Queue types:

`parallel-work-queue`

Default {unit}: Parallel Work Queue

Enabled by default: false

See Parallel Work Queue for the properties of this Work Queue type.

`traditional-work-queue`

Default {unit}: Traditional Work Queue

Enabled by default: false

See Traditional Work Queue for the properties of this Work Queue type.

Parallel Work Queue

Work Queues of type parallel-work-queue have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Parallel Work Queue implementation.

Default Value

org.opends.server.extensions.ParallelWorkQueue

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.WorkQueue

Multi-valued

No

Required

Yes

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-worker-threads

Description

Specifies the number of worker threads to be used for processing operations placed in the queue. If the value is increased, the additional worker threads are created immediately. If the value is reduced, the appropriate number of threads are destroyed as operations complete processing.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Traditional Work Queue

Work Queues of type traditional-work-queue have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Traditional Work Queue implementation.

Default Value

org.opends.server.extensions.TraditionalWorkQueue

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.WorkQueue

Multi-valued

No

Required

Yes

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-work-queue-capacity

Description

Specifies the maximum number of queued operations that can be in the work queue at any given time. If the work queue is already full and additional requests are received by the server, then the server front end, and possibly the client, will be blocked until the work queue has available capacity.

Default Value

1000

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

num-worker-threads

Description

Specifies the number of worker threads to be used for processing operations placed in the queue. If the value is increased, the additional worker threads are created immediately. If the value is reduced, the appropriate number of threads are destroyed as operations complete processing.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-access-log-filtering-criteria(1)

Name

dsconfig list-access-log-filtering-criteria - Lists existing Access Log Filtering Criteria

Synopsis

`dsconfig list-access-log-filtering-criteria` {options}

Description

Lists existing Access Log Filtering Criteria.

Options

The `dsconfig list-access-log-filtering-criteria` command takes the following options:

`--publisher-name {name}`

The name of the Access Log Publisher.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

`--property {property}`

The name of a property to be displayed.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default {property}: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default {unit}: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default {unit}: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

Access Log Filtering Criteria

Access Log Filtering Criteria of type access-log-filtering-criteria have the following properties:

connection-client-address-equal-to

Description

Filters log records associated with connections which match at least one of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-client-address-not-equal-to

Description

Filters log records associated with connections which do not match any of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-port-equal-to

Description

Filters log records associated with connections to any of the specified listener port numbers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-protocol-equal-to

Description

Filters log records associated with connections which match any of the specified protocols. Typical values include "ldap", "ldaps", or "jmx".

Default Value

None

Allowed Values

The protocol name as reported in the access log.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-type

Description

Filters log records based on their type.

Default Value

None

Allowed Values

abandon

Abandon operations

add

Add operations

bind

Bind operations

compare

Compare operations

connect

Client connections

delete

Delete operations

disconnect

Client disconnections

extended

Extended operations

modify

Modify operations

rename

Rename operations

search

Search operations

unbind

Unbind operations

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-equal-to

Description

Filters operation log records associated with operations which target entries matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-not-equal-to

Description

Filters operation log records associated with operations which target entries matching none of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in**

uid=dmiller,,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-greater-than

Description

Filters operation response log records associated with operations which took longer than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-less-than

Description

Filters operation response log records associated with operations which took less than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-equal-to

Description

Filters operation response log records associated with operations which include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-not-equal-to

Description

Filters operation response log records associated with operations which do not include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-is-indexed

Description

Filters search operation response log records associated with searches which were either

indexed or unindexed. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-greater-than

Description

Filters search operation response log records associated with searches which returned more than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-less-than

Description

Filters search operation response log records associated with searches which returned less than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-equal-to

Description

Filters log records associated with users matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-not-equal-to

Description

Filters log records associated with users which do not match any of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-member-of

Description

Filters log records associated with users which are members of at least one of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-not-member-of

Description

Filters log records associated with users which are not members of any of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-account-status-notification-handlers(1)

Name

dsconfig list-account-status-notification-handlers - Lists existing Account Status Notification Handlers

Synopsis

`dsconfig list-account-status-notification-handlers` {options}

Description

Lists existing Account Status Notification Handlers.

Options

The `dsconfig list-account-status-notification-handlers` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

`error-log-account-status-notification-handler`

Default {property}: Error Log Account Status Notification Handler

Enabled by default: true

See Error Log Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`smtp-account-status-notification-handler`

Default {property}: SMTP Account Status Notification Handler

Enabled by default: true

See SMTP Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

`error-log-account-status-notification-handler`

Default {unit}: Error Log Account Status Notification Handler

Enabled by default: true

See Error Log Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`smtp-account-status-notification-handler`

Default {unit}: SMTP Account Status Notification Handler

Enabled by default: true

See SMTP Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

`error-log-account-status-notification-handler`

Default {unit}: Error Log Account Status Notification Handler

Enabled by default: true

See Error Log Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`smtp-account-status-notification-handler`

Default {unit}: SMTP Account Status Notification Handler

Enabled by default: true

See SMTP Account Status Notification Handler for the properties of this Account Status

Notification Handler type.

Error Log Account Status Notification Handler

Account Status Notification Handlers of type error-log-account-status-notification-handler have the following properties:

account-status-notification-type

Description

Indicates which types of event can trigger an account status notification.

Default Value

None

Allowed Values

account-disabled

Generate a notification whenever a user account has been disabled by an administrator.

account-enabled

Generate a notification whenever a user account has been enabled by an administrator.

account-expired

Generate a notification whenever a user authentication has failed because the account has expired.

account-idle-locked

Generate a notification whenever a user account has been locked because it was idle for too long.

account-permanently-locked

Generate a notification whenever a user account has been permanently locked after too many failed attempts.

account-reset-locked

Generate a notification whenever a user account has been locked, because the password had been reset by an administrator but not changed by the user within the required interval.

account-temporarily-locked

Generate a notification whenever a user account has been temporarily locked after too many failed attempts.

account-unlocked

Generate a notification whenever a user account has been unlocked by an administrator.

password-changed

Generate a notification whenever a user changes his/her own password.

password-expired

Generate a notification whenever a user authentication has failed because the password has expired.

password-expiring

Generate a notification whenever a password expiration warning is encountered for a user password for the first time.

password-reset

Generate a notification whenever a user's password is reset by an administrator.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Error Log Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.ErrorLogAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

SMTP Account Status Notification Handler

Account Status Notification Handlers of type smtp-account-status-notification-handler have the following properties:

email-address-attribute-type

Description

Specifies which attribute in the user's entries may be used to obtain the email address when notifying the end user. You can specify more than one email address as separate values. In this case, the OpenDJ server sends a notification to all email addresses identified.

Default Value

If no email address attribute types are specified, then no attempt is made to send email notification messages to end users. Only those users specified in the set of additional recipient addresses are sent the notification messages.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.SMTPAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this account status notification handler. The values for this property should begin with the name of an account status notification type followed by a colon and the subject that should be used for the associated notification message. If an email message is generated for an account status notification type for which no subject is defined, then that message is given a generic subject.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-template-file

Description

Specifies the path to the file containing the message template to generate the email notification messages. The values for this property should begin with the name of an account status notification type followed by a colon and the path to the template file that should be used for that notification type. If an account status notification has a notification type that is not associated with a message template file, then no email message is generated for that notification.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which notification messages are sent, either instead of or in addition to the end user for whom the notification has been generated. This may be used to ensure that server administrators also receive a copy of any notification messages that are generated.

Default Value

If no additional recipient addresses are specified, then only the end users that are the subjects of the account status notifications receive the notification messages.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

send-email-as-html

Description

Indicates whether an email notification message should be sent as HTML. If this value is true, email notification messages are marked as text/html. Otherwise outgoing email messages are assumed to be plaintext and marked as text/plain.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-message-without-end-user-address

Description

Indicates whether an email notification message should be generated and sent to the set of notification recipients even if the user entry does not contain any values for any of the email address attributes (that is, in cases when it is not be possible to notify the end user). This is only applicable if both one or more email address attribute types and one or more additional recipient addresses are specified.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

sender-address

Description

Specifies the email address from which the message is sent. Note that this does not necessarily have to be a legitimate email address.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-alert-handlers(1)

Name

dsconfig list-alert-handlers - Lists existing Alert Handlers

Synopsis

`dsconfig list-alert-handlers` {options}

Description

Lists existing Alert Handlers.

Options

The `dsconfig list-alert-handlers` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Alert Handler properties depend on the Alert Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

`jmx-alert-handler`

Default {property}: JMX Alert Handler

Enabled by default: true

See JMX Alert Handler for the properties of this Alert Handler type.

`smtp-alert-handler`

Default {property}: SMTP Alert Handler

Enabled by default: true

See SMTP Alert Handler for the properties of this Alert Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Alert Handler properties depend on the Alert Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

`jmx-alert-handler`

Default {unit}: JMX Alert Handler

Enabled by default: true

See JMX Alert Handler for the properties of this Alert Handler type.

`smtp-alert-handler`

Default {unit}: SMTP Alert Handler

Enabled by default: true

See SMTP Alert Handler for the properties of this Alert Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Alert Handler properties depend on the Alert Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

`jmx-alert-handler`

Default {unit}: JMX Alert Handler

Enabled by default: true

See JMX Alert Handler for the properties of this Alert Handler type.

`smtp-alert-handler`

Default {unit}: SMTP Alert Handler

Enabled by default: true

See SMTP Alert Handler for the properties of this Alert Handler type.

JMX Alert Handler

Alert Handlers of type jmx-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Alert Handler implementation.

Default Value

org.opends.server.extensions.JMXAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

SMTP Alert Handler

Alert Handlers of type smtp-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Alert Handler implementation.

Default Value

org.opends.server.extensions.SMTPAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-body

Description

Specifies the body that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which the messages should be sent. Multiple values may be provided if there should be more than one recipient.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

sender-address

Description

Specifies the email address to use as the sender for messages generated by this alert handler.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-backend-indexes(1)

Name

dsconfig list-backend-indexes - Lists existing Backend Indexes

Synopsis

`dsconfig list-backend-indexes` {options}

Description

Lists existing Backend Indexes.

Options

The `dsconfig list-backend-indexes` command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend Index properties depend on the Backend Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default {name}: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

`--property {property}`

The name of a property to be displayed.

Backend Index properties depend on the Backend Index type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default {property}: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Backend Index properties depend on the Backend Index type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default {unit}: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Backend Index properties depend on the Backend Index type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default {unit}: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

Backend Index

Backend Indexes of type backend-index have the following properties:

attribute

Description

Specifies the name of the attribute for which the index is to be maintained.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

confidentiality-enabled

Description

Specifies whether contents of the index should be confidential. Setting the flag to true will hash keys for equality type indexes using SHA-1 and encrypt the list of entries matching a substring key for substring indexes.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

If the index for the attribute must be protected for security purposes and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate. The property cannot be set on a backend for which confidentiality is not enabled.

Advanced Property

No

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that are allowed to match a given index key before that particular index key is no longer maintained. This is analogous to the ALL IDs threshold in the Sun Java System Directory Server. If this is specified, its value overrides the JE backend-wide

configuration. For no limit, use 0 for the value.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

If any index keys have already reached this limit, indexes must be rebuilt before they will be allowed to use the new limit.

Advanced Property

No

Read-only

No

index-extensible-matching-rule

Description

The extensible matching rule in an extensible index. An extensible matching rule must be specified using either LOCALE or OID of the matching rule.

Default Value

No extensible matching rules will be indexed.

Allowed Values

A Locale or an OID.

Multi-valued

Yes

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

No

Read-only

No

index-type

Description

Specifies the type(s) of indexing that should be performed for the associated attribute. For equality, presence, and substring index types, the associated attribute type must have a corresponding matching rule.

Default Value

None

Allowed Values

approximate

This index type is used to improve the efficiency of searches using approximate matching search filters.

equality

This index type is used to improve the efficiency of searches using equality search filters.

extensible

This index type is used to improve the efficiency of searches using extensible matching search filters.

ordering

This index type is used to improve the efficiency of searches using "greater than or equal to" or "less then or equal to" search filters.

presence

This index type is used to improve the efficiency of searches using the presence search filters.

substring

This index type is used to improve the efficiency of searches using substring search filters.

Multi-valued

Yes

Required

Yes

Admin Action Required

If any new index types are added for an attribute, and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate.

Advanced Property

No

Read-only

No

substring-length

Description

The length of substrings in a substring index.

Default Value

6

Allowed Values

An integer value. Lower value is 3.

Multi-valued

No

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-backend-vlv-indexes(1)

Name

dsconfig list-backend-vlv-indexes - Lists existing Backend VLV Indexes

Synopsis

`dsconfig list-backend-vlv-indexes` {options}

Description

Lists existing Backend VLV Indexes.

Options

The `dsconfig list-backend-vlv-indexes` command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default {name}: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

`--property {property}`

The name of a property to be displayed.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default {property}: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default {unit}: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default {unit}: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

Backend VLV Index

Backend VLV Indexes of type backend-vlv-index have the following properties:

base-dn

Description

Specifies the base DN used in the search query that is being indexed.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

filter

Description

Specifies the LDAP filter used in the query that is being indexed.

Default Value

None

Allowed Values

A valid LDAP search filter.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

name

Description

Specifies a unique name for this VLV index.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

NoneThe VLV index name cannot be altered after the index is created.

Advanced Property

No

Read-only

Yes

scope

Description

Specifies the LDAP scope of the query that is being indexed.

Default Value

None

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

sort-order

Description

Specifies the names of the attributes that are used to sort the entries for the query being indexed. Multiple attributes can be used to determine the sort order by listing the attribute names from highest to lowest precedence. Optionally, + or - can be prefixed to the attribute name to sort the attribute in ascending order or descending order respectively.

Default Value

None

Allowed Values

Valid attribute types defined in the schema, separated by a space and optionally prefixed by + or -.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

dsconfig list-backends(1)

Name

dsconfig list-backends - Lists existing Backends

Synopsis

`dsconfig list-backends` {options}

Description

Lists existing Backends.

Options

The `dsconfig list-backends` command takes the following options:

`--property {property}`
: The name of a property to be displayed.

  Backend properties depend on the Backend type, which depends on the {property} you provide.

  By default, OpenDJ directory server supports the following Backend types:

  `backup-backend`
  : Default {property}: Backup Backend

    Enabled by default: true

    See Backup Backend for the properties of this Backend type.

  `cas-backend`
  : Default {property}: CAS Backend

    Enabled by default: true

    See CAS Backend for the properties of this Backend type.

  `jdbc-backend`
  : Default {property}: JDBC Backend

    Enabled by default: true

    See JDBC Backend for the properties of this Backend type.

  `je-backend`
  : Default {property}: JE Backend

Enabled by default: true

See JE Backend for the properties of this Backend type.

`ldif-backend`

Default {property}: LDIF Backend

Enabled by default: true

See LDIF Backend for the properties of this Backend type.

`memory-backend`

Default {property}: Memory Backend

Enabled by default: true

See Memory Backend for the properties of this Backend type.

`monitor-backend`

Default {property}: Monitor Backend

Enabled by default: true

See Monitor Backend for the properties of this Backend type.

`null-backend`

Default {property}: Null Backend

Enabled by default: true

See Null Backend for the properties of this Backend type.

`pdb-backend`

Default {property}: PDB Backend

Enabled by default: true

See PDB Backend for the properties of this Backend type.

`schema-backend`

Default {property}: Schema Backend

Enabled by default: true

See Schema Backend for the properties of this Backend type.

`task-backend`

Default {property}: Task Backend

Enabled by default: true

See Task Backend for the properties of this Backend type.

`trust-store-backend`

Default {property}: Trust Store Backend

Enabled by default: true

See Trust Store Backend for the properties of this Backend type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Backend properties depend on the Backend type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend types:

`backup-backend`

Default {unit}: Backup Backend

Enabled by default: true

See Backup Backend for the properties of this Backend type.

`cas-backend`

Default {unit}: CAS Backend

Enabled by default: true

See CAS Backend for the properties of this Backend type.

`jdbc-backend`

Default {unit}: JDBC Backend

Enabled by default: true

See JDBC Backend for the properties of this Backend type.

`je-backend`

Default {unit}: JE Backend

Enabled by default: true

See JE Backend for the properties of this Backend type.

`ldif-backend`

Default {unit}: LDIF Backend

Enabled by default: true

See LDIF Backend for the properties of this Backend type.

`memory-backend`

Default {unit}: Memory Backend

Enabled by default: true

See Memory Backend for the properties of this Backend type.

`monitor-backend`

Default {unit}: Monitor Backend

Enabled by default: true

See Monitor Backend for the properties of this Backend type.

`null-backend`

Default {unit}: Null Backend

Enabled by default: true

See Null Backend for the properties of this Backend type.

`pdb-backend`

Default {unit}: PDB Backend

Enabled by default: true

See PDB Backend for the properties of this Backend type.

`schema-backend`

Default {unit}: Schema Backend

Enabled by default: true

See Schema Backend for the properties of this Backend type.

`task-backend`

Default {unit}: Task Backend

Enabled by default: true

See Task Backend for the properties of this Backend type.

`trust-store-backend`

Default {unit}: Trust Store Backend

Enabled by default: true

See Trust Store Backend for the properties of this Backend type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w

(milliseconds, seconds, minutes, hours, days, or weeks).

Backend properties depend on the Backend type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend types:

`backup-backend`

Default {unit}: Backup Backend

Enabled by default: true

See Backup Backend for the properties of this Backend type.

`cas-backend`

Default {unit}: CAS Backend

Enabled by default: true

See CAS Backend for the properties of this Backend type.

`jdbc-backend`

Default {unit}: JDBC Backend

Enabled by default: true

See JDBC Backend for the properties of this Backend type.

`je-backend`

Default {unit}: JE Backend

Enabled by default: true

See JE Backend for the properties of this Backend type.

`ldif-backend`

Default {unit}: LDIF Backend

Enabled by default: true

See LDIF Backend for the properties of this Backend type.

`memory-backend`

Default {unit}: Memory Backend

Enabled by default: true

See Memory Backend for the properties of this Backend type.

`monitor-backend`

Default {unit}: Monitor Backend

Enabled by default: true

See Monitor Backend for the properties of this Backend type.

`null-backend`

Default {unit}: Null Backend

Enabled by default: true

See Null Backend for the properties of this Backend type.

`pdb-backend`

Default {unit}: PDB Backend

Enabled by default: true

See PDB Backend for the properties of this Backend type.

`schema-backend`

Default {unit}: Schema Backend

Enabled by default: true

See Schema Backend for the properties of this Backend type.

`task-backend`

Default {unit}: Task Backend

Enabled by default: true

See Task Backend for the properties of this Backend type.

`trust-store-backend`

Default {unit}: Trust Store Backend

Enabled by default: true

See Trust Store Backend for the properties of this Backend type.

Backup Backend

Backends of type backup-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

backup-directory

Description

Specifies the path to a backup directory containing one or more backups for a particular backend. This is a multivalued property. Each value may specify a different backup directory if desired (one for each backend for which backups are taken). Values may be either absolute paths or paths that are relative to the base of the OpenDJ directory server installation.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.BackupBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

CAS Backend

Backends of type cas-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-directory

Description

Specifies the keyspace name The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

ldap_opendj

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search

filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.cassandra.Backend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

JDBC Backend

Backends of type jdbc-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-directory

Description

Specifies the connection string jdbc:postgresql://localhost/test

Default Value

jdbc:postgresql://localhost/test

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.jdbc.Backend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be

more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

JE Backend

Backends of type je-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be

responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-bytes-interval

Description

Specifies the maximum number of bytes that may be written to the database before it is forced to perform a checkpoint. This can be used to bound the recovery time that may be required if the database environment is opened without having been properly closed. If this property is set to a non-zero value, the checkpointer wakeup interval is not used. To use time-based checkpointing, set this property to zero.

Default Value

500mb

Allowed Values

Upper value is 9223372036854775807.

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. Note that this is only used if the value of the checkpointer bytes interval is zero.

Default Value

30s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.Upper limit is 4294 seconds.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-cleaner-min-utilization

Description

Specifies the occupancy percentage for "live" data in this backend's database. When the amount of "live" data in the database drops below this value, cleaners will act to increase the occupancy percentage by compacting the database.

Default Value

50

Allowed Values

An integer value. Lower value is 0. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Berkeley DB Java Edition database files containing the data for this backend. The path may be either an absolute path or a

path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-core-threads

Description

Specifies the core number of threads in the eviction thread pool. Specifies the core number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

1

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-keep-alive

Description

The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

600s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.Upper limit is 86400 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-lru-only

Description

Indicates whether the database should evict existing data from the cache based on an LRU policy (where the least recently used information will be evicted first). If set to "false", then the eviction keeps internal nodes of the underlying Btree in the cache over leaf nodes, even if the leaf nodes have been accessed more recently. This may be a better configuration for databases in which only a very small portion of the data is cached.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-max-threads

Description

Specifies the maximum number of threads in the eviction thread pool. Specifies the maximum number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-nodes-per-scan

Description

Specifies the number of Btree nodes that should be evicted from the cache in a single pass if it is determined that it is necessary to free existing data in order to make room for new information. Changes to this property do not take effect until the backend is restarted. It is recommended that you also change this property when you set db-evictor-lru-only to false. This setting controls the number of Btree nodes that are considered, or sampled, each time a node is evicted. A setting of 10 often produces good results, but this may vary from application to application. The larger the nodes per scan, the more accurate the algorithm. However, don't set it too high. When considering larger numbers of nodes for each eviction, the evictor may delay the completion of a given database operation, which impacts the response time of the application thread. In JE 4.1 and later, setting this value too high in an application that is largely CPU bound can reduce the effectiveness of cache eviction. It's best to start with the default value, and increase it gradually to see if it is beneficial for your application.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 1000.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-file-max

Description

Specifies the maximum size for a database log file.

Default Value

100mb

Allowed Values

Lower value is 1000000.Upper value is 4294967296.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-filecache-size

Description

Specifies the size of the file handle cache. The file handle cache is used to keep as much opened log files as possible. When the cache is smaller than the number of logs, the database needs to close some handles and open log files it needs, resulting in less optimal performances. Ideally, the size of the cache should be higher than the number of files contained in the database. Make sure the OS number of open files per process is also tuned appropriately.

Default Value

100

Allowed Values

An integer value. Lower value is 3. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-file-handler-on

Description

Indicates whether the database should maintain a je.info file in the same directory as the database log directory. This file contains information about the internal processing performed by the underlying database.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-level

Description

Specifies the log level that should be used by the database when it is writing information into the je.info file. The database trace logging level is (in increasing order of verbosity) chosen from: OFF, SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST, ALL.

Default Value

CONFIG

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-cleaner-threads

Description

Specifies the number of threads that the backend should maintain to keep the database log files at or near the desired utilization. In environments with high write throughput, multiple cleaner threads may be required to maintain the desired utilization.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-lock-tables

Description

Specifies the number of lock tables that are used by the underlying database. This can be particularly important to help improve scalability by avoiding contention on systems with large numbers of CPUs. The value of this configuration property should be set to a prime number that is less than or equal to the number of worker threads configured for use in the server.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 32767.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-run-cleaner

Description

Indicates whether the cleaner threads should be enabled to compact the database. The cleaner threads are used to periodically compact the database when it reaches a percentage of occupancy lower than the amount specified by the db-cleaner-min-utilization property. They identify database files with a low percentage of live data, and relocate their remaining live data to the end of the log.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-write-no-sync

Description

Indicates whether the database should synchronously flush data as it is written to disk. If this value is set to "false", then all data written to disk is synchronously flushed to persistent storage and thereby providing full durability. If it is set to "true", then data may be cached for a period of time by the underlying operating system before actually being written to disk. This may improve performance, but could cause the most recent changes to be lost in the event of an underlying OS or hardware failure (but not in the case that the OpenDJ directory server or the JVM exits abnormally).

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by

this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.jeb.JEBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

je-property

Description

Specifies the database and environment properties for the Berkeley DB Java Edition database serving the data for this backend. Any Berkeley DB Java Edition property can be specified using the following form: property-name=property-value. Refer to OpenDJ documentation for further information on related properties, their implications, and range values. The definitive identification of all the property parameters is available in the example.properties file of Berkeley DB Java Edition distribution.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be

more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

LDIF Backend

Backends of type ldif-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be

responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

is-private-backend

Description

Indicates whether the backend should be considered a private backend, which indicates that it is used for storing operational data rather than user-defined information.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.LDIFBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-file

Description

Specifies the path to the LDIF file containing the data for this backend.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Memory Backend

Backends of type memory-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its

contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MemoryBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Monitor Backend

Backends of type monitor-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MonitorBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Null Backend

Backends of type null-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.NullBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

PDB Backend

Backends of type pdb-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents.

Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. This setting controls the elapsed time between attempts to write a checkpoint to the journal. A longer interval allows more updates to accumulate in buffers before they are required to be written to disk, but also potentially causes recovery from an abrupt termination (crash) to take more time.

Default Value

15s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 10 seconds.Upper limit is 3600 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Persistit database files containing the data for this backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.pdb.PDBBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be

more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Schema Backend

Backends of type schema-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be

responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.SchemaBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

schema-entry-dn

Description

Defines the base DNs of the subtrees in which the schema information is published in addition to the value included in the base-dn property. The value provided in the base-dn property is the only one that appears in the subschemaSubentry operational attribute of the server's root DSE (which is necessary because that is a single-valued attribute) and as a virtual attribute in other entries. The schema-entry-dn attribute may be used to make the schema information available in other locations to accommodate certain client applications that have been hard-coded to expect the schema to reside in a specific location.

Default Value

cn=schema

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

show-all-attributes

Description

Indicates whether to treat all attributes in the schema entry as if they were user attributes regardless of their configuration. This may provide compatibility with some applications that expect schema attributes like attributeTypes and objectClasses to be included by default even if they are not requested. Note that the ldapSyntaxes attribute is always treated as operational in order to avoid problems with attempts to modify the schema over protocol.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Task Backend

Backends of type task-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.task.TaskBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

notification-sender-address

Description

Specifies the email address to use as the sender (that is, the "From:" address) address for notification mail messages generated when a task completes execution.

Default Value

The default sender address used is "opendj-task-notification@" followed by the canonical address of the system on which the server is running.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

task-backing-file

Description

Specifies the path to the backing file for storing information about the tasks configured in the server. It may be either an absolute path or a relative path to the base of the OpenDJ directory server instance.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

task-retention-time

Description

Specifies the length of time that task entries should be retained after processing on the associated task has been completed.

Default Value

24 hours

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Trust Store Backend

Backends of type trust-store-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.TrustStoreBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file that stores the trust information. It may be an absolute path, or a path that is relative to the OpenDJ instance root.

Default Value

config/ads-truststore

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the

clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well.

Default Value

The JVM default value is used.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect the next time that the key manager is accessed.

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-certificate-mappers(1)

Name

dsconfig list-certificate-mappers - Lists existing Certificate Mappers

Synopsis

`dsconfig list-certificate-mappers` {options}

Description

Lists existing Certificate Mappers.

Options

The `dsconfig list-certificate-mappers` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

`fingerprint-certificate-mapper`

Default {property}: Fingerprint Certificate Mapper

Enabled by default: true

See Fingerprint Certificate Mapper for the properties of this Certificate Mapper type.

`subject-attribute-to-user-attribute-certificate-mapper`

Default {property}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See Subject Attribute To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-dn-to-user-attribute-certificate-mapper`

Default {property}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See Subject DN To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-equals-dn-certificate-mapper`

Default {property}: Subject Equals DN Certificate Mapper

Enabled by default: true

See Subject Equals DN Certificate Mapper for the properties of this Certificate Mapper type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

`fingerprint-certificate-mapper`

Default {unit}: Fingerprint Certificate Mapper

Enabled by default: true

See Fingerprint Certificate Mapper for the properties of this Certificate Mapper type.

`subject-attribute-to-user-attribute-certificate-mapper`

Default {unit}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See Subject Attribute To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-dn-to-user-attribute-certificate-mapper`

Default {unit}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See Subject DN To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-equals-dn-certificate-mapper`

Default {unit}: Subject Equals DN Certificate Mapper

Enabled by default: true

See Subject Equals DN Certificate Mapper for the properties of this Certificate Mapper type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the

{unit} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

`fingerprint-certificate-mapper`

Default {unit}: Fingerprint Certificate Mapper

Enabled by default: true

See Fingerprint Certificate Mapper for the properties of this Certificate Mapper type.

`subject-attribute-to-user-attribute-certificate-mapper`

Default {unit}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See Subject Attribute To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-dn-to-user-attribute-certificate-mapper`

Default {unit}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See Subject DN To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-equals-dn-certificate-mapper`

Default {unit}: Subject Equals DN Certificate Mapper

Enabled by default: true

See Subject Equals DN Certificate Mapper for the properties of this Certificate Mapper type.

Fingerprint Certificate Mapper

Certificate Mappers of type fingerprint-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-algorithm

Description

Specifies the name of the digest algorithm to compute the fingerprint of client certificates.

Default Value

None

Allowed Values

md5

Use the MD5 digest algorithm to compute certificate fingerprints.

sha1

Use the SHA-1 digest algorithm to compute certificate fingerprints.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-attribute

Description

Specifies the attribute in which to look for the fingerprint. Values of the fingerprint attribute should exactly match the MD5 or SHA1 representation of the certificate fingerprint.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fingerprint Certificate Mapper implementation.

Default Value

org.opends.server.extensions.FingerprintCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs are used when performing searches to map the client certificates to a user entry.

Default Value

The server performs the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subject Attribute To User Attribute Certificate Mapper

Certificate Mappers of type subject-attribute-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Attribute To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectAttributeToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute-mapping

Description

Specifies a mapping between certificate attributes and user attributes. Each value should be in the form "certattr:userattr" where certattr is the name of the attribute in the certificate subject and userattr is the name of the corresponding attribute in user entries. There may be multiple mappings defined, and when performing the mapping values for all attributes present in the certificate subject that have mappings defined must be present in the corresponding user entries.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subject DN To User Attribute Certificate Mapper

Certificate Mappers of type subject-dn-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject DN To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectDNToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute

Description

Specifies the name or OID of the attribute whose value should exactly match the certificate subject DN.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subject Equals DN Certificate Mapper

Certificate Mappers of type subject-equals-dn-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Equals DN Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectEqualsDNCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-connection-handlers(1)

Name

dsconfig list-connection-handlers - Lists existing Connection Handlers

Synopsis

`dsconfig list-connection-handlers` {options}

Description

Lists existing Connection Handlers.

Options

The `dsconfig list-connection-handlers` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Connection Handler properties depend on the Connection Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

`http-connection-handler`

Default {property}: HTTP Connection Handler

Enabled by default: true

See HTTP Connection Handler for the properties of this Connection Handler type.

`jmx-connection-handler`

Default {property}: JMX Connection Handler

Enabled by default: true

See JMX Connection Handler for the properties of this Connection Handler type.

`ldap-connection-handler`

Default {property}: LDAP Connection Handler

Enabled by default: true

See LDAP Connection Handler for the properties of this Connection Handler type.

`ldif-connection-handler`

Default {property}: LDIF Connection Handler

Enabled by default: true

See LDIF Connection Handler for the properties of this Connection Handler type.

`snmp-connection-handler`

Default {property}: SNMP Connection Handler

Enabled by default: true

See SNMP Connection Handler for the properties of this Connection Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Connection Handler properties depend on the Connection Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

`http-connection-handler`

Default {unit}: HTTP Connection Handler

Enabled by default: true

See HTTP Connection Handler for the properties of this Connection Handler type.

`jmx-connection-handler`

Default {unit}: JMX Connection Handler

Enabled by default: true

See JMX Connection Handler for the properties of this Connection Handler type.

`ldap-connection-handler`

Default {unit}: LDAP Connection Handler

Enabled by default: true

See LDAP Connection Handler for the properties of this Connection Handler type.

`ldif-connection-handler`

Default {unit}: LDIF Connection Handler

Enabled by default: true

See LDIF Connection Handler for the properties of this Connection Handler type.

`snmp-connection-handler`

Default {unit}: SNMP Connection Handler

Enabled by default: true

See SNMP Connection Handler for the properties of this Connection Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Connection Handler properties depend on the Connection Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

`http-connection-handler`

Default {unit}: HTTP Connection Handler

Enabled by default: true

See HTTP Connection Handler for the properties of this Connection Handler type.

`jmx-connection-handler`

Default {unit}: JMX Connection Handler

Enabled by default: true

See JMX Connection Handler for the properties of this Connection Handler type.

`ldap-connection-handler`

Default {unit}: LDAP Connection Handler

Enabled by default: true

See LDAP Connection Handler for the properties of this Connection Handler type.

`ldif-connection-handler`

Default {unit}: LDIF Connection Handler

Enabled by default: true

See LDIF Connection Handler for the properties of this Connection Handler type.

`snmp-connection-handler`

Default {unit}: SNMP Connection Handler

Enabled by default: true

See SNMP Connection Handler for the properties of this Connection Handler type.

HTTP Connection Handler

Connection Handlers of type http-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the HTTP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the HTTP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer HTTP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Connection Handler implementation.

Default Value

org.opends.server.protocols.http.HTTPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the HTTP Connection Handler should keep statistics. If enabled, the HTTP Connection Handler maintains statistics about the number and types of operations requested over HTTP and the amount of data sent and received.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this HTTP Connection Handler should listen for connections from HTTP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the HTTP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take

effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the HTTP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to HTTP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-concurrent-ops-per-connection

Description

Specifies the maximum number of internal operations that each HTTP client connection can execute concurrently. This property allow to limit the impact that each HTTP request can have on the whole server by limiting the number of internal operations that each HTTP request can execute concurrently. A value of 0 means that no limit is enforced.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest HTTP request message that will be allowed by the HTTP

Connection Handler. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The HTTP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take

effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the HTTP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the HTTP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the HTTP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the HTTP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the HTTP Connection Handler should use SSL. If enabled, the HTTP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the HTTP Connection Handler should use TCP keep-alive. If enabled, the

SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the HTTP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

JMX Connection Handler

Connection Handlers of type jmx-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully

qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Connection Handler implementation.

Default Value

org.opends.server.protocols.jmx.JmxConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this JMX Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the JMX Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address on which this JMX Connection Handler should listen for connections from JMX clients. If no value is provided, then the JMX Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the JMX Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

rmi-port

Description

Specifies the port number on which the JMX RMI service will listen for connections from clients. A value of 0 indicates the service to choose a port of its own. If the value provided is different than 0, the value will be used as the RMI port. Otherwise, the RMI service will choose a port of its own.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the JMX Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the JMX Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the JMX Connection Handler should use SSL. If enabled, the JMX Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

LDAP Connection Handler

Connection Handlers of type ldap-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-ldap-v2

Description

Indicates whether connections from LDAPv2 clients are allowed. If LDAPv2 clients are allowed, then only a minimal degree of special support are provided for them to ensure that LDAPv3-specific protocol elements (for example, Configuration Guide 25 controls, extended response messages, intermediate response messages, referrals) are not sent to an LDAPv2 client.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-start-tls

Description

Indicates whether clients are allowed to use StartTLS. If enabled, the LDAP Connection Handler allows clients to use the StartTLS extended operation to initiate secure communication over an otherwise insecure channel. Note that this is only allowed if the LDAP Connection Handler is not configured to use SSL, and if the server is configured with a valid key manager provider and a valid trust manager provider.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the LDAP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully

qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the LDAP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer LDAP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDAP Connection Handler implementation.

Default Value

org.opends.server.protocols.ldap.LDAPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the LDAP Connection Handler should keep statistics. If enabled, the LDAP Connection Handler maintains statistics about the number and types of operations requested over LDAP and the amount of data sent and received.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this LDAP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this LDAP Connection Handler should listen for connections from LDAP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the LDAP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the LDAP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to LDAP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest LDAP request message that will be allowed by this LDAP

Connection handler. This property is analogous to the maxBERSize configuration attribute of the Sun Java System Directory Server. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The LDAP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-rejection-notice

Description

Indicates whether the LDAP Connection Handler should send a notice of disconnection extended response message to the client if a new connection is rejected for some reason. The extended response message may provide an explanation indicating the reason that the connection was rejected.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the LDAP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to

retrieve both the public key and the private key. This is only applicable when the LDAP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the LDAP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or StartTLS

communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the LDAP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Connection Handler should use SSL. If enabled, the LDAP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the LDAP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the LDAP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

LDIF Connection Handler

Connection Handlers of type ldif-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDIF Connection Handler implementation.

Default Value

org.opends.server.protocols.LDIFConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-directory

Description

Specifies the path to the directory in which the LDIF files should be placed.

Default Value

config/auto-process-ldif

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

poll-interval

Description

Specifies how frequently the LDIF connection handler should check the LDIF directory to determine whether a new LDIF file has been added.

Default Value

5 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

SNMP Connection Handler

Connection Handlers of type snmp-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

allowed-manager

Description

Specifies the hosts of the managers to be granted the access rights. This property is required for SNMP v1 and v2 security configuration. An asterisk (*) opens access to all managers.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

allowed-user

Description

Specifies the users to be granted the access rights. This property is required for SNMP v3 security

configuration. An asterisk (*) opens access to all users.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

community

Description

Specifies the v1,v2 community or the v3 context name allowed to access the MIB 2605 monitoring information or the USM MIB. The mapping between "community" and "context name" is set.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SNMP Connection Handler implementation.

Default Value

org.opends.server.snmp.SNMPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this SNMP Connection Handler should listen for connections from SNMP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the SNMP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

Yes

listen-port

Description

Specifies the port number on which the SNMP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

opendmk-jarfile

Description

Indicates the OpenDMK runtime jar file location

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

registered-mbean

Description

Indicates whether the SNMP objects have to be registered in the directory server MBeanServer or not allowing to access SNMP Objects with RMI connector if enabled.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-agent-file

Description

Specifies the USM security configuration to receive authenticated only SNMP requests.

Default Value

config/snmp/security/opendj-snmp.security

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-level

Description

Specifies the type of security level : NoAuthNoPriv : No security mechanisms activated, AuthNoPriv : Authentication activated with no privacy, AuthPriv : Authentication with privacy activated. This property is required for SNMP V3 security configuration.

Default Value

authnopriv

Allowed Values

authnopriv

Authentication activated with no privacy.

authpriv

Authentication with privacy activated.

noauthnopriv

No security mechanisms activated.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trap-port

Description

Specifies the port to use to send SNMP Traps.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take

effect

Advanced Property

No

Read-only

No

traps-community

Description

Specifies the community string that must be included in the traps sent to define managers (trap-destinations). This property is used in the context of SNMP v1, v2 and v3.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-destination

Description

Specifies the hosts to which V1 traps will be sent. V1 Traps are sent to every host listed. If this list is empty, V1 traps are sent to "localhost". Each host in the list must be identifed by its name or complete IP Addess.

Default Value

If the list is empty, V1 traps are sent to "localhost".

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig list-debug-targets(1)

Name

dsconfig list-debug-targets - Lists existing Debug Targets

Synopsis

`dsconfig list-debug-targets` {options}

Description

Lists existing Debug Targets.

Options

The `dsconfig list-debug-targets` command takes the following options:

`--publisher-name {name}`

The name of the Debug Log Publisher.

Debug Target properties depend on the Debug Target type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default {name}: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

`--property {property}`

The name of a property to be displayed.

Debug Target properties depend on the Debug Target type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default {property}: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Debug Target properties depend on the Debug Target type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default {unit}: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Debug Target properties depend on the Debug Target type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default {unit}: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

Debug Target

Debug Targets of type debug-target have the following properties:

debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

debug-scope

Description

Specifies the fully-qualified OpenDJ Java package, class, or method affected by the settings in this target definition. Use the number character (#) to separate the class name and the method name (that is, org.opends.server.core.DirectoryServer#startUp).

Default Value

None

Allowed Values

The fully-qualified OpenDJ Java package, class, or method name.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the Debug Target is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

include-throwable-cause

Description

Specifies the property to indicate whether to include the cause of exceptions in exception thrown and caught messages.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-entry-arguments

Description

Specifies the property to indicate whether to include method arguments in debug messages.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-return-value

Description

Specifies the property to indicate whether to include the return value in debug messages.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

throwable-stack-frames

Description

Specifies the property to indicate the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

0

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-entry-caches(1)

Name

dsconfig list-entry-caches - Lists existing Entry Caches

Synopsis

`dsconfig list-entry-caches` {options}

Description

Lists existing Entry Caches.

Options

The `dsconfig list-entry-caches` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Entry Cache properties depend on the Entry Cache type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

`fifo-entry-cache`

Default {property}: FIFO Entry Cache

Enabled by default: true

See FIFO Entry Cache for the properties of this Entry Cache type.

`soft-reference-entry-cache`

Default {property}: Soft Reference Entry Cache

Enabled by default: true

See Soft Reference Entry Cache for the properties of this Entry Cache type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Entry Cache properties depend on the Entry Cache type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

`fifo-entry-cache`

Default {unit}: FIFO Entry Cache

Enabled by default: true

See FIFO Entry Cache for the properties of this Entry Cache type.

`soft-reference-entry-cache`

Default {unit}: Soft Reference Entry Cache

Enabled by default: true

See Soft Reference Entry Cache for the properties of this Entry Cache type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Entry Cache properties depend on the Entry Cache type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

`fifo-entry-cache`

Default {unit}: FIFO Entry Cache

Enabled by default: true

See FIFO Entry Cache for the properties of this Entry Cache type.

`soft-reference-entry-cache`

Default {unit}: Soft Reference Entry Cache

Enabled by default: true

See Soft Reference Entry Cache for the properties of this Entry Cache type.

FIFO Entry Cache

Entry Caches of type fifo-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the FIFO Entry Cache implementation.

Default Value

org.opends.server.extensions.FIFOEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time to wait while attempting to acquire a read or write lock.

Default Value

2000.0ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-entries

Description

Specifies the maximum number of entries that we will allow in the cache.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-memory-percent

Description

Specifies the maximum percentage of JVM memory used by the server before the entry caches stops caching and begins purging itself. Very low settings such as 10 or 20 (percent) can prevent this entry cache from having enough space to hold any of the entries to cache, making it appear that the server is ignoring or skipping the entry cache entirely.

Default Value

90

Allowed Values

An integer value. Lower value is 1. Upper value is 100.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Soft Reference Entry Cache

Entry Caches of type soft-reference-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Soft Reference Entry Cache implementation.

Default Value

org.opends.server.extensions.SoftReferenceEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time in milliseconds to wait while attempting to acquire a read or write lock.

Default Value

3000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-extended-operation-handlers(1)

Name

dsconfig list-extended-operation-handlers - Lists existing Extended Operation Handlers

Synopsis

`dsconfig list-extended-operation-handlers` {options}

Description

Lists existing Extended Operation Handlers.

Options

The `dsconfig list-extended-operation-handlers` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

`cancel-extended-operation-handler`

Default {property}: Cancel Extended Operation Handler

Enabled by default: true

See Cancel Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-connection-id-extended-operation-handler`

Default {property}: Get Connection Id Extended Operation Handler

Enabled by default: true

See Get Connection Id Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-symmetric-key-extended-operation-handler`

Default {property}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See Get Symmetric Key Extended Operation Handler for the properties of this Extended

Operation Handler type.

`password-modify-extended-operation-handler`

Default {property}: Password Modify Extended Operation Handler

Enabled by default: true

See Password Modify Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-policy-state-extended-operation-handler`

Default {property}: Password Policy State Extended Operation Handler

Enabled by default: true

See Password Policy State Extended Operation Handler for the properties of this Extended Operation Handler type.

`start-tls-extended-operation-handler`

Default {property}: Start TLS Extended Operation Handler

Enabled by default: true

See Start TLS Extended Operation Handler for the properties of this Extended Operation Handler type.

`who-am-i-extended-operation-handler`

Default {property}: Who Am I Extended Operation Handler

Enabled by default: true

See Who Am I Extended Operation Handler for the properties of this Extended Operation Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

`cancel-extended-operation-handler`

Default {unit}: Cancel Extended Operation Handler

Enabled by default: true

See Cancel Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-connection-id-extended-operation-handler`

Default {unit}: Get Connection Id Extended Operation Handler

Enabled by default: true

See Get Connection Id Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-symmetric-key-extended-operation-handler`

Default {unit}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See Get Symmetric Key Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-modify-extended-operation-handler`

Default {unit}: Password Modify Extended Operation Handler

Enabled by default: true

See Password Modify Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-policy-state-extended-operation-handler`

Default {unit}: Password Policy State Extended Operation Handler

Enabled by default: true

See Password Policy State Extended Operation Handler for the properties of this Extended Operation Handler type.

`start-tls-extended-operation-handler`

Default {unit}: Start TLS Extended Operation Handler

Enabled by default: true

See Start TLS Extended Operation Handler for the properties of this Extended Operation Handler type.

`who-am-i-extended-operation-handler`

Default {unit}: Who Am I Extended Operation Handler

Enabled by default: true

See Who Am I Extended Operation Handler for the properties of this Extended Operation Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

`cancel-extended-operation-handler`

Default {unit}: Cancel Extended Operation Handler

Enabled by default: true

See Cancel Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-connection-id-extended-operation-handler`

Default {unit}: Get Connection Id Extended Operation Handler

Enabled by default: true

See Get Connection Id Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-symmetric-key-extended-operation-handler`

Default {unit}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See Get Symmetric Key Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-modify-extended-operation-handler`

Default {unit}: Password Modify Extended Operation Handler

Enabled by default: true

See Password Modify Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-policy-state-extended-operation-handler`

Default {unit}: Password Policy State Extended Operation Handler

Enabled by default: true

See Password Policy State Extended Operation Handler for the properties of this Extended Operation Handler type.

`start-tls-extended-operation-handler`

Default {unit}: Start TLS Extended Operation Handler

Enabled by default: true

See Start TLS Extended Operation Handler for the properties of this Extended Operation

Handler type.

`who-am-i-extended-operation-handler`

Default {unit}: Who Am I Extended Operation Handler

Enabled by default: true

See Who Am I Extended Operation Handler for the properties of this Extended Operation Handler type.

Cancel Extended Operation Handler

Extended Operation Handlers of type cancel-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Cancel Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.CancelExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Get Connection Id Extended Operation Handler

Extended Operation Handlers of type get-connection-id-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Connection Id Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.GetConnectionIDExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Get Symmetric Key Extended Operation Handler

Extended Operation Handlers of type get-symmetric-key-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Symmetric Key Extended Operation Handler implementation.

Default Value

org.opends.server.crypto.GetSymmetricKeyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Modify Extended Operation Handler

Extended Operation Handlers of type password-modify-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that should be used in conjunction with the password modify extended operation. This property is used to identify a user based on an authorization ID in the 'u:' form. Changes to this property take effect immediately.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Password Modify Extended Operation Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Modify Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordModifyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Policy State Extended Operation Handler

Extended Operation Handlers of type password-policy-state-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Policy State Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordPolicyStateExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Start TLS Extended Operation Handler

Extended Operation Handlers of type start-tls-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Start TLS Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.StartTLSExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Who Am I Extended Operation Handler

Extended Operation Handlers of type who-am-i-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Who Am I Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.WhoAmIExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-group-implementations(1)

Name

dsconfig list-group-implementations - Lists existing Group Implementations

Synopsis

`dsconfig list-group-implementations` {options}

Description

Lists existing Group Implementations.

Options

The `dsconfig list-group-implementations` command takes the following options:

`--property {property}`
: The name of a property to be displayed.

  Group Implementation properties depend on the Group Implementation type, which depends on the {property} you provide.

  By default, OpenDJ directory server supports the following Group Implementation types:

  `dynamic-group-implementation`
  : Default {property}: Dynamic Group Implementation

    Enabled by default: true

    See Dynamic Group Implementation for the properties of this Group Implementation type.

  `static-group-implementation`
  : Default {property}: Static Group Implementation

    Enabled by default: true

    See Static Group Implementation for the properties of this Group Implementation type.

  `virtual-static-group-implementation`
  : Default {property}: Virtual Static Group Implementation

    Enabled by default: true

    See Virtual Static Group Implementation for the properties of this Group Implementation type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Group Implementation properties depend on the Group Implementation type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

`dynamic-group-implementation`

Default {unit}: Dynamic Group Implementation

Enabled by default: true

See Dynamic Group Implementation for the properties of this Group Implementation type.

`static-group-implementation`

Default {unit}: Static Group Implementation

Enabled by default: true

See Static Group Implementation for the properties of this Group Implementation type.

`virtual-static-group-implementation`

Default {unit}: Virtual Static Group Implementation

Enabled by default: true

See Virtual Static Group Implementation for the properties of this Group Implementation type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Group Implementation properties depend on the Group Implementation type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

`dynamic-group-implementation`

Default {unit}: Dynamic Group Implementation

Enabled by default: true

See Dynamic Group Implementation for the properties of this Group Implementation type.

`static-group-implementation`

Default {unit}: Static Group Implementation

Enabled by default: true

See Static Group Implementation for the properties of this Group Implementation type.

`virtual-static-group-implementation`

Default {unit}: Virtual Static Group Implementation

Enabled by default: true

See Virtual Static Group Implementation for the properties of this Group Implementation type.

Dynamic Group Implementation

Group Implementations of type dynamic-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Dynamic Group Implementation implementation.

Default Value

org.opends.server.extensions.DynamicGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Static Group Implementation

Group Implementations of type static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Group Implementation implementation.

Default Value

org.opends.server.extensions.StaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Virtual Static Group Implementation

Group Implementations of type virtual-static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Virtual Static Group Implementation implementation.

Default Value

org.opends.server.extensions.VirtualStaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-http-authorization-mechanisms(1)

Name

dsconfig list-http-authorization-mechanisms - Lists existing HTTP Authorization Mechanisms

Synopsis

`dsconfig list-http-authorization-mechanisms` {options}

Description

Lists existing HTTP Authorization Mechanisms.

Options

The `dsconfig list-http-authorization-mechanisms` command takes the following options:

`--property {property}`

The name of a property to be displayed.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

`http-anonymous-authorization-mechanism`

Default {property}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See HTTP Anonymous Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-basic-authorization-mechanism`

Default {property}: HTTP Basic Authorization Mechanism

Enabled by default: true

See HTTP Basic Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-cts-authorization-mechanism`

Default {property}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Cts Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-file-authorization-mechanism`

Default {property}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 File Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-openam-authorization-mechanism`

Default {property}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Openam Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-token-introspection-authorization-mechanism`

Default {property}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Token Introspection Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

`http-anonymous-authorization-mechanism`

Default {unit}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See HTTP Anonymous Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-basic-authorization-mechanism`

Default {unit}: HTTP Basic Authorization Mechanism

Enabled by default: true

See HTTP Basic Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-cts-authorization-mechanism`

Default {unit}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Cts Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-file-authorization-mechanism`

Default {unit}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 File Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-openam-authorization-mechanism`

Default {unit}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Openam Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-token-introspection-authorization-mechanism`

Default {unit}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Token Introspection Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

`http-anonymous-authorization-mechanism`

Default {unit}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See HTTP Anonymous Authorization Mechanism for the properties of this HTTP

Authorization Mechanism type.

`http-basic-authorization-mechanism`

Default {unit}: HTTP Basic Authorization Mechanism

Enabled by default: true

See HTTP Basic Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-cts-authorization-mechanism`

Default {unit}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Cts Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-file-authorization-mechanism`

Default {unit}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 File Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-openam-authorization-mechanism`

Default {unit}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Openam Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-token-introspection-authorization-mechanism`

Default {unit}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Token Introspection Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

HTTP Anonymous Authorization Mechanism

HTTP Authorization Mechanisms of type http-anonymous-authorization-mechanism have the following properties:

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Anonymous Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpAnonymousAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-dn

Description

The authorization DN which will be used for performing anonymous operations.

Default Value

By default, operations will be performed using an anonymously bound connection.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

HTTP Basic Authorization Mechanism

HTTP Authorization Mechanisms of type http-basic-authorization-mechanism have the following properties:

alt-authentication-enabled

Description

Specifies whether user credentials may be provided using alternative headers to the standard 'Authorize' header.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-password-header

Description

Alternate HTTP headers to get the user's password from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-username-header

Description

Alternate HTTP headers to get the user's name from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper used to get the user's entry corresponding to the user-id provided in the HTTP authentication header.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Basic Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Basic Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpBasicAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

HTTP Oauth2 Cts Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-cts-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

The base DN of the Core Token Service where access token are stored. (example: ou=famrecords,ou=openam-session,ou=tokens,dc=example,dc=com)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Cts Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2CtsAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

HTTP Oauth2 File Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-file-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-directory

Description

Directory containing token files. File names must be equal to the token strings. The file content must a JSON object with the following attributes: 'scope', 'expireTime' and all the field(s) needed to resolve the authzIdTemplate.

Default Value

oauth2-demo/

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 File Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2FileAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

HTTP Oauth2 Openam Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-openam-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Openam Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2OpenAmAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Openam Authorization Mechanism .

Default Value

By default the system key manager(s) will be used.

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-info-url

Description

Defines the OpenAM endpoint URL where the access-token resolution request should be sent.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

HTTP Oauth2 Token Introspection Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-token-introspection-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-id

Description

Client's ID to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-secret

Description

Client's secret to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Token Introspection Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2TokenIntrospectionAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Token Introspection Authorization Mechanism .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent requests to the

authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-introspection-url

Description

Defines the token introspection endpoint URL where the access-token resolution request should be sent. (example: http://example.com/introspect)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

dsconfig list-http-endpoints(1)

Name

dsconfig list-http-endpoints - Lists existing HTTP Endpoints

Synopsis

`dsconfig list-http-endpoints` {options}

Description

Lists existing HTTP Endpoints.

Options

The `dsconfig list-http-endpoints` command takes the following options:

`--property {property}`

The name of a property to be displayed.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

`admin-endpoint`

Default {property}: Admin Endpoint

Enabled by default: true

See Admin Endpoint for the properties of this HTTP Endpoint type.

`rest2ldap-endpoint`

Default {property}: Rest2ldap Endpoint

Enabled by default: true

See Rest2ldap Endpoint for the properties of this HTTP Endpoint type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

`admin-endpoint`

Default {unit}: Admin Endpoint

Enabled by default: true

See Admin Endpoint for the properties of this HTTP Endpoint type.

`rest2ldap-endpoint`

Default {unit}: Rest2ldap Endpoint

Enabled by default: true

See Rest2ldap Endpoint for the properties of this HTTP Endpoint type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

`admin-endpoint`

Default {unit}: Admin Endpoint

Enabled by default: true

See Admin Endpoint for the properties of this HTTP Endpoint type.

`rest2ldap-endpoint`

Default {unit}: Rest2ldap Endpoint

Enabled by default: true

See Rest2ldap Endpoint for the properties of this HTTP Endpoint type.

Admin Endpoint

HTTP Endpoints of type admin-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Admin Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.AdminEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Rest2ldap Endpoint

HTTP Endpoints of type rest2ldap-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

config-directory

Description

The directory containing the Rest2Ldap configuration file(s) for this specific endpoint. The directory must be readable by the server and may contain multiple configuration files, one for each supported version of the REST endpoint. If a relative path is used then it will be resolved against the server's instance directory.

Default Value

None

Allowed Values

A directory that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Rest2ldap Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.Rest2LdapEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-identity-mappers(1)

Name

dsconfig list-identity-mappers - Lists existing Identity Mappers

Synopsis

`dsconfig list-identity-mappers` {options}

Description

Lists existing Identity Mappers.

Options

The `dsconfig list-identity-mappers` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Identity Mapper properties depend on the Identity Mapper type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

`exact-match-identity-mapper`

Default {property}: Exact Match Identity Mapper

Enabled by default: true

See Exact Match Identity Mapper for the properties of this Identity Mapper type.

`regular-expression-identity-mapper`

Default {property}: Regular Expression Identity Mapper

Enabled by default: true

See Regular Expression Identity Mapper for the properties of this Identity Mapper type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Identity Mapper properties depend on the Identity Mapper type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

`exact-match-identity-mapper`

Default {unit}: Exact Match Identity Mapper

Enabled by default: true

See Exact Match Identity Mapper for the properties of this Identity Mapper type.

`regular-expression-identity-mapper`

Default {unit}: Regular Expression Identity Mapper

Enabled by default: true

See Regular Expression Identity Mapper for the properties of this Identity Mapper type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Identity Mapper properties depend on the Identity Mapper type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

`exact-match-identity-mapper`

Default {unit}: Exact Match Identity Mapper

Enabled by default: true

See Exact Match Identity Mapper for the properties of this Identity Mapper type.

`regular-expression-identity-mapper`

Default {unit}: Regular Expression Identity Mapper

Enabled by default: true

See Regular Expression Identity Mapper for the properties of this Identity Mapper type.

Exact Match Identity Mapper

Identity Mappers of type exact-match-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Exact Match Identity Mapper implementation.

Default Value

org.opends.server.extensions.ExactMatchIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the attribute whose value should exactly match the ID string provided to this identity mapper. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry. The internal search performed includes a logical OR across all of these values.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs will be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Regular Expression Identity Mapper

Identity Mappers of type regular-expression-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Regular Expression Identity Mapper implementation.

Default Value

org.opends.server.extensions.RegularExpressionIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name or OID of the attribute whose value should match the provided identifier string after it has been processed by the associated regular expression. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the base DN(s) that should be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all the specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

match-pattern

Description

Specifies the regular expression pattern that is used to identify portions of the ID string that will be replaced. Any portion of the ID string that matches this pattern is replaced in accordance with the provided replace pattern (or is removed if no replace pattern is specified). If multiple substrings within the given ID string match this pattern, all occurrences are replaced. If no part of the given ID string matches this pattern, the ID string is not altered. Exactly one match pattern value must be provided, and it must be a valid regular expression as described in the API documentation for the java.util.regex.Pattern class, including support for capturing groups.

Default Value

None

Allowed Values

Any valid regular expression pattern which is supported by the javax.util.regex.Pattern class (see http://download.oracle.com/docs/cd/E17409_01/javase/6/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 6).

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replace-pattern

Description

Specifies the replacement pattern that should be used for substrings in the ID string that match the provided regular expression pattern. If no replacement pattern is provided, then any matching portions of the ID string will be removed (i.e., replaced with an empty string). The replacement pattern may include a string from a capturing group by using a dollar sign ($) followed by an integer value that indicates which capturing group should be used.

Default Value

The replace pattern will be the empty string.

Allowed Values

Any valid replacement string that is allowed by the javax.util.regex.Matcher class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-key-manager-providers(1)

Name

dsconfig list-key-manager-providers - Lists existing Key Manager Providers

Synopsis

`dsconfig list-key-manager-providers` {options}

Description

Lists existing Key Manager Providers.

Options

The `dsconfig list-key-manager-providers` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

`file-based-key-manager-provider`

Default {property}: File Based Key Manager Provider

Enabled by default: true

See File Based Key Manager Provider for the properties of this Key Manager Provider type.

`ldap-key-manager-provider`

Default {property}: LDAP Key Manager Provider

Enabled by default: true

See LDAP Key Manager Provider for the properties of this Key Manager Provider type.

`pkcs11-key-manager-provider`

Default {property}: PKCS11 Key Manager Provider

Enabled by default: true

See PKCS11 Key Manager Provider for the properties of this Key Manager Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

`file-based-key-manager-provider`

Default {unit}: File Based Key Manager Provider

Enabled by default: true

See File Based Key Manager Provider for the properties of this Key Manager Provider type.

`ldap-key-manager-provider`

Default {unit}: LDAP Key Manager Provider

Enabled by default: true

See LDAP Key Manager Provider for the properties of this Key Manager Provider type.

`pkcs11-key-manager-provider`

Default {unit}: PKCS11 Key Manager Provider

Enabled by default: true

See PKCS11 Key Manager Provider for the properties of this Key Manager Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

`file-based-key-manager-provider`

Default {unit}: File Based Key Manager Provider

Enabled by default: true

See File Based Key Manager Provider for the properties of this Key Manager Provider type.

`ldap-key-manager-provider`

Default {unit}: LDAP Key Manager Provider

Enabled by default: true

See LDAP Key Manager Provider for the properties of this Key Manager Provider type.

`pkcs11-key-manager-provider`

Default {unit}: PKCS11 Key Manager Provider

Enabled by default: true

See PKCS11 Key Manager Provider for the properties of this Key Manager Provider type.

File Based Key Manager Provider

Key Manager Providers of type file-based-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Key Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager

Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well. If no value is provided, the JVM-default value is used. Changes to this configuration attribute will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

LDAP Key Manager Provider

Key Manager Providers of type ldap-key-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Key Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

PKCS11 Key Manager Provider

Key Manager Providers of type pkcs11-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Key Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11KeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access

the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig list-log-publishers(1)

Name

dsconfig list-log-publishers - Lists existing Log Publishers

Synopsis

`dsconfig list-log-publishers` {options}

Description

Lists existing Log Publishers.

Options

The `dsconfig list-log-publishers` command takes the following options:

`--property {property}`
: The name of a property to be displayed.

  Log Publisher properties depend on the Log Publisher type, which depends on the {property} you provide.

  By default, OpenDJ directory server supports the following Log Publisher types:

  `csv-file-access-log-publisher`
  : Default {property}: Csv File Access Log Publisher

    Enabled by default: true

    See Csv File Access Log Publisher for the properties of this Log Publisher type.

  `csv-file-http-access-log-publisher`
  : Default {property}: Csv File HTTP Access Log Publisher

    Enabled by default: true

    See Csv File HTTP Access Log Publisher for the properties of this Log Publisher type.

  `external-access-log-publisher`
  : Default {property}: External Access Log Publisher

    Enabled by default: true

    See External Access Log Publisher for the properties of this Log Publisher type.

`external-http-access-log-publisher`

Default {property}: External HTTP Access Log Publisher

Enabled by default: true

See External HTTP Access Log Publisher for the properties of this Log Publisher type.

`file-based-access-log-publisher`

Default {property}: File Based Access Log Publisher

Enabled by default: true

See File Based Access Log Publisher for the properties of this Log Publisher type.

`file-based-audit-log-publisher`

Default {property}: File Based Audit Log Publisher

Enabled by default: true

See File Based Audit Log Publisher for the properties of this Log Publisher type.

`file-based-debug-log-publisher`

Default {property}: File Based Debug Log Publisher

Enabled by default: true

See File Based Debug Log Publisher for the properties of this Log Publisher type.

`file-based-error-log-publisher`

Default {property}: File Based Error Log Publisher

Enabled by default: true

See File Based Error Log Publisher for the properties of this Log Publisher type.

`file-based-http-access-log-publisher`

Default {property}: File Based HTTP Access Log Publisher

Enabled by default: true

See File Based HTTP Access Log Publisher for the properties of this Log Publisher type.

`json-file-access-log-publisher`

Default {property}: Json File Access Log Publisher

Enabled by default: true

See Json File Access Log Publisher for the properties of this Log Publisher type.

`json-file-http-access-log-publisher`

Default {property}: Json File HTTP Access Log Publisher

Enabled by default: true

See Json File HTTP Access Log Publisher for the properties of this Log Publisher type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Log Publisher properties depend on the Log Publisher type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

`csv-file-access-log-publisher`

Default {unit}: Csv File Access Log Publisher

Enabled by default: true

See Csv File Access Log Publisher for the properties of this Log Publisher type.

`csv-file-http-access-log-publisher`

Default {unit}: Csv File HTTP Access Log Publisher

Enabled by default: true

See Csv File HTTP Access Log Publisher for the properties of this Log Publisher type.

`external-access-log-publisher`

Default {unit}: External Access Log Publisher

Enabled by default: true

See External Access Log Publisher for the properties of this Log Publisher type.

`external-http-access-log-publisher`

Default {unit}: External HTTP Access Log Publisher

Enabled by default: true

See External HTTP Access Log Publisher for the properties of this Log Publisher type.

`file-based-access-log-publisher`

Default {unit}: File Based Access Log Publisher

Enabled by default: true

See File Based Access Log Publisher for the properties of this Log Publisher type.

`file-based-audit-log-publisher`

Default {unit}: File Based Audit Log Publisher

Enabled by default: true

See File Based Audit Log Publisher for the properties of this Log Publisher type.

`file-based-debug-log-publisher`

Default {unit}: File Based Debug Log Publisher

Enabled by default: true

See File Based Debug Log Publisher for the properties of this Log Publisher type.

`file-based-error-log-publisher`

Default {unit}: File Based Error Log Publisher

Enabled by default: true

See File Based Error Log Publisher for the properties of this Log Publisher type.

`file-based-http-access-log-publisher`

Default {unit}: File Based HTTP Access Log Publisher

Enabled by default: true

See File Based HTTP Access Log Publisher for the properties of this Log Publisher type.

`json-file-access-log-publisher`

Default {unit}: Json File Access Log Publisher

Enabled by default: true

See Json File Access Log Publisher for the properties of this Log Publisher type.

`json-file-http-access-log-publisher`

Default {unit}: Json File HTTP Access Log Publisher

Enabled by default: true

See Json File HTTP Access Log Publisher for the properties of this Log Publisher type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Log Publisher properties depend on the Log Publisher type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

`csv-file-access-log-publisher`

Default {unit}: Csv File Access Log Publisher

Enabled by default: true

See Csv File Access Log Publisher for the properties of this Log Publisher type.

`csv-file-http-access-log-publisher`

Default {unit}: Csv File HTTP Access Log Publisher

Enabled by default: true

See Csv File HTTP Access Log Publisher for the properties of this Log Publisher type.

`external-access-log-publisher`

Default {unit}: External Access Log Publisher

Enabled by default: true

See External Access Log Publisher for the properties of this Log Publisher type.

`external-http-access-log-publisher`

Default {unit}: External HTTP Access Log Publisher

Enabled by default: true

See External HTTP Access Log Publisher for the properties of this Log Publisher type.

`file-based-access-log-publisher`

Default {unit}: File Based Access Log Publisher

Enabled by default: true

See File Based Access Log Publisher for the properties of this Log Publisher type.

`file-based-audit-log-publisher`

Default {unit}: File Based Audit Log Publisher

Enabled by default: true

See File Based Audit Log Publisher for the properties of this Log Publisher type.

`file-based-debug-log-publisher`

Default {unit}: File Based Debug Log Publisher

Enabled by default: true

See File Based Debug Log Publisher for the properties of this Log Publisher type.

`file-based-error-log-publisher`

Default {unit}: File Based Error Log Publisher

Enabled by default: true

See File Based Error Log Publisher for the properties of this Log Publisher type.

`file-based-http-access-log-publisher`

Default {unit}: File Based HTTP Access Log Publisher

Enabled by default: true

See File Based HTTP Access Log Publisher for the properties of this Log Publisher type.

`json-file-access-log-publisher`

Default {unit}: Json File Access Log Publisher

Enabled by default: true

See Json File Access Log Publisher for the properties of this Log Publisher type.

`json-file-http-access-log-publisher`

Default {unit}: Json File HTTP Access Log Publisher

Enabled by default: true

See Json File HTTP Access Log Publisher for the properties of this Log Publisher type.

Csv File Access Log Publisher

Log Publishers of type csv-file-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writting in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CsvFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Csv File Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when the tamper-evident option is enabled.

Default Value

3s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Csv File HTTP Access Log Publisher

Log Publishers of type csv-file-http-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File HTTP Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Csv File HTTP Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when secure option is enabled.

Default Value

3s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a

significative impact on performance of the server.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

External Access Log Publisher

Log Publishers of type external-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External Access Log Publisher implementation.

Default Value

org.opends.server.loggers.ExternalAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

External HTTP Access Log Publisher

Log Publishers of type external-http-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External HTTP Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Access Log Publisher

Log Publishers of type file-based-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the access log.

Default Value

multi-line

Allowed Values

combined

Combine log records for operation requests and responses into a single record. This format should be used when log records are to be filtered based on response criteria (e.g. result code).

multi-line

Outputs separate log records for operation requests and responses.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Audit Log Publisher

Log Publishers of type file-based-audit-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Audit Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Audit Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAuditLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Audit Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Audit Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Audit Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Audit Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Debug Log Publisher

Log Publishers of type file-based-debug-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Debug Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-include-throwable-cause

Description

Indicates whether to include the cause of exceptions in exception thrown and caught messages logged by default.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-entry-arguments

Description

Indicates whether to include method arguments in debug messages logged by default.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-return-value

Description

Indicates whether to include the return value in debug messages logged by default.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-throwable-stack-frames

Description

Indicates the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Debug Log Publisher implementation.

Default Value

org.opends.server.loggers.TextDebugLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Debug Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Debug Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Debug Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Debug Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Error Log Publisher

Log Publishers of type file-based-error-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Error Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer will be flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-severity

Description

Specifies the default severity levels for the logger.

Default Value

error warning

Allowed Values

all

Messages of all severity levels are logged.

debug

The error log severity that is used for messages that provide debugging information triggered during processing.

error

The error log severity that is used for messages that provide information about errors which may force the server to shut down or operate in a significantly degraded state.

info

The error log severity that is used for messages that provide information about significant events within the server that are not warnings or errors.

none

No messages of any severity are logged by default. This value is intended to be used in conjunction with the override-severity property to define an error logger that will publish no error message beside the errors of a given category.

notice

The error log severity that is used for the most important informational messages (i.e., information that should almost always be logged but is not associated with a warning or error condition).

warning

The error log severity that is used for messages that provide information about warnings triggered during processing.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Error Log Publisher implementation.

Default Value

org.opends.server.loggers.TextErrorLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Error Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Error Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

override-severity

Description

Specifies the override severity levels for the logger based on the category of the messages. Each override severity level should include the category and the severity levels to log for that category, for example, core=error,info,warning. Valid categories are: core, extensions, protocol, config, log, util, schema, plugin, jeb, backend, tools, task, access-control, admin, sync, version, quicksetup, admin-tool, dsconfig, user-defined. Valid severities are: all, error, info, warning, notice, debug.

Default Value

All messages with the default severity levels are logged.

Allowed Values

A string in the form category=severity1,severity2...

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Error Log Publisher . When multiple policies are used, log files will be cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files will never be cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Error Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based HTTP Access Log Publisher

Log Publishers of type file-based-http-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based HTTP Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based HTTP Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the HTTP access log.

Default Value

cs-host c-ip cs-username x-datetime cs-method cs-uri-stem cs-uri-query cs-version sc-status cs(User-Agent) x-connection-id x-etime x-transaction-id

Allowed Values

A space separated list of fields describing the extended log format to be used for logging HTTP accesses. Available values are listed on the W3C working draft http://www.w3.org/TR/WD-logfile.html and Microsoft website http://www.microsoft.com/technet/prodtechnol/

WindowsServer2003/Library/IIS/676400bc-8969-4aa7-851a-9319490a9bbb.mspx?mfr=true
OpenDJ supports the following standard fields: "c-ip", "c-port", "cs-host", "cs-method", "cs-uri", "cs-uri-stem", "cs-uri-query", "cs(User-Agent)", "cs-username", "cs-version", "s-computername", "s-ip", "s-port", "sc-status". OpenDJ supports the following application specific field extensions: "x-connection-id" displays the internal connection ID assigned to the HTTP client connection, "x-datetime" displays the completion date and time for the logged HTTP request and its ouput is controlled by the "ds-cfg-log-record-time-format" property, "x-etime" displays the total execution time for the logged HTTP request, "x-transaction-id" displays the transaction id associated to a request

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Json File Access Log Publisher

Log Publishers of type json-file-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.JsonFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Json File HTTP Access Log Publisher

Log Publishers of type json-file-http-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-log-retention-policies(1)

Name

dsconfig list-log-retention-policies - Lists existing Log Retention Policies

Synopsis

`dsconfig list-log-retention-policies` {options}

Description

Lists existing Log Retention Policies.

Options

The `dsconfig list-log-retention-policies` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

`file-count-log-retention-policy`

Default {property}: File Count Log Retention Policy

Enabled by default: false

See File Count Log Retention Policy for the properties of this Log Retention Policy type.

`free-disk-space-log-retention-policy`

Default {property}: Free Disk Space Log Retention Policy

Enabled by default: false

See Free Disk Space Log Retention Policy for the properties of this Log Retention Policy type.

`size-limit-log-retention-policy`

Default {property}: Size Limit Log Retention Policy

Enabled by default: false

See Size Limit Log Retention Policy for the properties of this Log Retention Policy type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

`file-count-log-retention-policy`

Default {unit}: File Count Log Retention Policy

Enabled by default: false

See File Count Log Retention Policy for the properties of this Log Retention Policy type.

`free-disk-space-log-retention-policy`

Default {unit}: Free Disk Space Log Retention Policy

Enabled by default: false

See Free Disk Space Log Retention Policy for the properties of this Log Retention Policy type.

`size-limit-log-retention-policy`

Default {unit}: Size Limit Log Retention Policy

Enabled by default: false

See Size Limit Log Retention Policy for the properties of this Log Retention Policy type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

`file-count-log-retention-policy`

Default {unit}: File Count Log Retention Policy

Enabled by default: false

See File Count Log Retention Policy for the properties of this Log Retention Policy type.

`free-disk-space-log-retention-policy`

Default {unit}: Free Disk Space Log Retention Policy

Enabled by default: false

See Free Disk Space Log Retention Policy for the properties of this Log Retention Policy type.

`size-limit-log-retention-policy`

Default {unit}: Size Limit Log Retention Policy

Enabled by default: false

See Size Limit Log Retention Policy for the properties of this Log Retention Policy type.

File Count Log Retention Policy

Log Retention Policies of type file-count-log-retention-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the File Count Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FileNumberRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

number-of-files

Description

Specifies the number of archived log files to retain before the oldest ones are cleaned.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Free Disk Space Log Retention Policy

Log Retention Policies of type free-disk-space-log-retention-policy have the following properties:

free-disk-space

Description

Specifies the minimum amount of free disk space that should be available on the file system on which the archived log files are stored.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Free Disk Space Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FreeDiskSpaceRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Size Limit Log Retention Policy

Log Retention Policies of type size-limit-log-retention-policy have the following properties:

disk-space-used

Description

Specifies the maximum total disk space used by the log files.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Retention Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-log-rotation-policies(1)

Name

dsconfig list-log-rotation-policies - Lists existing Log Rotation Policies

Synopsis

`dsconfig list-log-rotation-policies` {options}

Description

Lists existing Log Rotation Policies.

Options

The `dsconfig list-log-rotation-policies` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

`fixed-time-log-rotation-policy`

Default {property}: Fixed Time Log Rotation Policy

Enabled by default: false

See Fixed Time Log Rotation Policy for the properties of this Log Rotation Policy type.

`size-limit-log-rotation-policy`

Default {property}: Size Limit Log Rotation Policy

Enabled by default: false

See Size Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`time-limit-log-rotation-policy`

Default {property}: Time Limit Log Rotation Policy

Enabled by default: false

See Time Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

`fixed-time-log-rotation-policy`

Default {unit}: Fixed Time Log Rotation Policy

Enabled by default: false

See Fixed Time Log Rotation Policy for the properties of this Log Rotation Policy type.

`size-limit-log-rotation-policy`

Default {unit}: Size Limit Log Rotation Policy

Enabled by default: false

See Size Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`time-limit-log-rotation-policy`

Default {unit}: Time Limit Log Rotation Policy

Enabled by default: false

See Time Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

`fixed-time-log-rotation-policy`

Default {unit}: Fixed Time Log Rotation Policy

Enabled by default: false

See Fixed Time Log Rotation Policy for the properties of this Log Rotation Policy type.

`size-limit-log-rotation-policy`

Default {unit}: Size Limit Log Rotation Policy

Enabled by default: false

See Size Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`time-limit-log-rotation-policy`

Default {unit}: Time Limit Log Rotation Policy

Enabled by default: false

See Time Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

Fixed Time Log Rotation Policy

Log Rotation Policies of type fixed-time-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fixed Time Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.FixedTimeRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-of-day

Description

Specifies the time of day at which log rotation should occur.

Default Value

None

Allowed Values

24 hour time of day in HHmm format.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Size Limit Log Rotation Policy

Log Rotation Policies of type size-limit-log-rotation-policy have the following properties:

file-size-limit

Description

Specifies the maximum size that a log file can reach before it is rotated.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Time Limit Log Rotation Policy

Log Rotation Policies of type time-limit-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Time Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.TimeLimitRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

rotation-interval

Description

Specifies the time interval between rotations.

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-monitor-providers(1)

Name

dsconfig list-monitor-providers - Lists existing Monitor Providers

Synopsis

`dsconfig list-monitor-providers` {options}

Description

Lists existing Monitor Providers.

Options

The `dsconfig list-monitor-providers` command takes the following options:

`--property {property}`
: The name of a property to be displayed.

  Monitor Provider properties depend on the Monitor Provider type, which depends on the {property} you provide.

  By default, OpenDJ directory server supports the following Monitor Provider types:

  `client-connection-monitor-provider`
  : Default {property}: Client Connection Monitor Provider

    Enabled by default: true

    See Client Connection Monitor Provider for the properties of this Monitor Provider type.

  `entry-cache-monitor-provider`
  : Default {property}: Entry Cache Monitor Provider

    Enabled by default: true

    See Entry Cache Monitor Provider for the properties of this Monitor Provider type.

  `memory-usage-monitor-provider`
  : Default {property}: Memory Usage Monitor Provider

    Enabled by default: true

    See Memory Usage Monitor Provider for the properties of this Monitor Provider type.

`stack-trace-monitor-provider`

Default {property}: Stack Trace Monitor Provider

Enabled by default: true

See Stack Trace Monitor Provider for the properties of this Monitor Provider type.

`system-info-monitor-provider`

Default {property}: System Info Monitor Provider

Enabled by default: true

See System Info Monitor Provider for the properties of this Monitor Provider type.

`version-monitor-provider`

Default {property}: Version Monitor Provider

Enabled by default: true

See Version Monitor Provider for the properties of this Monitor Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Monitor Provider properties depend on the Monitor Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

`client-connection-monitor-provider`

Default {unit}: Client Connection Monitor Provider

Enabled by default: true

See Client Connection Monitor Provider for the properties of this Monitor Provider type.

`entry-cache-monitor-provider`

Default {unit}: Entry Cache Monitor Provider

Enabled by default: true

See Entry Cache Monitor Provider for the properties of this Monitor Provider type.

`memory-usage-monitor-provider`

Default {unit}: Memory Usage Monitor Provider

Enabled by default: true

See Memory Usage Monitor Provider for the properties of this Monitor Provider type.

`stack-trace-monitor-provider`

Default {unit}: Stack Trace Monitor Provider

Enabled by default: true

See Stack Trace Monitor Provider for the properties of this Monitor Provider type.

`system-info-monitor-provider`

Default {unit}: System Info Monitor Provider

Enabled by default: true

See System Info Monitor Provider for the properties of this Monitor Provider type.

`version-monitor-provider`

Default {unit}: Version Monitor Provider

Enabled by default: true

See Version Monitor Provider for the properties of this Monitor Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Monitor Provider properties depend on the Monitor Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

`client-connection-monitor-provider`

Default {unit}: Client Connection Monitor Provider

Enabled by default: true

See Client Connection Monitor Provider for the properties of this Monitor Provider type.

`entry-cache-monitor-provider`

Default {unit}: Entry Cache Monitor Provider

Enabled by default: true

See Entry Cache Monitor Provider for the properties of this Monitor Provider type.

`memory-usage-monitor-provider`

Default {unit}: Memory Usage Monitor Provider

Enabled by default: true

See Memory Usage Monitor Provider for the properties of this Monitor Provider type.

`stack-trace-monitor-provider`

Default {unit}: Stack Trace Monitor Provider

Enabled by default: true

See Stack Trace Monitor Provider for the properties of this Monitor Provider type.

`system-info-monitor-provider`

Default {unit}: System Info Monitor Provider

Enabled by default: true

See System Info Monitor Provider for the properties of this Monitor Provider type.

`version-monitor-provider`

Default {unit}: Version Monitor Provider

Enabled by default: true

See Version Monitor Provider for the properties of this Monitor Provider type.

Client Connection Monitor Provider

Monitor Providers of type client-connection-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Client Connection Monitor Provider implementation.

Default Value

org.opends.server.monitors.ClientConnectionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Entry Cache Monitor Provider

Monitor Providers of type entry-cache-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Entry Cache Monitor Provider implementation.

Default Value

org.opends.server.monitors.EntryCacheMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Memory Usage Monitor Provider

Monitor Providers of type memory-usage-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Memory Usage Monitor Provider implementation.

Default Value

org.opends.server.monitors.MemoryUsageMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Stack Trace Monitor Provider

Monitor Providers of type stack-trace-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Stack Trace Monitor Provider implementation.

Default Value

org.opends.server.monitors.StackTraceMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

System Info Monitor Provider

Monitor Providers of type system-info-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the System Info Monitor Provider implementation.

Default Value

org.opends.server.monitors.SystemInfoMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Version Monitor Provider

Monitor Providers of type version-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Version Monitor Provider implementation.

Default Value

org.opends.server.monitors.VersionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-password-generators(1)

Name

dsconfig list-password-generators - Lists existing Password Generators

Synopsis

`dsconfig list-password-generators` {options}

Description

Lists existing Password Generators.

Options

The `dsconfig list-password-generators` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Password Generator properties depend on the Password Generator type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

`random-password-generator`

Default {property}: Random Password Generator

Enabled by default: true

See Random Password Generator for the properties of this Password Generator type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Password Generator properties depend on the Password Generator type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

`random-password-generator`

Default {unit}: Random Password Generator

Enabled by default: true

See Random Password Generator for the properties of this Password Generator type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Password Generator properties depend on the Password Generator type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

`random-password-generator`

Default {unit}: Random Password Generator

Enabled by default: true

See Random Password Generator for the properties of this Password Generator type.

Random Password Generator

Password Generators of type random-password-generator have the following properties:

enabled

Description

Indicates whether the Password Generator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Random Password Generator implementation.

Default Value

org.opends.server.extensions.RandomPasswordGenerator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordGenerator

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

password-character-set

Description

Specifies one or more named character sets. This is a multi-valued property, with each value defining a different character set. The format of the character set is the name of the set followed by a colon and the characters that are in that set. For example, the value "alpha:abcdefghijklmnopqrstuvwxyz" defines a character set named "alpha" containing all of the lower-case ASCII alphabetic characters.

Default Value

None

Allowed Values

A character set name (consisting of ASCII letters) followed by a colon and the set of characters that are included in that character set.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-format

Description

Specifies the format to use for the generated password. The value is a comma-delimited list of elements in which each of those elements is comprised of the name of a character set defined in the password-character-set property, a colon, and the number of characters to include from that set. For example, a value of "alpha:3,numeric:2,alpha:3" generates an 8-character password in which the first three characters are from the "alpha" set, the next two are from the "numeric" set, and the final three are from the "alpha" set.

Default Value

None

Allowed Values

A comma-delimited list whose elements comprise a valid character set name, a colon, and a positive integer indicating the number of characters from that set to be included.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-password-policies(1)

Name

dsconfig list-password-policies - Lists existing Password Policies

Synopsis

`dsconfig list-password-policies` {options}

Description

Lists existing Password Policies.

Options

The `dsconfig list-password-policies` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Authentication Policy properties depend on the Authentication Policy type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

`ldap-pass-through-authentication-policy`

Default {property}: LDAP Pass Through Authentication Policy

Enabled by default: false

See LDAP Pass Through Authentication Policy for the properties of this Authentication Policy type.

`password-policy`

Default {property}: Password Policy

Enabled by default: false

See Password Policy for the properties of this Authentication Policy type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Authentication Policy properties depend on the Authentication Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

`ldap-pass-through-authentication-policy`

Default {unit}: LDAP Pass Through Authentication Policy

Enabled by default: false

See LDAP Pass Through Authentication Policy for the properties of this Authentication Policy type.

`password-policy`

Default {unit}: Password Policy

Enabled by default: false

See Password Policy for the properties of this Authentication Policy type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Authentication Policy properties depend on the Authentication Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

`ldap-pass-through-authentication-policy`

Default {unit}: LDAP Pass Through Authentication Policy

Enabled by default: false

See LDAP Pass Through Authentication Policy for the properties of this Authentication Policy type.

`password-policy`

Default {unit}: Password Policy

Enabled by default: false

See Password Policy for the properties of this Authentication Policy type.

LDAP Pass Through Authentication Policy

Authentication Policies of type ldap-pass-through-authentication-policy have the following properties:

cached-password-storage-scheme

Description

Specifies the name of a password storage scheme which should be used for encoding cached

passwords. Changing the password storage scheme will cause all existing cached passwords to be discarded.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cached-password-ttl

Description

Specifies the maximum length of time that a locally cached password may be used for authentication before it is refreshed from the remote LDAP service. This property represents a cache timeout. Increasing the timeout period decreases the frequency that bind operations are delegated to the remote LDAP service, but increases the risk of users authenticating using stale passwords. Note that authentication attempts which fail because the provided password does not match the locally cached password will always be retried against the remote LDAP service.

Default Value

8 hours

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-timeout

Description

Specifies the timeout used when connecting to remote LDAP directory servers, performing SSL negotiation, and for individual search and bind requests. If the timeout expires then the current operation will be aborted and retried against another LDAP server if one is available.

Default Value

3 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the LDAP Pass Through Authentication Policy implementation.

Default Value

org.opends.server.extensions.LDAPPassThroughAuthenticationPolicyFactory

Allowed Values

A Java class that implements or extends the class(es):

org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

mapped-attribute

Description

Specifies one or more attributes in the user's entry whose value(s) will determine the bind DN used when authenticating to the remote LDAP directory service. This property is mandatory when using the "mapped-bind" or "mapped-search" mapping policies. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. At least one of the named attributes must exist in a user's local entry in order for authentication to proceed. When multiple attributes or values are found in the user's entry then the behavior is determined by the mapping policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-base-dn

Description

Specifies the set of base DNs below which to search for users in the remote LDAP directory service. This property is mandatory when using the "mapped-search" mapping policy. If multiple values are given, searches are performed below all specified base DNs.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-dn

Description

Specifies the bind DN which should be used to perform user searches in the remote LDAP directory service.

Default Value

Searches will be performed anonymously.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password

Description

Specifies the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-environment-variable

Description

Specifies the name of an environment variable containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-file

Description

Specifies the name of a file containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-property

Description

Specifies the name of a Java property containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-filter-template

Description

If defined, overrides the filter used when searching for the user, substituting %s with the value of the local entry's "mapped-attribute". The filter-template may include ZERO or ONE %s substitutions. If multiple mapped-attributes are configured, multiple renditions of this template will be aggregated into one larger filter using an OR (|) operator. An example use-case for this property would be to use a different attribute type on the mapped search. For example, mapped-attribute could be set to "uid" and filter-template to "(samAccountName=%s)". You can also use the filter to restrict search results. For example: "(&(uid=%s)(objectclass=student))"

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapping-policy

Description

Specifies the mapping algorithm for obtaining the bind DN from the user's entry.

Default Value

unmapped

Allowed Values

mapped-bind

Bind to the remote LDAP directory service using a DN obtained from an attribute in the user’s entry. This policy will check each attribute named in the "mapped-attribute" property. If more than one attribute or value is present then the first one will be used.

mapped-search

Bind to the remote LDAP directory service using the DN of an entry obtained using a search against the remote LDAP directory service. The search filter will comprise of an equality matching filter whose attribute type is the "mapped-attribute" property, and whose assertion value is the attribute value obtained from the user’s entry. If more than one attribute or value is present then the filter will be composed of multiple equality filters combined using a logical OR (union).

unmapped

Bind to the remote LDAP directory service using the DN of the user’s entry in this directory server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

primary-remote-ldap-server

Description

Specifies the primary list of remote LDAP servers which should be used for pass through authentication. If more than one LDAP server is specified then operations may be distributed across them. If all of the primary LDAP servers are unavailable then operations will fail-over to the set of secondary LDAP servers, if defined.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-remote-ldap-server

Description

Specifies the secondary list of remote LDAP servers which should be used for pass through authentication in the event that the primary LDAP servers are unavailable. If more than one LDAP server is specified then operations may be distributed across them. Operations will be rerouted to the primary LDAP servers as soon as they are determined to be available.

Default Value

No secondary LDAP servers.

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols which are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections

with remote LDAP directory servers.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

use-password-caching

Description

Indicates whether passwords should be cached locally within the user's entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Pass Through Authentication Policy should use SSL. If enabled, the LDAP Pass Through Authentication Policy will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether LDAP connections should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether LDAP connections should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Policy

Authentication Policies of type password-policy have the following properties:

account-status-notification-handler

Description

Specifies the names of the account status notification handlers that are used with the associated password storage scheme.

Default Value

None

Allowed Values

The DN of any Account Status Notification Handler. The referenced account status notification handlers must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-expired-password-changes

Description

Indicates whether a user whose password is expired is still allowed to change that password using the password modify extended operation.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-multiple-password-values

Description

Indicates whether user entries can have multiple distinct values for the password attribute. This is potentially dangerous because many mechanisms used to change the password do not work well with such a configuration. If multiple password values are allowed, then any of them can be used to authenticate, and they are all subject to the same policy constraints.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-pre-encoded-passwords

Description

Indicates whether users can change their passwords by providing a pre-encoded value. This can cause a security risk because the clear-text version of the password is not known and therefore validation checks cannot be applied to it.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-user-password-changes

Description

Indicates whether users can change their own passwords. This check is made in addition to access control evaluation. Both must allow the password change for it to occur.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-password-storage-scheme

Description

Specifies the names of the password storage schemes that are used to encode clear-text passwords for this password policy.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

deprecated-password-storage-scheme

Description

Specifies the names of the password storage schemes that are considered deprecated for this password policy. If a user with this password policy authenticates to the server and his/her password is encoded with a deprecated scheme, those values are removed and replaced with values encoded using the default password storage scheme(s).

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

expire-passwords-without-warning

Description

Indicates whether the directory server allows a user's password to expire even if that user has never seen an expiration warning notification. If this property is true, accounts always expire when the expiration time arrives. If this property is false or disabled, the user always receives at least one warning notification, and the password expiration is set to the warning time plus the warning interval.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-add

Description

Indicates whether users are forced to change their passwords upon first authenticating to the directory server after their account has been created.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-reset

Description

Indicates whether users are forced to change their passwords if they are reset by an administrator. For this purpose, anyone with permission to change a given user's password other than that user is considered an administrator.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

grace-login-count

Description

Specifies the number of grace logins that a user is allowed after the account has expired to allow that user to choose a new password. A value of 0 indicates that no grace logins are allowed.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

idle-lockout-interval

Description

Specifies the maximum length of time that an account may remain idle (that is, the associated user does not authenticate to the server) before that user is locked out. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that idle accounts are not automatically locked out. This feature is available only if the last login time is maintained.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the Password Policy implementation.

Default Value

org.opends.server.core.PasswordPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

last-login-time-attribute

Description

Specifies the name or OID of the attribute type that is used to hold the last login time for users with the associated password policy. This attribute type must be defined in the directory server schema and must either be defined as an operational attribute or must be allowed by the set of objectClasses for all users with the associated password policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

last-login-time-format

Description

Specifies the format string that is used to generate the last login time value for users with the associated password policy. This format string conforms to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-duration

Description

Specifies the length of time that an account is locked after too many authentication failures. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the account must remain locked until an administrator resets the password.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-count

Description

Specifies the maximum number of authentication failures that a user is allowed before the account is locked out. A value of 0 indicates that accounts are never locked out due to failed attempts.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-expiration-interval

Description

Specifies the length of time before an authentication failure is no longer counted against a user for the purposes of account lockout. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the authentication failures must never expire. The failure count is always cleared upon a successful authentication.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-age

Description

Specifies the maximum length of time that a user can continue using the same password before it must be changed (that is, the password expiration interval). The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables password expiration.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-reset-age

Description

Specifies the maximum length of time that users have to change passwords after they have been reset by an administrator before they become locked. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables this feature.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-age

Description

Specifies the minimum length of time after a password change before the user is allowed to change the password again. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. This setting can be used to prevent users from changing their passwords repeatedly over a short period of time to flush an old password from the history so that it can be re-used.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-attribute

Description

Specifies the attribute type used to hold user passwords. This attribute type must be defined in the server schema, and it must have either the user password or auth password syntax.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-change-requires-current-password

Description

Indicates whether user password changes must use the password modify extended operation and must include the user's current password before the change is allowed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-expiration-warning-interval

Description

Specifies the maximum length of time before a user's password actually expires that the server begins to include warning notifications in bind responses for that user. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables the warning interval.

Default Value

5 days

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-generator

Description

Specifies the name of the password generator that is used with the associated password policy. This is used in conjunction with the password modify extended operation to generate a new password for a user when none was provided in the request.

Default Value

None

Allowed Values

The DN of any Password Generator. The referenced password generator must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-count

Description

Specifies the maximum number of former passwords to maintain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero indicates that either no password history is to be maintained (if the password history duration has a value of zero seconds), or that there is no maximum number of passwords to maintain in the history (if the password history duration has a value greater than zero seconds).

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-duration

Description

Specifies the maximum length of time that passwords remain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero seconds indicates that either no password history is to be maintained (if the password history count has a value of zero), or that there is no maximum duration for passwords in the history (if the password history count has a value greater than zero).

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-validator

Description

Specifies the names of the password validators that are used with the associated password storage scheme. The password validators are invoked when a user attempts to provide a new password, to determine whether the new password is acceptable.

Default Value

None

Allowed Values

The DN of any Password Validator. The referenced password validators must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

previous-last-login-time-format

Description

Specifies the format string(s) that might have been used with the last login time at any point in the past for users associated with the password policy. These values are used to make it possible

to parse previous values, but are not used to set new values. The format strings conform to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-change-by-time

Description

Specifies the time by which all users with the associated password policy must change their passwords. The value is expressed in a generalized time format. If this time is equal to the current time or is in the past, then all users are required to change their passwords immediately. The behavior of the server in this mode is identical to the behavior observed when users are forced to change their passwords after an administrative reset.

Default Value

None

Allowed Values

A valid timestamp in generalized time form (for example, a value of "20070409185811Z" indicates a value of April 9, 2007 at 6:58:11 pm GMT).

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-authentication

Description

Indicates whether users with the associated password policy are required to authenticate in a secure manner. This might mean either using a secure communication channel between the client and the server, or using a SASL mechanism that does not expose the credentials.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-password-changes

Description

Indicates whether users with the associated password policy are required to change their password in a secure manner that does not expose the credentials.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

skip-validation-for-administrators

Description

Indicates whether passwords set by administrators are allowed to bypass the password validation process that is required for user password changes.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

state-update-failure-policy

Description

Specifies how the server deals with the inability to update password policy state information during an authentication attempt. In particular, this property can be used to control whether an otherwise successful bind operation fails if a failure occurs while attempting to update password policy state information (for example, to clear a record of previous authentication failures or to update the last login time). It can also be used to control whether to reject a bind request if it is known ahead of time that it will not be possible to update the authentication failure times in the

event of an unsuccessful bind attempt (for example, if the backend writability mode is disabled).

Default Value

reactive

Allowed Values

ignore

If a bind attempt would otherwise be successful, then do not reject it if a problem occurs while attempting to update the password policy state information for the user.

proactive

Proactively reject any bind attempt if it is known ahead of time that it would not be possible to update the user's password policy state information.

reactive

Even if a bind attempt would otherwise be successful, reject it if a problem occurs while attempting to update the password policy state information for the user.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-password-storage-schemes(1)

Name

dsconfig list-password-storage-schemes - Lists existing Password Storage Schemes

Synopsis

`dsconfig list-password-storage-schemes` {options}

Description

Lists existing Password Storage Schemes.

Options

The `dsconfig list-password-storage-schemes` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

`aes-password-storage-scheme`

Default {property}: AES Password Storage Scheme

Enabled by default: true

See AES Password Storage Scheme for the properties of this Password Storage Scheme type.

`base64-password-storage-scheme`

Default {property}: Base64 Password Storage Scheme

Enabled by default: true

See Base64 Password Storage Scheme for the properties of this Password Storage Scheme type.

`bcrypt-password-storage-scheme`

Default {property}: Bcrypt Password Storage Scheme

Enabled by default: true

See Bcrypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`blowfish-password-storage-scheme`

Default {property}: Blowfish Password Storage Scheme

Enabled by default: true

See Blowfish Password Storage Scheme for the properties of this Password Storage Scheme type.

`clear-password-storage-scheme`

Default {property}: Clear Password Storage Scheme

Enabled by default: true

See Clear Password Storage Scheme for the properties of this Password Storage Scheme type.

`crypt-password-storage-scheme`

Default {property}: Crypt Password Storage Scheme

Enabled by default: true

See Crypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`md5-password-storage-scheme`

Default {property}: MD5 Password Storage Scheme

Enabled by default: true

See MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha256-password-storage-scheme`

Default {property}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha512-password-storage-scheme`

Default {property}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pkcs5s2-password-storage-scheme`

Default {property}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See PKCS5S2 Password Storage Scheme for the properties of this Password Storage Scheme

type.

`rc4-password-storage-scheme`

Default {property}: RC4 Password Storage Scheme

Enabled by default: true

See RC4 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-md5-password-storage-scheme`

Default {property}: Salted MD5 Password Storage Scheme

Enabled by default: true

See Salted MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha1-password-storage-scheme`

Default {property}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See Salted SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha256-password-storage-scheme`

Default {property}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See Salted SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha384-password-storage-scheme`

Default {property}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See Salted SHA384 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha512-password-storage-scheme`

Default {property}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See Salted SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`sha1-password-storage-scheme`

Default {property}: SHA1 Password Storage Scheme

Enabled by default: true

See SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`triple-des-password-storage-scheme`

Default {property}: Triple DES Password Storage Scheme

Enabled by default: true

See Triple DES Password Storage Scheme for the properties of this Password Storage Scheme type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

`aes-password-storage-scheme`

Default {unit}: AES Password Storage Scheme

Enabled by default: true

See AES Password Storage Scheme for the properties of this Password Storage Scheme type.

`base64-password-storage-scheme`

Default {unit}: Base64 Password Storage Scheme

Enabled by default: true

See Base64 Password Storage Scheme for the properties of this Password Storage Scheme type.

`bcrypt-password-storage-scheme`

Default {unit}: Bcrypt Password Storage Scheme

Enabled by default: true

See Bcrypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`blowfish-password-storage-scheme`

Default {unit}: Blowfish Password Storage Scheme

Enabled by default: true

See Blowfish Password Storage Scheme for the properties of this Password Storage Scheme type.

`clear-password-storage-scheme`

Default {unit}: Clear Password Storage Scheme

Enabled by default: true

See Clear Password Storage Scheme for the properties of this Password Storage Scheme type.

`crypt-password-storage-scheme`

Default {unit}: Crypt Password Storage Scheme

Enabled by default: true

See Crypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`md5-password-storage-scheme`

Default {unit}: MD5 Password Storage Scheme

Enabled by default: true

See MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha256-password-storage-scheme`

Default {unit}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha512-password-storage-scheme`

Default {unit}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pkcs5s2-password-storage-scheme`

Default {unit}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See PKCS5S2 Password Storage Scheme for the properties of this Password Storage Scheme type.

`rc4-password-storage-scheme`

Default {unit}: RC4 Password Storage Scheme

Enabled by default: true

See RC4 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-md5-password-storage-scheme`

Default {unit}: Salted MD5 Password Storage Scheme

Enabled by default: true

See Salted MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha1-password-storage-scheme`

Default {unit}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See Salted SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha256-password-storage-scheme`

Default {unit}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See Salted SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha384-password-storage-scheme`

Default {unit}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See Salted SHA384 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha512-password-storage-scheme`

Default {unit}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See Salted SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`sha1-password-storage-scheme`

Default {unit}: SHA1 Password Storage Scheme

Enabled by default: true

See SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`triple-des-password-storage-scheme`

Default {unit}: Triple DES Password Storage Scheme

Enabled by default: true

See Triple DES Password Storage Scheme for the properties of this Password Storage Scheme type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

`aes-password-storage-scheme`

Default {unit}: AES Password Storage Scheme

Enabled by default: true

See AES Password Storage Scheme for the properties of this Password Storage Scheme type.

`base64-password-storage-scheme`

Default {unit}: Base64 Password Storage Scheme

Enabled by default: true

See Base64 Password Storage Scheme for the properties of this Password Storage Scheme type.

`bcrypt-password-storage-scheme`

Default {unit}: Bcrypt Password Storage Scheme

Enabled by default: true

See Bcrypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`blowfish-password-storage-scheme`

Default {unit}: Blowfish Password Storage Scheme

Enabled by default: true

See Blowfish Password Storage Scheme for the properties of this Password Storage Scheme type.

`clear-password-storage-scheme`

Default {unit}: Clear Password Storage Scheme

Enabled by default: true

See Clear Password Storage Scheme for the properties of this Password Storage Scheme type.

`crypt-password-storage-scheme`

Default {unit}: Crypt Password Storage Scheme

Enabled by default: true

See Crypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`md5-password-storage-scheme`

Default {unit}: MD5 Password Storage Scheme

Enabled by default: true

See MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha256-password-storage-scheme`

Default {unit}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha512-password-storage-scheme`

Default {unit}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pkcs5s2-password-storage-scheme`

Default {unit}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See PKCS5S2 Password Storage Scheme for the properties of this Password Storage Scheme type.

`rc4-password-storage-scheme`

Default {unit}: RC4 Password Storage Scheme

Enabled by default: true

See RC4 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-md5-password-storage-scheme`

Default {unit}: Salted MD5 Password Storage Scheme

Enabled by default: true

See Salted MD5 Password Storage Scheme for the properties of this Password Storage Scheme

type.

`salted-sha1-password-storage-scheme`

Default {unit}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See Salted SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha256-password-storage-scheme`

Default {unit}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See Salted SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha384-password-storage-scheme`

Default {unit}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See Salted SHA384 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha512-password-storage-scheme`

Default {unit}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See Salted SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`sha1-password-storage-scheme`

Default {unit}: SHA1 Password Storage Scheme

Enabled by default: true

See SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`triple-des-password-storage-scheme`

Default {unit}: Triple DES Password Storage Scheme

Enabled by default: true

See Triple DES Password Storage Scheme for the properties of this Password Storage Scheme type.

AES Password Storage Scheme

Password Storage Schemes of type aes-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the AES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.AESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Base64 Password Storage Scheme

Password Storage Schemes of type base64-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Base64 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.Base64PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Bcrypt Password Storage Scheme

Password Storage Schemes of type bcrypt-password-storage-scheme have the following properties:

bcrypt-cost

Description

The cost parameter specifies a key expansion iteration count as a power of two. A default value of 12 (2^12 iterations) is considered in 2016 as a reasonable balance between responsiveness and security for regular users.

Default Value

12

Allowed Values

An integer value. Lower value is 1. Upper value is 30.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Bcrypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BcryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Blowfish Password Storage Scheme

Password Storage Schemes of type blowfish-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Blowfish Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BlowfishPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Clear Password Storage Scheme

Password Storage Schemes of type clear-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Clear Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.ClearPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Crypt Password Storage Scheme

Password Storage Schemes of type crypt-password-storage-scheme have the following properties:

crypt-password-storage-encryption-algorithm

Description

Specifies the algorithm to use to encrypt new passwords. Select the crypt algorithm to use to encrypt new passwords. The value can either be "unix", which means the password is encrypted with the weak Unix crypt algorithm, or "md5" which means the password is encrypted with the BSD MD5 algorithm and has a 1 prefix, or "sha256" which means the password is encrypted with the SHA256 algorithm and has a 5 prefix, or "sha512" which means the password is encrypted with the SHA512 algorithm and has a 6 prefix.

Default Value

unix

Allowed Values

md5

New passwords are encrypted with the BSD MD5 algorithm.

sha256

New passwords are encrypted with the Unix crypt SHA256 algorithm.

sha512

New passwords are encrypted with the Unix crypt SHA512 algorithm.

unix

New passwords are encrypted with the Unix crypt algorithm. Passwords are truncated at 8 characters and the top bit of each character is ignored.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Crypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.CryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

MD5 Password Storage Scheme

Password Storage Schemes of type md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.MD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

PBKDF2 Hmac SHA256 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

PBKDF2 Hmac SHA512 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

PKCS5S2 Password Storage Scheme

Password Storage Schemes of type pkcs5s2-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PKCS5S2 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PKCS5S2PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

RC4 Password Storage Scheme

Password Storage Schemes of type rc4-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the RC4 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.RC4PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted MD5 Password Storage Scheme

Password Storage Schemes of type salted-md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedMD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA1 Password Storage Scheme

Password Storage Schemes of type salted-sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA256 Password Storage Scheme

Password Storage Schemes of type salted-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA384 Password Storage Scheme

Password Storage Schemes of type salted-sha384-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA384 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA384PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA512 Password Storage Scheme

Password Storage Schemes of type salted-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

SHA1 Password Storage Scheme

Password Storage Schemes of type sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Triple DES Password Storage Scheme

Password Storage Schemes of type triple-des-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Triple DES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.TripleDESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-password-validators(1)

Name

dsconfig list-password-validators - Lists existing Password Validators

Synopsis

`dsconfig list-password-validators` {options}

Description

Lists existing Password Validators.

Options

The `dsconfig list-password-validators` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Password Validator properties depend on the Password Validator type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

`attribute-value-password-validator`

Default {property}: Attribute Value Password Validator

Enabled by default: true

See Attribute Value Password Validator for the properties of this Password Validator type.

`character-set-password-validator`

Default {property}: Character Set Password Validator

Enabled by default: true

See Character Set Password Validator for the properties of this Password Validator type.

`dictionary-password-validator`

Default {property}: Dictionary Password Validator

Enabled by default: true

See Dictionary Password Validator for the properties of this Password Validator type.

`length-based-password-validator`

Default {property}: Length Based Password Validator

Enabled by default: true

See Length Based Password Validator for the properties of this Password Validator type.

`repeated-characters-password-validator`

Default {property}: Repeated Characters Password Validator

Enabled by default: true

See Repeated Characters Password Validator for the properties of this Password Validator type.

`similarity-based-password-validator`

Default {property}: Similarity Based Password Validator

Enabled by default: true

See Similarity Based Password Validator for the properties of this Password Validator type.

`unique-characters-password-validator`

Default {property}: Unique Characters Password Validator

Enabled by default: true

See Unique Characters Password Validator for the properties of this Password Validator type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Password Validator properties depend on the Password Validator type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

`attribute-value-password-validator`

Default {unit}: Attribute Value Password Validator

Enabled by default: true

See Attribute Value Password Validator for the properties of this Password Validator type.

`character-set-password-validator`

Default {unit}: Character Set Password Validator

Enabled by default: true

See Character Set Password Validator for the properties of this Password Validator type.

`dictionary-password-validator`

Default {unit}: Dictionary Password Validator

Enabled by default: true

See Dictionary Password Validator for the properties of this Password Validator type.

`length-based-password-validator`

Default {unit}: Length Based Password Validator

Enabled by default: true

See Length Based Password Validator for the properties of this Password Validator type.

`repeated-characters-password-validator`

Default {unit}: Repeated Characters Password Validator

Enabled by default: true

See Repeated Characters Password Validator for the properties of this Password Validator type.

`similarity-based-password-validator`

Default {unit}: Similarity Based Password Validator

Enabled by default: true

See Similarity Based Password Validator for the properties of this Password Validator type.

`unique-characters-password-validator`

Default {unit}: Unique Characters Password Validator

Enabled by default: true

See Unique Characters Password Validator for the properties of this Password Validator type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Password Validator properties depend on the Password Validator type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

`attribute-value-password-validator`

Default {unit}: Attribute Value Password Validator

Enabled by default: true

See Attribute Value Password Validator for the properties of this Password Validator type.

`character-set-password-validator`

Default {unit}: Character Set Password Validator

Enabled by default: true

See Character Set Password Validator for the properties of this Password Validator type.

`dictionary-password-validator`

Default {unit}: Dictionary Password Validator

Enabled by default: true

See Dictionary Password Validator for the properties of this Password Validator type.

`length-based-password-validator`

Default {unit}: Length Based Password Validator

Enabled by default: true

See Length Based Password Validator for the properties of this Password Validator type.

`repeated-characters-password-validator`

Default {unit}: Repeated Characters Password Validator

Enabled by default: true

See Repeated Characters Password Validator for the properties of this Password Validator type.

`similarity-based-password-validator`

Default {unit}: Similarity Based Password Validator

Enabled by default: true

See Similarity Based Password Validator for the properties of this Password Validator type.

`unique-characters-password-validator`

Default {unit}: Unique Characters Password Validator

Enabled by default: true

See Unique Characters Password Validator for the properties of this Password Validator type.

Attribute Value Password Validator

Password Validators of type attribute-value-password-validator have the following properties:

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against attribute values. If "false" then only match the entire password against attribute values otherwise ("true") check whether the password contains attribute values.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.AttributeValuePasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name(s) of the attribute(s) whose values should be checked to determine whether they match the provided password. If no values are provided, then the server checks if the proposed password matches the value of any attribute in the user's entry.

Default Value

All attributes in the user entry will be checked.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator should test the reversed value of the provided password as well as the order in which it was given.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Character Set Password Validator

Password Validators of type character-set-password-validator have the following properties:

allow-unclassified-characters

Description

Indicates whether this password validator allows passwords to contain characters outside of any of the user-defined character sets and ranges. If this is "false", then only those characters in the user-defined character sets and ranges may be used in passwords. Any password containing a character not included in any character set or range will be rejected.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set

Description

Specifies a character set containing characters that a password may contain and a value indicating the minimum number of characters required from that set. Each value must be an integer (indicating the minimum required characters from the set which may be zero, indicating that the character set is optional) followed by a colon and the characters to include in that set (for example, "3:abcdefghijklmnopqrstuvwxyz" indicates that a user password must contain at least three characters from the set of lowercase ASCII letters). Multiple character sets can be defined in separate values, although no character can appear in more than one character set.

Default Value

If no sets are specified, the validator only uses the defined character ranges.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set-ranges

Description

Specifies a character range containing characters that a password may contain and a value indicating the minimum number of characters required from that range. Each value must be an integer (indicating the minimum required characters from the range which may be zero, indicating that the character range is optional) followed by a colon and one or more range specifications. A range specification is 3 characters: the first character allowed, a minus, and the last character allowed. For example, "3:A-Za-z0-9". The ranges in each value should not overlap, and the characters in each range specification should be ordered.

Default Value

If no ranges are specified, the validator only uses the defined character sets.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.CharacterSetPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-character-sets

Description

Specifies the minimum number of character sets and ranges that a password must contain. This property should only be used in conjunction with optional character sets and ranges (those requiring zero characters). Its value must include any mandatory character sets and ranges (those requiring greater than zero characters). This is useful in situations where a password must contain characters from mandatory character sets and ranges, and characters from at least N optional character sets and ranges. For example, it is quite common to require that a password contains at least one non-alphanumeric character as well as characters from two alphanumeric character sets (lower-case, upper-case, digits). In this case, this property should be set to 3.

Default Value

The password must contain characters from each of the mandatory character sets and ranges and, if there are optional character sets and ranges, at least one character from one of the optional character sets and ranges.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Dictionary Password Validator

Password Validators of type dictionary-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator is to treat password characters in a case-sensitive manner. If it is set to true, then the validator rejects a password only if it appears in the dictionary with exactly the same capitalization as provided by the user.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against dictionary words. If "false" then only match the entire password against words otherwise ("true") check whether the password contains words.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dictionary-file

Description

Specifies the path to the file containing a list of words that cannot be used as passwords. It should be formatted with one word per line. The value can be an absolute path or a path that is relative to the OpenDJ instance root.

Default Value

For Unix and Linux systems: config/wordlist.txt. For Windows systems: config\wordlist.txt

Allowed Values

The path to any text file contained on the system that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.DictionaryPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator is to test the reversed value of the provided password as well as the order in which it was given. For example, if the user provides a new password of "password" and this configuration attribute is set to true, then the value "drowssap" is also tested against attribute values in the user's entry.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Length Based Password Validator

Password Validators of type length-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.LengthBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-password-length

Description

Specifies the maximum number of characters that can be included in a proposed password. A value of zero indicates that there will be no upper bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-length

Description

Specifies the minimum number of characters that must be included in a proposed password. A value of zero indicates that there will be no lower bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

6

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Repeated Characters Password Validator

Password Validators of type repeated-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. If the value of this property is false, the validator ignores any differences in capitalization when looking for consecutive characters in the password. If the value is true, the validator considers a character to be repeating only if all consecutive occurrences use the same capitalization.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.RepeatedCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-consecutive-length

Description

Specifies the maximum number of times that any character can appear consecutively in a password value. A value of zero indicates that no maximum limit is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Similarity Based Password Validator

Password Validators of type similarity-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.SimilarityBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-password-difference

Description

Specifies the minimum difference of new and old password. A value of zero indicates that no difference between passwords is acceptable.

Default Value

None

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Unique Characters Password Validator

Password Validators of type unique-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. A value of true indicates that the validator does not consider a capital letter to be the

same as its lower-case counterpart. A value of false indicates that the validator ignores differences in capitalization when looking at the number of unique characters in the password.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.UniqueCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-unique-characters

Description

Specifies the minimum number of unique characters that a password will be allowed to contain. A value of zero indicates that no minimum value is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-plugins(1)

Name

dsconfig list-plugins - Lists existing Plugins

Synopsis

`dsconfig list-plugins` {options}

Description

Lists existing Plugins.

Options

The `dsconfig list-plugins` command takes the following options:

`--property {property}`
: The name of a property to be displayed.

  Plugin properties depend on the Plugin type, which depends on the {property} you provide.

  By default, OpenDJ directory server supports the following Plugin types:

  `attribute-cleanup-plugin`
  : Default {property}: Attribute Cleanup Plugin

    Enabled by default: true

    See Attribute Cleanup Plugin for the properties of this Plugin type.

  `change-number-control-plugin`
  : Default {property}: Change Number Control Plugin

    Enabled by default: true

    See Change Number Control Plugin for the properties of this Plugin type.

  `entry-uuid-plugin`
  : Default {property}: Entry UUID Plugin

    Enabled by default: true

    See Entry UUID Plugin for the properties of this Plugin type.

  `fractional-ldif-import-plugin`
  : Default {property}: Fractional LDIF Import Plugin

Enabled by default: true

See Fractional LDIF Import Plugin for the properties of this Plugin type.

`last-mod-plugin`

Default {property}: Last Mod Plugin

Enabled by default: true

See Last Mod Plugin for the properties of this Plugin type.

`ldap-attribute-description-list-plugin`

Default {property}: LDAP Attribute Description List Plugin

Enabled by default: true

See LDAP Attribute Description List Plugin for the properties of this Plugin type.

`password-policy-import-plugin`

Default {property}: Password Policy Import Plugin

Enabled by default: true

See Password Policy Import Plugin for the properties of this Plugin type.

`profiler-plugin`

Default {property}: Profiler Plugin

Enabled by default: true

See Profiler Plugin for the properties of this Plugin type.

`referential-integrity-plugin`

Default {property}: Referential Integrity Plugin

Enabled by default: true

See Referential Integrity Plugin for the properties of this Plugin type.

`samba-password-plugin`

Default {property}: Samba Password Plugin

Enabled by default: true

See Samba Password Plugin for the properties of this Plugin type.

`seven-bit-clean-plugin`

Default {property}: Seven Bit Clean Plugin

Enabled by default: true

See Seven Bit Clean Plugin for the properties of this Plugin type.

`unique-attribute-plugin`

Default {property}: Unique Attribute Plugin

Enabled by default: true

See Unique Attribute Plugin for the properties of this Plugin type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Plugin properties depend on the Plugin type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Plugin types:

`attribute-cleanup-plugin`

Default {unit}: Attribute Cleanup Plugin

Enabled by default: true

See Attribute Cleanup Plugin for the properties of this Plugin type.

`change-number-control-plugin`

Default {unit}: Change Number Control Plugin

Enabled by default: true

See Change Number Control Plugin for the properties of this Plugin type.

`entry-uuid-plugin`

Default {unit}: Entry UUID Plugin

Enabled by default: true

See Entry UUID Plugin for the properties of this Plugin type.

`fractional-ldif-import-plugin`

Default {unit}: Fractional LDIF Import Plugin

Enabled by default: true

See Fractional LDIF Import Plugin for the properties of this Plugin type.

`last-mod-plugin`

Default {unit}: Last Mod Plugin

Enabled by default: true

See Last Mod Plugin for the properties of this Plugin type.

`ldap-attribute-description-list-plugin`

Default {unit}: LDAP Attribute Description List Plugin

Enabled by default: true

See LDAP Attribute Description List Plugin for the properties of this Plugin type.

`password-policy-import-plugin`

Default {unit}: Password Policy Import Plugin

Enabled by default: true

See Password Policy Import Plugin for the properties of this Plugin type.

`profiler-plugin`

Default {unit}: Profiler Plugin

Enabled by default: true

See Profiler Plugin for the properties of this Plugin type.

`referential-integrity-plugin`

Default {unit}: Referential Integrity Plugin

Enabled by default: true

See Referential Integrity Plugin for the properties of this Plugin type.

`samba-password-plugin`

Default {unit}: Samba Password Plugin

Enabled by default: true

See Samba Password Plugin for the properties of this Plugin type.

`seven-bit-clean-plugin`

Default {unit}: Seven Bit Clean Plugin

Enabled by default: true

See Seven Bit Clean Plugin for the properties of this Plugin type.

`unique-attribute-plugin`

Default {unit}: Unique Attribute Plugin

Enabled by default: true

See Unique Attribute Plugin for the properties of this Plugin type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w

(milliseconds, seconds, minutes, hours, days, or weeks).

Plugin properties depend on the Plugin type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Plugin types:

`attribute-cleanup-plugin`
: Default {unit}: Attribute Cleanup Plugin

  Enabled by default: true

  See Attribute Cleanup Plugin for the properties of this Plugin type.

`change-number-control-plugin`
: Default {unit}: Change Number Control Plugin

  Enabled by default: true

  See Change Number Control Plugin for the properties of this Plugin type.

`entry-uuid-plugin`
: Default {unit}: Entry UUID Plugin

  Enabled by default: true

  See Entry UUID Plugin for the properties of this Plugin type.

`fractional-ldif-import-plugin`
: Default {unit}: Fractional LDIF Import Plugin

  Enabled by default: true

  See Fractional LDIF Import Plugin for the properties of this Plugin type.

`last-mod-plugin`
: Default {unit}: Last Mod Plugin

  Enabled by default: true

  See Last Mod Plugin for the properties of this Plugin type.

`ldap-attribute-description-list-plugin`
: Default {unit}: LDAP Attribute Description List Plugin

  Enabled by default: true

  See LDAP Attribute Description List Plugin for the properties of this Plugin type.

`password-policy-import-plugin`
: Default {unit}: Password Policy Import Plugin

  Enabled by default: true

See Password Policy Import Plugin for the properties of this Plugin type.

`profiler-plugin`

Default {unit}: Profiler Plugin

Enabled by default: true

See Profiler Plugin for the properties of this Plugin type.

`referential-integrity-plugin`

Default {unit}: Referential Integrity Plugin

Enabled by default: true

See Referential Integrity Plugin for the properties of this Plugin type.

`samba-password-plugin`

Default {unit}: Samba Password Plugin

Enabled by default: true

See Samba Password Plugin for the properties of this Plugin type.

`seven-bit-clean-plugin`

Default {unit}: Seven Bit Clean Plugin

Enabled by default: true

See Seven Bit Clean Plugin for the properties of this Plugin type.

`unique-attribute-plugin`

Default {unit}: Unique Attribute Plugin

Enabled by default: true

See Unique Attribute Plugin for the properties of this Plugin type.

Attribute Cleanup Plugin

Plugins of type attribute-cleanup-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.AttributeCleanupPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparseadd preparsemodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

remove-inbound-attributes

Description

A list of attributes which should be removed from incoming add or modify requests.

Default Value

No attributes will be removed

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rename-inbound-attributes

Description

A list of attributes which should be renamed in incoming add or modify requests.

Default Value

No attributes will be renamed

Allowed Values

An attribute name mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Change Number Control Plugin

Plugins of type change-number-control-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ChangeNumberControlPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postOperationAdd postOperationDelete postOperationModify postOperationModifyDN

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Entry UUID Plugin

Plugins of type entry-uuid-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.EntryUUIDPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport preoperationadd

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the

client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Fractional LDIF Import Plugin

Plugins of type fractional-ldif-import-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

None

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

None

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

Last Mod Plugin

Plugins of type last-mod-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LastModPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd preoperationmodify preoperationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

LDAP Attribute Description List Plugin

Plugins of type ldap-attribute-description-list-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LDAPADListPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparsesearch

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Policy Import Plugin

Plugins of type password-policy-import-plugin have the following properties:

default-auth-password-storage-scheme

Description

Specifies the names of password storage schemes that to be used for encoding passwords contained in attributes with the auth password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy should be used to govern them.

Default Value

If the default password policy uses an attribute with the auth password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes auth password values using the "SHA1" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import plug-in is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-user-password-storage-scheme

Description

Specifies the names of the password storage schemes to be used for encoding passwords contained in attributes with the user password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy is to be used to govern them.

Default Value

If the default password policy uses the attribute with the user password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes user password values using the "SSHA" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import Plugin is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.PasswordPolicyImportPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Profiler Plugin

Plugins of type profiler-plugin have the following properties:

enable-profiling-on-startup

Description

Indicates whether the profiler plug-in is to start collecting data automatically when the directory server is started. This property is read only when the server is started, and any changes take effect on the next restart. This property is typically set to "false" unless startup profiling is required, because otherwise the volume of data that can be collected can cause the server to run out of memory if it is not turned off in a timely manner.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.profiler.ProfilerPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

startup

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

profile-action

Description

Specifies the action that should be taken by the profiler. A value of "start" causes the profiler thread to start collecting data if it is not already active. A value of "stop" causes the profiler thread to stop collecting data and write it to disk, and a value of "cancel" causes the profiler thread to stop collecting data and discard anything that has been captured. These operations occur immediately.

Default Value

none

Allowed Values

cancel

Stop collecting profile data and discard what has been captured.

none

Do not take any action.

start

Start collecting profile data.

stop

Stop collecting profile data and write what has been captured to a file in the profile directory.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-directory

Description

Specifies the path to the directory where profile information is to be written. This path may be either an absolute path or a path that is relative to the root of the OpenDJ directory server instance. The directory must exist and the directory server must have permission to create new files in it.

Default Value

None

Allowed Values

The path to any directory that exists on the filesystem and that can be read and written by the server user.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-sample-interval

Description

Specifies the sample interval in milliseconds to be used when capturing profiling information in the server. When capturing data, the profiler thread sleeps for this length of time between calls to obtain traces for all threads running in the JVM.

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

NoneChanges to this configuration attribute take effect the next time the profiler is started.

Advanced Property

No

Read-only

No

Referential Integrity Plugin

Plugins of type referential-integrity-plugin have the following properties:

attribute-type

Description

Specifies the attribute types for which referential integrity is to be maintained. At least one attribute type must be specified, and the syntax of any attributes must be either a distinguished name (1.3.6.1.4.1.1466.115.121.1.12) or name and optional UID (1.3.6.1.4.1.1466.115.121.1.34).

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN that limits the scope within which referential integrity is maintained.

Default Value

Referential integrity is maintained in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references

Description

Specifies whether reference attributes must refer to existing entries. When this property is set to true, this plugin will ensure that any new references added as part of an add or modify operation point to existing entries, and that the referenced entries match the filter criteria for the referencing attribute, if specified.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-filter-criteria

Description

Specifies additional filter criteria which will be enforced when checking references. If a reference attribute has filter criteria defined then this plugin will ensure that any new references added as part of an add or modify operation refer to an existing entry which matches the specified filter.

Default Value

None

Allowed Values

An attribute-filter mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-scope-criteria

Description

Specifies whether referenced entries must reside within the same naming context as the entry containing the reference. The reference scope will only be enforced when reference checking is enabled.

Default Value

global

Allowed Values

global

References may refer to existing entries located anywhere in the Directory.

naming-context

References must refer to existing entries located within the same naming context.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ReferentialIntegrityPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

Specifies the log file location where the update records are written when the plug-in is in background-mode processing. The default location is the logs directory of the server instance, using the file name "referint".

Default Value

logs/referint

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postoperationdelete postoperationmodifydn subordinatemodifydn subordinatedelete preoperationadd preoperationmodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

update-interval

Description

Specifies the interval in seconds when referential integrity updates are made. If this value is 0, then the updates are made synchronously in the foreground.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Samba Password Plugin

Plugins of type samba-password-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SambaPasswordPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationmodify postoperationextended

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pwd-sync-policy

Description

Specifies which Samba passwords should be kept synchronized.

Default Value

sync-nt-password

Allowed Values

sync-lm-password

Synchronize the LanMan password attribute "sambaLMPassword"

sync-nt-password

Synchronize the NT password attribute "sambaNTPassword"

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

samba-administrator-dn

Description

Specifies the distinguished name of the user which Samba uses to perform Password Modify extended operations against this directory server in order to synchronize the userPassword attribute after the LanMan or NT passwords have been updated. The user must have the 'password-reset' privilege and should not be a root user. This user name can be used in order to identify Samba connections and avoid double re-synchronization of the same password. If this property is left undefined, then no password updates will be skipped.

Default Value

Synchronize all updates to user passwords

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Seven Bit Clean Plugin

Plugins of type seven-bit-clean-plugin have the following properties:

attribute-type

Description

Specifies the name or OID of an attribute type for which values should be checked to ensure that they are 7-bit clean.

Default Value

uid mail userPassword

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN below which the checking is performed. Any attempt to update a value for one of the configured attributes below this base DN must be 7-bit clean for the operation to be allowed.

Default Value

All entries below all public naming contexts will be checked.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SevenBitCleanPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport preparseadd preparsemodify preparsemodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Unique Attribute Plugin

Plugins of type unique-attribute-plugin have the following properties:

base-dn

Description

Specifies a base DN within which the attribute must be unique.

Default Value

The plug-in uses the server's public naming contexts in the searches.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.UniqueAttributePlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd preoperationmodify preoperationmodifydn postoperationadd postoperationmodify postoperationmodifydn postsynchronizationadd postsynchronizationmodify postsynchronizationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

type

Description

Specifies the type of attributes to check for value uniqueness.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-properties(1)

Name

dsconfig list-properties - Describes managed objects and their properties

Synopsis

`dsconfig list-properties` {options}

Description

Describes managed objects and their properties.

Options

The `dsconfig list-properties` command takes the following options:

`-c | --category {category}`
: The category of components whose properties should be described.

`-t | --type {type}`
: The type of components whose properties should be described. The value for TYPE must be one of the component types associated with the CATEGORY specified using the "--category" option.

`--inherited`
: Modifies the display output to show the inherited properties of components.

`--property {property}`
: The name of a property to be displayed.

dsconfig list-replication-domains(1)

Name

dsconfig list-replication-domains - Lists existing Replication Domains

Synopsis

`dsconfig list-replication-domains` {options}

Description

Lists existing Replication Domains.

Options

The `dsconfig list-replication-domains` command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default {name}: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

`--property {property}`

The name of a property to be displayed.

Replication Domain properties depend on the Replication Domain type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default {property}: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Replication Domain properties depend on the Replication Domain type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default {unit}: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Replication Domain properties depend on the Replication Domain type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default {unit}: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

Replication Domain

Replication Domains of type replication-domain have the following properties:

assured-sd-level

Description

The level of acknowledgment for Safe Data assured sub mode. When assured replication is configured in Safe Data mode, this value defines the number of replication servers (with the same group ID of the local server) that should acknowledge the sent update before the LDAP client call can return.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-timeout

Description

The timeout value when waiting for assured replication acknowledgments. Defines the amount of milliseconds the server will wait for assured acknowledgments (in either Safe Data or Safe Read assured replication modes) before returning anyway the LDAP client call.

Default Value

2000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-type

Description

Defines the assured replication mode of the replicated domain. The assured replication can be disabled or enabled. When enabled, two modes are available: Safe Data or Safe Read modes.

Default Value

not-assured

Allowed Values

not-assured

Assured replication is not enabled. Updates sent for replication (for being replayed on other LDAP servers in the topology) are sent without waiting for any acknowledgment and the LDAP client call returns immediately.

safe-data

Assured replication is enabled in Safe Data mode: updates sent for replication are subject to acknowledgment from the replication servers that have the same group ID as the local server (defined with the group-id property). The number of acknowledgments to expect is defined by the assured-sd-level property. After acknowledgments are received, LDAP client call returns.

safe-read

Assured replication is enabled in Safe Read mode: updates sent for replication are subject to acknowledgments from the LDAP servers in the topology that have the same group ID as the local server (defined with the group-id property). After acknowledgments are received, LDAP client call returns.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN of the replicated data.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

changetime-heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when sending its local change time to the Replication Server. The directory server sends a regular heart-beat to the Replication within the specified interval. The heart-beat indicates the change time of the directory server to the Replication Server.

Default Value

1000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

conflicts-historical-purge-delay

Description

This delay indicates the time (in minutes) the domain keeps the historical information necessary

to solve conflicts.When a change stored in the historical part of the user entry has a date (from its replication ChangeNumber) older than this delay, it is candidate to be purged. The purge is applied on 2 events: modify of the entry, dedicated purge task.

Default Value

1440m

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 minutes.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-exclude

Description

Allows to exclude some attributes to replicate to this server. If fractional-exclude configuration attribute is used, attributes specified in this attribute will be ignored (not added/modified/deleted) when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-include attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be excluded. The object class may be "*" indicating that the attribute type(s) should be excluded regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-include

Description

Allows to include some attributes to replicate to this server. If fractional-include configuration attribute is used, only attributes specified in this attribute will be added/modified/deleted when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-exclude attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be included. The object class may be "*" indicating that the attribute type(s) should be included regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group ID associated with this replicated domain. This value defines the group ID of the replicated domain. The replication system will preferably connect and send updates to replicate to a replication server with the same group ID as its own one (the local server group ID).

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when communicating with Replication Servers. The directory server expects a regular heart-beat coming from the Replication Server within the specified interval. If a heartbeat is not received within the interval, the Directory Server closes its connection and connects to another Replication Server.

Default Value

10000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 100 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

initialization-window-size

Description

Specifies the window size that this directory server may use when communicating with remote Directory Servers for initialization.

Default Value

100

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

isolation-policy

Description

Specifies the behavior of the directory server if a write operation is attempted on the data within the Replication Domain when none of the configured Replication Servers are available.

Default Value

reject-all-updates

Allowed Values

accept-all-updates

Indicates that updates should be accepted even though it is not possible to send them to any Replication Server. Best effort is made to re-send those updates to a Replication Servers when one of them is available, however those changes are at risk because they are only available from the historical information. This mode can also introduce high replication latency.

reject-all-updates

Indicates that all updates attempted on this Replication Domain are rejected when no

Replication Server is available.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-changenumber

Description

Indicates if this server logs the ChangeNumber in access log. This boolean indicates if the domain should log the ChangeNumber of replicated operations in the access log.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

referrals-url

Description

The URLs other LDAP servers should use to refer to the local server. URLs used by peer servers in the topology to refer to the local server through LDAP referrals. If this attribute is not defined,

every URLs available to access this server will be used. If defined, only URLs specified here will be used.

Default Value

None

Allowed Values

A LDAP URL compliant with RFC 2255.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of the Replication Servers within the Replication Domain to which the directory server should try to connect at startup time. Addresses must be specified using the syntax: hostname:port

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

server-id

Description

Specifies a unique identifier for the directory server within the Replication Domain. Each directory server within the same Replication Domain must have a different server ID. A directory server which is a member of multiple Replication Domains may use the same server ID for each of its Replication Domain configurations.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

solve-conflicts

Description

Indicates if this server solves conflict. This boolean indicates if this domain keeps the historical information necessary to solve conflicts. When set to false the server will not maintain historical information and will therefore not be able to solve conflict. This should therefore be done only if the replication is used in a single master type of deployment.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the directory server will use when communicating with Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-replication-server(1)

Name

dsconfig list-replication-server - Lists existing Replication Server

Synopsis

`dsconfig list-replication-server` {options}

Description

Lists existing Replication Server.

Options

The `dsconfig list-replication-server` command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Server properties depend on the Replication Server type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

`replication-server`

Default {name}: Replication Server

Enabled by default: false

See Replication Server for the properties of this Replication Server type.

`--property {property}`

The name of a property to be displayed.

Replication Server properties depend on the Replication Server type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

`replication-server`

Default {property}: Replication Server

Enabled by default: false

See Replication Server for the properties of this Replication Server type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Replication Server properties depend on the Replication Server type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

`replication-server`

Default {unit}: Replication Server

Enabled by default: false

See Replication Server for the properties of this Replication Server type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Replication Server properties depend on the Replication Server type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

`replication-server`

Default {unit}: Replication Server

Enabled by default: false

See Replication Server for the properties of this Replication Server type.

Replication Server

Replication Servers of type replication-server have the following properties:

assured-timeout

Description

The timeout value when waiting for assured mode acknowledgments. Defines the number of milliseconds that the replication server will wait for assured acknowledgments (in either Safe Data or Safe Read assured sub modes) before forgetting them and answer to the entity that sent an update and is waiting for acknowledgment.

Default Value

1000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these

default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compute-change-number

Description

Whether the replication server will compute change numbers. This boolean tells the replication server to compute change numbers for each replicated change by maintaining a change number index database. Changenumbers are computed according to http://tools.ietf.org/html/draft-good-ldap-changelog-04. Note this functionality has an impact on CPU, disk accesses and storage. If changenumbers are not required, it is advisable to set this value to false.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the replication change-log should make records readable only by Directory Server. Throughput and disk space are affected by the more expensive operations taking place. Confidentiality is achieved by encrypting records on all domains managed by this replication server. Encrypting the records prevents unauthorized parties from accessing contents of LDAP operations. For complete protection, consider enabling secure communications between servers. Change number indexing is not affected by the setting.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect operations performed after the change.

Advanced Property

No

Read-only

No

degraded-status-threshold

Description

The number of pending changes as threshold value for putting a directory server in degraded status. This value represents a number of pending changes a replication server has in queue for sending to a directory server. Once this value is crossed, the matching directory server goes in degraded status. When number of pending changes goes back under this value, the directory

server is put back in normal status. 0 means status analyzer is disabled and directory servers are never put in degraded status.

Default Value

5000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group id for the replication server. This value defines the group id of the replication server. The replication system of a LDAP server uses the group id of the replicated domain and tries to connect, if possible, to a replication with the same group id.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

monitoring-period

Description

The period between sending of monitoring messages. Defines the duration that the replication server will wait before sending new monitoring messages to its peers (replication servers and directory servers). Larger values increase the length of time it takes for a directory server to detect and switch to a more suitable replication server, whereas smaller values increase the amount of background network traffic.

Default Value

60s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

Specifies the number of changes that are kept in memory for each directory server in the Replication Domain.

Default Value

10000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

replication-db-directory

Description

The path where the Replication Server stores all persistent information.

Default Value

changelogDb

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

replication-port

Description

The port on which this Replication Server waits for connections from other Replication Servers or Directory Servers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-purge-delay

Description

The time (in seconds) after which the Replication Server erases all persistent information.

Default Value

3 days

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of other Replication Servers to which this Replication Server tries to connect at startup time. Addresses must be specified using the syntax: "hostname:port". If IPv6

addresses are used as the hostname, they must be specified using the syntax "[IPv6Address]:port".

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server-id

Description

Specifies a unique identifier for the Replication Server. Each Replication Server must have a different server ID.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

weight

Description

The weight of the replication server. The weight affected to the replication server. Each replication server of the topology has a weight. When combined together, the weights of the replication servers of a same group can be translated to a percentage that determines the quantity of directory servers of the topology that should be connected to a replication server. For instance imagine a topology with 3 replication servers (with the same group id) with the following weights: RS1=1, RS2=1, RS3=2. This means that RS1 should have 25% of the directory servers connected in the topology, RS2 25%, and RS3 50%. This may be useful if the replication servers of the topology have a different power and one wants to spread the load between the replication servers according to their power.

Default Value

1

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the Replication Server uses when communicating with other Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-sasl-mechanism-handlers(1)

Name

dsconfig list-sasl-mechanism-handlers - Lists existing SASL Mechanism Handlers

Synopsis

`dsconfig list-sasl-mechanism-handlers` {options}

Description

Lists existing SASL Mechanism Handlers.

Options

The `dsconfig list-sasl-mechanism-handlers` command takes the following options:

`--property {property}`

The name of a property to be displayed.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

`anonymous-sasl-mechanism-handler`

Default {property}: Anonymous SASL Mechanism Handler

Enabled by default: true

See Anonymous SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`cram-md5-sasl-mechanism-handler`

Default {property}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See Cram MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`digest-md5-sasl-mechanism-handler`

Default {property}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See Digest MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler

type.

`external-sasl-mechanism-handler`

Default {property}: External SASL Mechanism Handler

Enabled by default: true

See External SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`gssapi-sasl-mechanism-handler`

Default {property}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See GSSAPI SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`plain-sasl-mechanism-handler`

Default {property}: Plain SASL Mechanism Handler

Enabled by default: true

See Plain SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

`anonymous-sasl-mechanism-handler`

Default {unit}: Anonymous SASL Mechanism Handler

Enabled by default: true

See Anonymous SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`cram-md5-sasl-mechanism-handler`

Default {unit}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See Cram MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`digest-md5-sasl-mechanism-handler`

Default {unit}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See Digest MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`external-sasl-mechanism-handler`

Default {unit}: External SASL Mechanism Handler

Enabled by default: true

See External SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`gssapi-sasl-mechanism-handler`

Default {unit}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See GSSAPI SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`plain-sasl-mechanism-handler`

Default {unit}: Plain SASL Mechanism Handler

Enabled by default: true

See Plain SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

`anonymous-sasl-mechanism-handler`

Default {unit}: Anonymous SASL Mechanism Handler

Enabled by default: true

See Anonymous SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`cram-md5-sasl-mechanism-handler`

Default {unit}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See Cram MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`digest-md5-sasl-mechanism-handler`

Default {unit}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See Digest MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`external-sasl-mechanism-handler`

Default {unit}: External SASL Mechanism Handler

Enabled by default: true

See External SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`gssapi-sasl-mechanism-handler`

Default {unit}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See GSSAPI SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`plain-sasl-mechanism-handler`

Default {unit}: Plain SASL Mechanism Handler

Enabled by default: true

See Plain SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

Anonymous SASL Mechanism Handler

SASL Mechanism Handlers of type anonymous-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.AnonymousSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Cram MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type cram-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper used with this SASL mechanism handler to match the authentication ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Cram MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.CRAMMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Digest MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type digest-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Digest MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.DigestMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realms that is to be used by the server for DIGEST-MD5 authentication. If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Default Value

If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Allowed Values

Any realm string that does not contain a comma.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the server that is used when validating the digest-uri parameter during the authentication process. If this configuration attribute is present, then the server expects that clients use a digest-uri equal to "ldap/" followed by the value of this attribute. For example, if the attribute has a value of "directory.example.com", then the server expects clients to use a digest-uri of "ldap/directory.example.com". If no value is provided, then the server does not attempt to validate the digest-uri provided by the client and accepts any value.

Default Value

The server attempts to determine the fully-qualified domain name dynamically.

Allowed Values

The fully-qualified address that is expected for clients to use when connecting to the server and authenticating via DIGEST-MD5.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

External SASL Mechanism Handler

SASL Mechanism Handlers of type external-sasl-mechanism-handler have the following properties:

certificate-attribute

Description

Specifies the name of the attribute to hold user certificates. This property must specify the name of a valid attribute type defined in the server schema.

Default Value

userCertificate

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-mapper

Description

Specifies the name of the certificate mapper that should be used to match client certificates to user entries.

Default Value

None

Allowed Values

The DN of any Certificate Mapper. The referenced certificate mapper must be enabled when the External SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-validation-policy

Description

Indicates whether to attempt to validate the peer certificate against a certificate held in the user's entry.

Default Value

None

Allowed Values

always

Always require the peer certificate to be present in the user's entry.

ifpresent

If the user's entry contains one or more certificates, require that one of them match the peer certificate.

never

Do not look for the peer certificate to be present in the user's entry.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.ExternalSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

GSSAPI SASL Mechanism Handler

SASL Mechanism Handlers of type gssapi-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the Kerberos principal included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the GSSAPI SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.GSSAPISASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

kdc-address

Description

Specifies the address of the KDC that is to be used for Kerberos processing. If provided, this property must be a fully-qualified DNS-resolvable name. If this property is not provided, then the server attempts to determine it from the system-wide Kerberos configuration.

Default Value

The server attempts to determine the KDC address from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

keytab

Description

Specifies the path to the keytab file that should be used for Kerberos processing. If provided, this is either an absolute path or one that is relative to the server instance root.

Default Value

The server attempts to use the system-wide default keytab.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

principal-name

Description

Specifies the principal name. It can either be a simple user name or a service name such as host/example.com. If this property is not provided, then the server attempts to build the principal name by appending the fully qualified domain name to the string "ldap/".

Default Value

The server attempts to determine the principal name from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realm to be used for GSSAPI authentication.

Default Value

The server attempts to determine the realm from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the system.

Default Value

The server attempts to determine the fully-qualified domain name dynamically .

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Plain SASL Mechanism Handler

SASL Mechanism Handlers of type plain-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Plain SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.PlainSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-schema-providers(1)

Name

dsconfig list-schema-providers - Lists existing Schema Providers

Synopsis

`dsconfig list-schema-providers` {options}

Description

Lists existing Schema Providers.

Options

The `dsconfig list-schema-providers` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Schema Provider properties depend on the Schema Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

`core-schema`

Default {property}: Core Schema

Enabled by default: true

See Core Schema for the properties of this Schema Provider type.

`json-schema`

Default {property}: Json Schema

Enabled by default: true

See Json Schema for the properties of this Schema Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Schema Provider properties depend on the Schema Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

`core-schema`

Default {unit}: Core Schema

Enabled by default: true

See Core Schema for the properties of this Schema Provider type.

`json-schema`

Default {unit}: Json Schema

Enabled by default: true

See Json Schema for the properties of this Schema Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Schema Provider properties depend on the Schema Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

`core-schema`

Default {unit}: Core Schema

Enabled by default: true

See Core Schema for the properties of this Schema Provider type.

`json-schema`

Default {unit}: Json Schema

Enabled by default: true

See Json Schema for the properties of this Schema Provider type.

Core Schema

Schema Providers of type core-schema have the following properties:

allow-attribute-types-with-no-sup-or-syntax

Description

Indicates whether the schema should allow attribute type definitions that do not declare a superior attribute type or syntax When set to true, invalid attribute type definitions will use the default syntax.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-zero-length-values-directory-string

Description

Indicates whether zero-length (that is, an empty string) values are allowed for directory string. This is technically not allowed by the revised LDAPv3 specification, but some environments may require it for backward compatibility with servers that do allow it.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disabled-matching-rule

Description

The set of disabled matching rules. Matching rules must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled matching rule.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

disabled-syntax

Description

The set of disabled syntaxes. Syntaxes must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled syntax, or NONE

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Core Schema implementation.

Default Value

org.opends.server.schema.CoreSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

json-validation-policy

Description

Specifies the policy that will be used when validating JSON syntax values.

Default Value

strict

Allowed Values

disabled

JSON syntax values will not be validated and, as a result any sequence of bytes will be acceptable.

lenient

JSON syntax values must comply with RFC 7159 except: 1) comments are allowed, 2) single quotes may be used instead of double quotes, and 3) unquoted control characters are allowed in strings.

strict

JSON syntax values must strictly conform to RFC 7159.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-certificates

Description

Indicates whether X.509 Certificate values are required to strictly comply with the standard definition for this syntax. When set to false, certificates will not be validated and, as a result any sequence of bytes will be acceptable.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-country-string

Description

Indicates whether country code values are required to strictly comply with the standard definition for this syntax. When set to false, country codes will not be validated and, as a result any string containing 2 characters will be acceptable.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-jpeg-photos

Description

Indicates whether to require JPEG values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-telephone-numbers

Description

Indicates whether to require telephone number values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strip-syntax-min-upper-bound-attribute-type-description

Description

Indicates whether the suggested minimum upper bound appended to an attribute's syntax OID in it's schema definition Attribute Type Description is stripped off. When retrieving the server's schema, some APIs (JNDI) fail in their syntax lookup methods, because they do not parse this value correctly. This configuration option allows the server to be configured to provide schema definitions these APIs can parse correctly.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Json Schema

Schema Providers of type json-schema have the following properties:

case-sensitive-strings

Description

Indicates whether JSON string comparisons should be case-sensitive.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ignore-white-space

Description

Indicates whether JSON string comparisons should ignore white-space. When enabled all leading and trailing white space will be removed and intermediate white space will be reduced to a single character.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

indexed-field

Description

Specifies which JSON fields should be indexed. A field will be indexed if it matches any of the configured field patterns.

Default Value

All JSON fields will be indexed.

Allowed Values

A JSON pointer which may include wild-cards. A single '**' wild-card matches at most a single path element, whereas a double '**'** matches zero or more path elements.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Json Schema implementation.

Default Value

org.opends.server.schema.JsonSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

matching-rule-name

Description

The name of the custom JSON matching rule.

Default Value

The matching rule will not have a name.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

matching-rule-oid

Description

The numeric OID of the custom JSON matching rule.

Default Value

None

Allowed Values

The OID of the matching rule.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-service-discovery-mechanisms(1)

Name

dsconfig list-service-discovery-mechanisms - Lists existing Service Discovery Mechanisms

Synopsis

`dsconfig list-service-discovery-mechanisms` {options}

Description

Lists existing Service Discovery Mechanisms.

Options

The `dsconfig list-service-discovery-mechanisms` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

`replication-service-discovery-mechanism`

Default {property}: Replication Service Discovery Mechanism

Enabled by default: false

See Replication Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`static-service-discovery-mechanism`

Default {property}: Static Service Discovery Mechanism

Enabled by default: false

See Static Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

`replication-service-discovery-mechanism`

Default {unit}: Replication Service Discovery Mechanism

Enabled by default: false

See Replication Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`static-service-discovery-mechanism`

Default {unit}: Static Service Discovery Mechanism

Enabled by default: false

See Static Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

`replication-service-discovery-mechanism`

Default {unit}: Replication Service Discovery Mechanism

Enabled by default: false

See Replication Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`static-service-discovery-mechanism`

Default {unit}: Static Service Discovery Mechanism

Enabled by default: false

See Static Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

Replication Service Discovery Mechanism

Service Discovery Mechanisms of type replication-service-discovery-mechanism have the following properties:

bind-dn

Description

The bind DN for periodically reading replication server configurations The bind DN must be present on all replication servers and directory servers, it must be able to read the server configuration.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

bind-password

Description

The bind password for periodically reading replication server configurations The bind password must be the same on all replication and directory servers

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

discovery-interval

Description

Interval between two replication server configuration discovery queries. Specifies how frequently to query a replication server configuration in order to discover information about available directory server replicas.

Default Value

60s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.ReplicationServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-group-id

Description

Replication domain group ID of preferred directory server replicas. Directory server replicas with this replication domain group ID will be preferred over other directory server replicas. Secondary server replicas will only be used when all primary server replicas become unavailable.

Default Value

All the server replicas will be treated the same.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the list of replication servers to contact periodically when discovering server replicas.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

Static Service Discovery Mechanism

Service Discovery Mechanisms of type static-service-discovery-mechanism have the following properties:

discovery-interval

Description

Interval between two server configuration discovery executions. Specifies how frequently to read the configuration of the servers in order to discover their new information.

Default Value

60s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.StaticServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-server

Description

Specifies a list of servers that will be used in preference to secondary servers when available.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-server

Description

Specifies a list of servers that will be used in place of primary servers when all primary servers are unavailable.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig list-synchronization-providers(1)

Name

dsconfig list-synchronization-providers - Lists existing Synchronization Providers

Synopsis

`dsconfig list-synchronization-providers` {options}

Description

Lists existing Synchronization Providers.

Options

The `dsconfig list-synchronization-providers` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

`replication-synchronization-provider`

Default {property}: Replication Synchronization Provider

Enabled by default: true

See Replication Synchronization Provider for the properties of this Synchronization Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

`replication-synchronization-provider`

Default {unit}: Replication Synchronization Provider

Enabled by default: true

See Replication Synchronization Provider for the properties of this Synchronization Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

`replication-synchronization-provider`

Default {unit}: Replication Synchronization Provider

Enabled by default: true

See Replication Synchronization Provider for the properties of this Synchronization Provider type.

Replication Synchronization Provider

Synchronization Providers of type replication-synchronization-provider have the following properties:

connection-timeout

Description

Specifies the timeout used when connecting to peers and when performing SSL negotiation.

Default Value

5 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Synchronization Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Synchronization Provider implementation.

Default Value

org.opends.server.replication.plugin.MultimasterReplication

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SynchronizationProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-update-replay-threads

Description

Specifies the number of update replay threads. This value is the number of threads created for replaying every updates received for all the replication domains.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-trust-manager-providers(1)

Name

dsconfig list-trust-manager-providers - Lists existing Trust Manager Providers

Synopsis

`dsconfig list-trust-manager-providers` {options}

Description

Lists existing Trust Manager Providers.

Options

The `dsconfig list-trust-manager-providers` command takes the following options:

`--property {property}`
: The name of a property to be displayed.

  Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {property} you provide.

  By default, OpenDJ directory server supports the following Trust Manager Provider types:

  `blind-trust-manager-provider`
  : Default {property}: Blind Trust Manager Provider

    Enabled by default: true

    See Blind Trust Manager Provider for the properties of this Trust Manager Provider type.

  `file-based-trust-manager-provider`
  : Default {property}: File Based Trust Manager Provider

    Enabled by default: true

    See File Based Trust Manager Provider for the properties of this Trust Manager Provider type.

  `ldap-trust-manager-provider`
  : Default {property}: LDAP Trust Manager Provider

    Enabled by default: true

    See LDAP Trust Manager Provider for the properties of this Trust Manager Provider type.

`pkcs11-trust-manager-provider`

Default {property}: PKCS11 Trust Manager Provider

Enabled by default: true

See PKCS11 Trust Manager Provider for the properties of this Trust Manager Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

`blind-trust-manager-provider`

Default {unit}: Blind Trust Manager Provider

Enabled by default: true

See Blind Trust Manager Provider for the properties of this Trust Manager Provider type.

`file-based-trust-manager-provider`

Default {unit}: File Based Trust Manager Provider

Enabled by default: true

See File Based Trust Manager Provider for the properties of this Trust Manager Provider type.

`ldap-trust-manager-provider`

Default {unit}: LDAP Trust Manager Provider

Enabled by default: true

See LDAP Trust Manager Provider for the properties of this Trust Manager Provider type.

`pkcs11-trust-manager-provider`

Default {unit}: PKCS11 Trust Manager Provider

Enabled by default: true

See PKCS11 Trust Manager Provider for the properties of this Trust Manager Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

`blind-trust-manager-provider`

Default {unit}: Blind Trust Manager Provider

Enabled by default: true

See Blind Trust Manager Provider for the properties of this Trust Manager Provider type.

`file-based-trust-manager-provider`

Default {unit}: File Based Trust Manager Provider

Enabled by default: true

See File Based Trust Manager Provider for the properties of this Trust Manager Provider type.

`ldap-trust-manager-provider`

Default {unit}: LDAP Trust Manager Provider

Enabled by default: true

See LDAP Trust Manager Provider for the properties of this Trust Manager Provider type.

`pkcs11-trust-manager-provider`

Default {unit}: PKCS11 Trust Manager Provider

Enabled by default: true

See PKCS11 Trust Manager Provider for the properties of this Trust Manager Provider type.

Blind Trust Manager Provider

Trust Manager Providers of type blind-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Blind Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.BlindTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Trust Manager Provider

Trust Manager Providers of type file-based-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file containing the trust information. It can be an absolute path or a path that is relative to the OpenDJ instance root. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

An absolute path or a path that is relative to the OpenDJ directory server instance root.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the trust store file. Valid values always include 'JKS' and 'PKCS12', but different implementations can allow other values as well. If no value is provided, then the JVM default value is used. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment. The "JKS" and "PKCS12" formats are typically available in Java environments.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

LDAP Trust Manager Provider

Trust Manager Providers of type ldap-trust-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the

LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

PKCS11 Trust Manager Provider

Trust Manager Providers of type pkcs11-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11TrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig list-virtual-attributes(1)

Name

dsconfig list-virtual-attributes - Lists existing Virtual Attributes

Synopsis

`dsconfig list-virtual-attributes` {options}

Description

Lists existing Virtual Attributes.

Options

The `dsconfig list-virtual-attributes` command takes the following options:

`--property {property}`

The name of a property to be displayed.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

`collective-attribute-subentries-virtual-attribute`

Default {property}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See Collective Attribute Subentries Virtual Attribute for the properties of this Virtual Attribute type.

`entity-tag-virtual-attribute`

Default {property}: Entity Tag Virtual Attribute

Enabled by default: true

See Entity Tag Virtual Attribute for the properties of this Virtual Attribute type.

`entry-dn-virtual-attribute`

Default {property}: Entry DN Virtual Attribute

Enabled by default: true

See Entry DN Virtual Attribute for the properties of this Virtual Attribute type.

`entry-uuid-virtual-attribute`

Default {property}: Entry UUID Virtual Attribute

Enabled by default: true

See Entry UUID Virtual Attribute for the properties of this Virtual Attribute type.

`governing-structure-rule-virtual-attribute`

Default {property}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See Governing Structure Rule Virtual Attribute for the properties of this Virtual Attribute type.

`has-subordinates-virtual-attribute`

Default {property}: Has Subordinates Virtual Attribute

Enabled by default: true

See Has Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`is-member-of-virtual-attribute`

Default {property}: Is Member Of Virtual Attribute

Enabled by default: true

See Is Member Of Virtual Attribute for the properties of this Virtual Attribute type.

`member-virtual-attribute`

Default {property}: Member Virtual Attribute

Enabled by default: true

See Member Virtual Attribute for the properties of this Virtual Attribute type.

`num-subordinates-virtual-attribute`

Default {property}: Num Subordinates Virtual Attribute

Enabled by default: true

See Num Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`password-expiration-time-virtual-attribute`

Default {property}: Password Expiration Time Virtual Attribute

Enabled by default: true

See Password Expiration Time Virtual Attribute for the properties of this Virtual Attribute type.

`password-policy-subentry-virtual-attribute`

Default {property}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See Password Policy Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`structural-object-class-virtual-attribute`

Default {property}: Structural Object Class Virtual Attribute

Enabled by default: true

See Structural Object Class Virtual Attribute for the properties of this Virtual Attribute type.

`subschema-subentry-virtual-attribute`

Default {property}: Subschema Subentry Virtual Attribute

Enabled by default: true

See Subschema Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`user-defined-virtual-attribute`

Default {property}: User Defined Virtual Attribute

Enabled by default: true

See User Defined Virtual Attribute for the properties of this Virtual Attribute type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

`collective-attribute-subentries-virtual-attribute`

Default {unit}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See Collective Attribute Subentries Virtual Attribute for the properties of this Virtual Attribute type.

`entity-tag-virtual-attribute`

Default {unit}: Entity Tag Virtual Attribute

Enabled by default: true

See Entity Tag Virtual Attribute for the properties of this Virtual Attribute type.

`entry-dn-virtual-attribute`

Default {unit}: Entry DN Virtual Attribute

Enabled by default: true

See Entry DN Virtual Attribute for the properties of this Virtual Attribute type.

`entry-uuid-virtual-attribute`

Default {unit}: Entry UUID Virtual Attribute

Enabled by default: true

See Entry UUID Virtual Attribute for the properties of this Virtual Attribute type.

`governing-structure-rule-virtual-attribute`

Default {unit}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See Governing Structure Rule Virtual Attribute for the properties of this Virtual Attribute type.

`has-subordinates-virtual-attribute`

Default {unit}: Has Subordinates Virtual Attribute

Enabled by default: true

See Has Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`is-member-of-virtual-attribute`

Default {unit}: Is Member Of Virtual Attribute

Enabled by default: true

See Is Member Of Virtual Attribute for the properties of this Virtual Attribute type.

`member-virtual-attribute`

Default {unit}: Member Virtual Attribute

Enabled by default: true

See Member Virtual Attribute for the properties of this Virtual Attribute type.

`num-subordinates-virtual-attribute`

Default {unit}: Num Subordinates Virtual Attribute

Enabled by default: true

See Num Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`password-expiration-time-virtual-attribute`

Default {unit}: Password Expiration Time Virtual Attribute

Enabled by default: true

See Password Expiration Time Virtual Attribute for the properties of this Virtual Attribute type.

`password-policy-subentry-virtual-attribute`

Default {unit}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See Password Policy Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`structural-object-class-virtual-attribute`

Default {unit}: Structural Object Class Virtual Attribute

Enabled by default: true

See Structural Object Class Virtual Attribute for the properties of this Virtual Attribute type.

`subschema-subentry-virtual-attribute`

Default {unit}: Subschema Subentry Virtual Attribute

Enabled by default: true

See Subschema Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`user-defined-virtual-attribute`

Default {unit}: User Defined Virtual Attribute

Enabled by default: true

See User Defined Virtual Attribute for the properties of this Virtual Attribute type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

`collective-attribute-subentries-virtual-attribute`

Default {unit}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See Collective Attribute Subentries Virtual Attribute for the properties of this Virtual Attribute type.

`entity-tag-virtual-attribute`

Default {unit}: Entity Tag Virtual Attribute

Enabled by default: true

See Entity Tag Virtual Attribute for the properties of this Virtual Attribute type.

`entry-dn-virtual-attribute`

Default {unit}: Entry DN Virtual Attribute

Enabled by default: true

See Entry DN Virtual Attribute for the properties of this Virtual Attribute type.

`entry-uuid-virtual-attribute`

Default {unit}: Entry UUID Virtual Attribute

Enabled by default: true

See Entry UUID Virtual Attribute for the properties of this Virtual Attribute type.

`governing-structure-rule-virtual-attribute`

Default {unit}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See Governing Structure Rule Virtual Attribute for the properties of this Virtual Attribute type.

`has-subordinates-virtual-attribute`

Default {unit}: Has Subordinates Virtual Attribute

Enabled by default: true

See Has Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`is-member-of-virtual-attribute`

Default {unit}: Is Member Of Virtual Attribute

Enabled by default: true

See Is Member Of Virtual Attribute for the properties of this Virtual Attribute type.

`member-virtual-attribute`

Default {unit}: Member Virtual Attribute

Enabled by default: true

See Member Virtual Attribute for the properties of this Virtual Attribute type.

`num-subordinates-virtual-attribute`

Default {unit}: Num Subordinates Virtual Attribute

Enabled by default: true

See Num Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`password-expiration-time-virtual-attribute`

Default {unit}: Password Expiration Time Virtual Attribute

Enabled by default: true

See Password Expiration Time Virtual Attribute for the properties of this Virtual Attribute type.

`password-policy-subentry-virtual-attribute`

Default {unit}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See Password Policy Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`structural-object-class-virtual-attribute`

Default {unit}: Structural Object Class Virtual Attribute

Enabled by default: true

See Structural Object Class Virtual Attribute for the properties of this Virtual Attribute type.

`subschema-subentry-virtual-attribute`

Default {unit}: Subschema Subentry Virtual Attribute

Enabled by default: true

See Subschema Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`user-defined-virtual-attribute`

Default {unit}: User Defined Virtual Attribute

Enabled by default: true

See User Defined Virtual Attribute for the properties of this Virtual Attribute type.

Collective Attribute Subentries Virtual Attribute

Virtual Attributes of type collective-attribute-subentries-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

collectiveAttributeSubentries

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.CollectiveAttributeSubentriesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Entity Tag Virtual Attribute

Virtual Attributes of type entity-tag-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

etag

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

checksum-algorithm

Description

The algorithm which should be used for calculating the entity tag checksum value.

Default Value

adler-32

Allowed Values

adler-32

The Adler-32 checksum algorithm which is almost as reliable as a CRC-32 but can be computed much faster.

crc-32

The CRC-32 checksum algorithm.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

excluded-attribute

Description

The list of attributes which should be ignored when calculating the entity tag checksum value. Certain attributes like "ds-sync-hist" may vary between replicas due to different purging schedules and should not be included in the checksum.

Default Value

ds-sync-hist

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value

generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntityTagVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Entry DN Virtual Attribute

Virtual Attributes of type entry-dn-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryDN

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryDNVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Entry UUID Virtual Attribute

Virtual Attributes of type entry-uuid-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryUUID

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no

values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryUUIDVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Governing Structure Rule Virtual Attribute

Virtual Attributes of type governing-structure-rule-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

governingStructureRule

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.GoverningSturctureRuleVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Has Subordinates Virtual Attribute

Virtual Attributes of type has-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

hasSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.HasSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Is Member Of Virtual Attribute

Virtual Attributes of type is-member-of-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

isMemberOf

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry

and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those

filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.IsMemberOfVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Member Virtual Attribute

Virtual Attributes of type member-virtual-attribute have the following properties:

allow-retrieving-membership

Description

Indicates whether to handle requests that request all values for the virtual attribute. This operation can be very expensive in some cases and is not consistent with the primary function of virtual static groups, which is to make it possible to use static group idioms to determine whether a given user is a member. If this attribute is set to false, attempts to retrieve the entire set of values receive an empty set, and only attempts to determine whether the attribute has a specific value or set of values (which is the primary anticipated use for virtual static groups) are handled properly.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an

entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.MemberVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Num Subordinates Virtual Attribute

Virtual Attributes of type num-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

numSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry

and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those

filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.NumSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Password Expiration Time Virtual Attribute

Virtual Attributes of type password-expiration-time-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

ds-pwp-password-expiration-time

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordExpirationTimeVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Password Policy Subentry Virtual Attribute

Virtual Attributes of type password-policy-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

pwdPolicySubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no

values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordPolicySubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Structural Object Class Virtual Attribute

Virtual Attributes of type structural-object-class-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

structuralObjectClass

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.StructuralObjectClassVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subschema Subentry Virtual Attribute

Virtual Attributes of type subschema-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

subschemaSubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.SubschemaSubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

User Defined Virtual Attribute

Virtual Attributes of type user-defined-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry

and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those

filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.UserDefinedVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

value

Description

Specifies the values to be included in the virtual attribute.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-access-control-handler-prop(1)

Name

dsconfig set-access-control-handler-prop - Modifies Access Control Handler properties

Synopsis

`dsconfig set-access-control-handler-prop` {options}

Description

Modifies Access Control Handler properties.

Options

The `dsconfig set-access-control-handler-prop` command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Access Control Handler properties depend on the Access Control Handler type, which depends on the null option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Access Control Handler properties depend on the Access Control Handler type, which depends on the null option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Access Control Handler properties depend on the Access Control Handler type, which depends on the null option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Access Control Handler properties depend on the Access Control Handler type, which depends on the null option.

Dsee Compat Access Control Handler

Access Control Handlers of type dsee-compat-access-control-handler have the following properties:

enabled

Description

Indicates whether the Access Control Handler is enabled. If set to FALSE, then no access control is enforced, and any client (including unauthenticated or anonymous clients) could be allowed to perform any operation if not subject to other restrictions, such as those enforced by the privilege subsystem.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

global-aci

Description

Defines global access control rules. Global access control rules apply to all entries anywhere in the data managed by the OpenDJ directory server. The global access control rules may be overridden by more specific access control rules placed in the data.

Default Value

No global access control rules are defined, which means that no access is allowed for any data in the server unless specifically granted by access control rules in the data.

Allowed Values

<olink targetdoc="admin-guide" targetptr="about-acis" />

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Dsee Compat Access Control Handler implementation.

Default Value

org.opends.server.authorization.dseecompat.AciHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccessControlHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Access Control Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-access-log-filtering-criteria-prop(1)

Name

dsconfig set-access-log-filtering-criteria-prop - Modifies Access Log Filtering Criteria properties

Synopsis

`dsconfig set-access-log-filtering-criteria-prop` {options}

Description

Modifies Access Log Filtering Criteria properties.

Options

The `dsconfig set-access-log-filtering-criteria-prop` command takes the following options:

`--publisher-name {name}`

The name of the Access Log Publisher.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

`--criteria-name {name}`

The name of the Access Log Filtering Criteria.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

`access-log-filtering-criteria`

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See Access Log Filtering Criteria for the properties of this Access Log Filtering Criteria type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the `--criteria-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the `--criteria-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the `--criteria-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the `--criteria-name {name}` option.

Access Log Filtering Criteria

Access Log Filtering Criteria of type access-log-filtering-criteria have the following properties:

connection-client-address-equal-to

Description

Filters log records associated with connections which match at least one of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-client-address-not-equal-to

Description

Filters log records associated with connections which do not match any of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-port-equal-to

Description

Filters log records associated with connections to any of the specified listener port numbers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-protocol-equal-to

Description

Filters log records associated with connections which match any of the specified protocols. Typical values include "ldap", "ldaps", or "jmx".

Default Value

None

Allowed Values

The protocol name as reported in the access log.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-type

Description

Filters log records based on their type.

Default Value

None

Allowed Values

abandon

Abandon operations

add

Add operations

bind

Bind operations

compare

Compare operations

connect

Client connections

delete

Delete operations

disconnect

Client disconnections

extended

Extended operations

modify

Modify operations

rename

Rename operations

search

Search operations

unbind

Unbind operations

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-equal-to

Description

Filters operation log records associated with operations which target entries matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-not-equal-to

Description

Filters operation log records associated with operations which target entries matching none of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-greater-than

Description

Filters operation response log records associated with operations which took longer than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-less-than

Description

Filters operation response log records associated with operations which took less than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-equal-to

Description

Filters operation response log records associated with operations which include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-not-equal-to

Description

Filters operation response log records associated with operations which do not include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-is-indexed

Description

Filters search operation response log records associated with searches which were either indexed or unindexed. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-greater-than

Description

Filters search operation response log records associated with searches which returned more than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-less-than

Description

Filters search operation response log records associated with searches which returned less than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-equal-to

Description

Filters log records associated with users matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-not-equal-to

Description

Filters log records associated with users which do not match any of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard **replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-member-of

Description

Filters log records associated with users which are members of at least one of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-not-member-of

Description

Filters log records associated with users which are not members of any of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-account-status-notification-handler-prop(1)

Name

dsconfig set-account-status-notification-handler-prop - Modifies Account Status Notification Handler properties

Synopsis

`dsconfig set-account-status-notification-handler-prop` {options}

Description

Modifies Account Status Notification Handler properties.

Options

The `dsconfig set-account-status-notification-handler-prop` command takes the following options:

`--handler-name {name}`

The name of the Account Status Notification Handler.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

`error-log-account-status-notification-handler`

Default {name}: Error Log Account Status Notification Handler

Enabled by default: true

See Error Log Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`smtp-account-status-notification-handler`

Default {name}: SMTP Account Status Notification Handler

Enabled by default: true

See SMTP Account Status Notification Handler for the properties of this Account Status Notification Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the `--handler-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the `--handler-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the `--handler-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the `--handler-name {name}` option.

Error Log Account Status Notification Handler

Account Status Notification Handlers of type error-log-account-status-notification-handler have the following properties:

account-status-notification-type

Description

Indicates which types of event can trigger an account status notification.

Default Value

None

Allowed Values

account-disabled

Generate a notification whenever a user account has been disabled by an administrator.

account-enabled

Generate a notification whenever a user account has been enabled by an administrator.

account-expired

Generate a notification whenever a user authentication has failed because the account has expired.

account-idle-locked

Generate a notification whenever a user account has been locked because it was idle for too long.

account-permanently-locked

Generate a notification whenever a user account has been permanently locked after too many failed attempts.

account-reset-locked

Generate a notification whenever a user account has been locked, because the password had been reset by an administrator but not changed by the user within the required interval.

account-temporarily-locked

Generate a notification whenever a user account has been temporarily locked after too many failed attempts.

account-unlocked

Generate a notification whenever a user account has been unlocked by an administrator.

password-changed

Generate a notification whenever a user changes his/her own password.

password-expired

Generate a notification whenever a user authentication has failed because the password has expired.

password-expiring

Generate a notification whenever a password expiration warning is encountered for a user password for the first time.

password-reset

Generate a notification whenever a user's password is reset by an administrator.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Error Log Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.ErrorLogAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

SMTP Account Status Notification Handler

Account Status Notification Handlers of type smtp-account-status-notification-handler have the following properties:

email-address-attribute-type

Description

Specifies which attribute in the user's entries may be used to obtain the email address when notifying the end user. You can specify more than one email address as separate values. In this case, the OpenDJ server sends a notification to all email addresses identified.

Default Value

If no email address attribute types are specified, then no attempt is made to send email notification messages to end users. Only those users specified in the set of additional recipient addresses are sent the notification messages.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.SMTPAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this account status notification handler. The values for this property should begin with the name of an account status notification type followed by a colon and the subject that should be used for the associated notification message. If an email message is generated for an account status notification type for which no subject is defined, then that message is given a generic subject.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-template-file

Description

Specifies the path to the file containing the message template to generate the email notification messages. The values for this property should begin with the name of an account status notification type followed by a colon and the path to the template file that should be used for that notification type. If an account status notification has a notification type that is not associated with a message template file, then no email message is generated for that notification.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which notification messages are sent, either instead of or in addition to the end user for whom the notification has been generated. This may be used to ensure that server administrators also receive a copy of any notification messages that are generated.

Default Value

If no additional recipient addresses are specified, then only the end users that are the subjects of the account status notifications receive the notification messages.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

send-email-as-html

Description

Indicates whether an email notification message should be sent as HTML. If this value is true, email notification messages are marked as text/html. Otherwise outgoing email messages are assumed to be plaintext and marked as text/plain.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-message-without-end-user-address

Description

Indicates whether an email notification message should be generated and sent to the set of notification recipients even if the user entry does not contain any values for any of the email address attributes (that is, in cases when it is not be possible to notify the end user). This is only applicable if both one or more email address attribute types and one or more additional recipient addresses are specified.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

sender-address

Description

Specifies the email address from which the message is sent. Note that this does not necessarily have to be a legitimate email address.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-administration-connector-prop(1)

Name

dsconfig set-administration-connector-prop - Modifies Administration Connector properties

Synopsis

`dsconfig set-administration-connector-prop` {options}

Description

Modifies Administration Connector properties.

Options

The `dsconfig set-administration-connector-prop` command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Administration Connector properties depend on the Administration Connector type, which depends on the null option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Administration Connector properties depend on the Administration Connector type, which depends on the null option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Administration Connector properties depend on the Administration Connector type, which depends on the null option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Administration Connector properties depend on the Administration Connector type, which depends on the null option.

Administration Connector

Administration Connectors of type administration-connector have the following properties:

key-manager-provider

Description

Specifies the name of the key manager that is used with the Administration Connector .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

Yes

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this Administration Connector should listen for connections from LDAP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the Administration Connector listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the Administration Connector will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Administration Connector must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Administration Connector should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key

certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that is used with the Administration Connector .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

dsconfig set-alert-handler-prop(1)

Name

dsconfig set-alert-handler-prop - Modifies Alert Handler properties

Synopsis

`dsconfig set-alert-handler-prop` {options}

Description

Modifies Alert Handler properties.

Options

The `dsconfig set-alert-handler-prop` command takes the following options:

`--handler-name {name}`

The name of the Alert Handler.

Alert Handler properties depend on the Alert Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

`jmx-alert-handler`

Default {name}: JMX Alert Handler

Enabled by default: true

See JMX Alert Handler for the properties of this Alert Handler type.

`smtp-alert-handler`

Default {name}: SMTP Alert Handler

Enabled by default: true

See SMTP Alert Handler for the properties of this Alert Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Alert Handler properties depend on the Alert Handler type, which depends on the `--handler-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Alert Handler properties depend on the Alert Handler type, which depends on the `--handler-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Alert Handler properties depend on the Alert Handler type, which depends on the `--handler-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Alert Handler properties depend on the Alert Handler type, which depends on the `--handler-name {name}` option.

JMX Alert Handler

Alert Handlers of type jmx-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Alert Handler implementation.

Default Value

org.opends.server.extensions.JMXAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

SMTP Alert Handler

Alert Handlers of type smtp-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are

no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Alert Handler implementation.

Default Value

org.opends.server.extensions.SMTPAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-body

Description

Specifies the body that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-

message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which the messages should be sent. Multiple values may be provided if there should be more than one recipient.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

sender-address

Description

Specifies the email address to use as the sender for messages generated by this alert handler.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-backend-index-prop(1)

Name

dsconfig set-backend-index-prop - Modifies Backend Index properties

Synopsis

`dsconfig set-backend-index-prop` {options}

Description

Modifies Backend Index properties.

Options

The `dsconfig set-backend-index-prop` command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend Index properties depend on the Backend Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default {name}: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

`--index-name {name}`

The name of the Backend Index.

Backend Index properties depend on the Backend Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

`backend-index`

Default {name}: Backend Index

Enabled by default: false

See Backend Index for the properties of this Backend Index type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Backend Index properties depend on the Backend Index type, which depends on the `--index-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Backend Index properties depend on the Backend Index type, which depends on the `--index-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Backend Index properties depend on the Backend Index type, which depends on the `--index-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Backend Index properties depend on the Backend Index type, which depends on the `--index-name {name}` option.

Backend Index

Backend Indexes of type backend-index have the following properties:

attribute

Description

Specifies the name of the attribute for which the index is to be maintained.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

confidentiality-enabled

Description

Specifies whether contents of the index should be confidential. Setting the flag to true will hash keys for equality type indexes using SHA-1 and encrypt the list of entries matching a substring key for substring indexes.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

If the index for the attribute must be protected for security purposes and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate. The property cannot be set on a backend for which confidentiality is not enabled.

Advanced Property

No

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that are allowed to match a given index key before that particular index key is no longer maintained. This is analogous to the ALL IDs threshold in the Sun Java System Directory Server. If this is specified, its value overrides the JE backend-wide configuration. For no limit, use 0 for the value.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

If any index keys have already reached this limit, indexes must be rebuilt before they will be allowed to use the new limit.

Advanced Property

No

Read-only

No

index-extensible-matching-rule

Description

The extensible matching rule in an extensible index. An extensible matching rule must be specified using either LOCALE or OID of the matching rule.

Default Value

No extensible matching rules will be indexed.

Allowed Values

A Locale or an OID.

Multi-valued

Yes

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

No

Read-only

No

index-type

Description

Specifies the type(s) of indexing that should be performed for the associated attribute. For equality, presence, and substring index types, the associated attribute type must have a corresponding matching rule.

Default Value

None

Allowed Values

approximate

This index type is used to improve the efficiency of searches using approximate matching search filters.

equality

This index type is used to improve the efficiency of searches using equality search filters.

extensible

This index type is used to improve the efficiency of searches using extensible matching search filters.

ordering

This index type is used to improve the efficiency of searches using "greater than or equal to" or "less then or equal to" search filters.

presence

This index type is used to improve the efficiency of searches using the presence search filters.

substring

This index type is used to improve the efficiency of searches using substring search filters.

Multi-valued

Yes

Required

Yes

Admin Action Required

If any new index types are added for an attribute, and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate.

Advanced Property

No

Read-only

No

substring-length

Description

The length of substrings in a substring index.

Default Value

6

Allowed Values

An integer value. Lower value is 3.

Multi-valued

No

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-backend-prop(1)

Name

dsconfig set-backend-prop - Modifies Backend properties

Synopsis

`dsconfig set-backend-prop` {options}

Description

Modifies Backend properties.

Options

The `dsconfig set-backend-prop` command takes the following options:

`--backend-name {name}`

The name of the Backend.

Backend properties depend on the Backend type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend types:

`backup-backend`

Default {name}: Backup Backend

Enabled by default: true

See Backup Backend for the properties of this Backend type.

`cas-backend`

Default {name}: CAS Backend

Enabled by default: true

See CAS Backend for the properties of this Backend type.

`jdbc-backend`

Default {name}: JDBC Backend

Enabled by default: true

See JDBC Backend for the properties of this Backend type.

`je-backend`

Default {name}: JE Backend

Enabled by default: true

See JE Backend for the properties of this Backend type.

`ldif-backend`

Default {name}: LDIF Backend

Enabled by default: true

See LDIF Backend for the properties of this Backend type.

`memory-backend`

Default {name}: Memory Backend

Enabled by default: true

See Memory Backend for the properties of this Backend type.

`monitor-backend`

Default {name}: Monitor Backend

Enabled by default: true

See Monitor Backend for the properties of this Backend type.

`null-backend`

Default {name}: Null Backend

Enabled by default: true

See Null Backend for the properties of this Backend type.

`pdb-backend`

Default {name}: PDB Backend

Enabled by default: true

See PDB Backend for the properties of this Backend type.

`schema-backend`

Default {name}: Schema Backend

Enabled by default: true

See Schema Backend for the properties of this Backend type.

`task-backend`

Default {name}: Task Backend

Enabled by default: true

See Task Backend for the properties of this Backend type.

`trust-store-backend`

Default {name}: Trust Store Backend

Enabled by default: true

See Trust Store Backend for the properties of this Backend type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Backend properties depend on the Backend type, which depends on the `--backend-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Backend properties depend on the Backend type, which depends on the `--backend-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Backend properties depend on the Backend type, which depends on the `--backend-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Backend properties depend on the Backend type, which depends on the `--backend-name {name}` option.

Backup Backend

Backends of type backup-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

backup-directory

Description

Specifies the path to a backup directory containing one or more backups for a particular backend. This is a multivalued property. Each value may specify a different backup directory if desired (one for each backend for which backups are taken). Values may be either absolute paths or paths that are relative to the base of the OpenDJ directory server installation.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.BackupBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

CAS Backend

Backends of type cas-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-directory

Description

Specifies the keyspace name The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

ldap_opendj

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search

filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.cassandra.Backend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

JDBC Backend

Backends of type jdbc-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-directory

Description

Specifies the connection string jdbc:postgresql://localhost/test

Default Value

jdbc:postgresql://localhost/test

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.jdbc.Backend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be

more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

JE Backend

Backends of type je-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be

responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-bytes-interval

Description

Specifies the maximum number of bytes that may be written to the database before it is forced to perform a checkpoint. This can be used to bound the recovery time that may be required if the database environment is opened without having been properly closed. If this property is set to a non-zero value, the checkpointer wakeup interval is not used. To use time-based checkpointing, set this property to zero.

Default Value

500mb

Allowed Values

Upper value is 9223372036854775807.

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. Note that this is only used if the value of the checkpointer bytes interval is zero.

Default Value

30s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.Upper limit is 4294 seconds.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-cleaner-min-utilization

Description

Specifies the occupancy percentage for "live" data in this backend's database. When the amount of "live" data in the database drops below this value, cleaners will act to increase the occupancy percentage by compacting the database.

Default Value

50

Allowed Values

An integer value. Lower value is 0. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Berkeley DB Java Edition database files containing the data for this backend. The path may be either an absolute path or a

path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-core-threads

Description

Specifies the core number of threads in the eviction thread pool. Specifies the core number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

1

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-keep-alive

Description

The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

600s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.Upper limit is 86400 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-lru-only

Description

Indicates whether the database should evict existing data from the cache based on an LRU policy (where the least recently used information will be evicted first). If set to "false", then the eviction keeps internal nodes of the underlying Btree in the cache over leaf nodes, even if the leaf nodes have been accessed more recently. This may be a better configuration for databases in which only a very small portion of the data is cached.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-max-threads

Description

Specifies the maximum number of threads in the eviction thread pool. Specifies the maximum number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-nodes-per-scan

Description

Specifies the number of Btree nodes that should be evicted from the cache in a single pass if it is determined that it is necessary to free existing data in order to make room for new information. Changes to this property do not take effect until the backend is restarted. It is recommended that you also change this property when you set db-evictor-lru-only to false. This setting controls the number of Btree nodes that are considered, or sampled, each time a node is evicted. A setting of 10 often produces good results, but this may vary from application to application. The larger the nodes per scan, the more accurate the algorithm. However, don't set it too high. When considering larger numbers of nodes for each eviction, the evictor may delay the completion of a given database operation, which impacts the response time of the application thread. In JE 4.1 and later, setting this value too high in an application that is largely CPU bound can reduce the effectiveness of cache eviction. It's best to start with the default value, and increase it gradually to see if it is beneficial for your application.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 1000.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-file-max

Description

Specifies the maximum size for a database log file.

Default Value

100mb

Allowed Values

Lower value is 1000000.Upper value is 4294967296.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-filecache-size

Description

Specifies the size of the file handle cache. The file handle cache is used to keep as much opened log files as possible. When the cache is smaller than the number of logs, the database needs to close some handles and open log files it needs, resulting in less optimal performances. Ideally, the size of the cache should be higher than the number of files contained in the database. Make sure the OS number of open files per process is also tuned appropriately.

Default Value

100

Allowed Values

An integer value. Lower value is 3. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-file-handler-on

Description

Indicates whether the database should maintain a je.info file in the same directory as the database log directory. This file contains information about the internal processing performed by the underlying database.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-level

Description

Specifies the log level that should be used by the database when it is writing information into the je.info file. The database trace logging level is (in increasing order of verbosity) chosen from: OFF, SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST, ALL.

Default Value

CONFIG

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-cleaner-threads

Description

Specifies the number of threads that the backend should maintain to keep the database log files at or near the desired utilization. In environments with high write throughput, multiple cleaner threads may be required to maintain the desired utilization.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-lock-tables

Description

Specifies the number of lock tables that are used by the underlying database. This can be particularly important to help improve scalability by avoiding contention on systems with large numbers of CPUs. The value of this configuration property should be set to a prime number that is less than or equal to the number of worker threads configured for use in the server.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 32767.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-run-cleaner

Description

Indicates whether the cleaner threads should be enabled to compact the database. The cleaner threads are used to periodically compact the database when it reaches a percentage of occupancy lower than the amount specified by the db-cleaner-min-utilization property. They identify database files with a low percentage of live data, and relocate their remaining live data to the end of the log.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-write-no-sync

Description

Indicates whether the database should synchronously flush data as it is written to disk. If this value is set to "false", then all data written to disk is synchronously flushed to persistent storage and thereby providing full durability. If it is set to "true", then data may be cached for a period of time by the underlying operating system before actually being written to disk. This may improve performance, but could cause the most recent changes to be lost in the event of an underlying OS or hardware failure (but not in the case that the OpenDJ directory server or the JVM exits abnormally).

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by

this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.jeb.JEBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

je-property

Description

Specifies the database and environment properties for the Berkeley DB Java Edition database serving the data for this backend. Any Berkeley DB Java Edition property can be specified using the following form: property-name=property-value. Refer to OpenDJ documentation for further information on related properties, their implications, and range values. The definitive identification of all the property parameters is available in the example.properties file of Berkeley DB Java Edition distribution.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be

more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

LDIF Backend

Backends of type ldif-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be

responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

is-private-backend

Description

Indicates whether the backend should be considered a private backend, which indicates that it is used for storing operational data rather than user-defined information.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.LDIFBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-file

Description

Specifies the path to the LDIF file containing the data for this backend.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Memory Backend

Backends of type memory-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its

contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MemoryBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Monitor Backend

Backends of type monitor-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MonitorBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Null Backend

Backends of type null-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.NullBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

PDB Backend

Backends of type pdb-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents.

Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. This setting controls the elapsed time between attempts to write a checkpoint to the journal. A longer interval allows more updates to accumulate in buffers before they are required to be written to disk, but also potentially causes recovery from an abrupt termination (crash) to take more time.

Default Value

15s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 10 seconds.Upper limit is 3600 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Persistit database files containing the data for this backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

NoneIf any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.pdb.PDBBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be

more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Schema Backend

Backends of type schema-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be

responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.SchemaBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

schema-entry-dn

Description

Defines the base DNs of the subtrees in which the schema information is published in addition to the value included in the base-dn property. The value provided in the base-dn property is the only one that appears in the subschemaSubentry operational attribute of the server's root DSE (which is necessary because that is a single-valued attribute) and as a virtual attribute in other entries. The schema-entry-dn attribute may be used to make the schema information available in other locations to accommodate certain client applications that have been hard-coded to expect the schema to reside in a specific location.

Default Value

cn=schema

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

show-all-attributes

Description

Indicates whether to treat all attributes in the schema entry as if they were user attributes regardless of their configuration. This may provide compatibility with some applications that expect schema attributes like attributeTypes and objectClasses to be included by default even if they are not requested. Note that the ldapSyntaxes attribute is always treated as operational in order to avoid problems with attempts to modify the schema over protocol.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Task Backend

Backends of type task-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.task.TaskBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

notification-sender-address

Description

Specifies the email address to use as the sender (that is, the "From:" address) address for notification mail messages generated when a task completes execution.

Default Value

The default sender address used is "opendj-task-notification@" followed by the canonical address of the system on which the server is running.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

task-backing-file

Description

Specifies the path to the backing file for storing information about the tasks configured in the server. It may be either an absolute path or a relative path to the base of the OpenDJ directory server instance.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

task-retention-time

Description

Specifies the length of time that task entries should be retained after processing on the associated task has been completed.

Default Value

24 hours

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Trust Store Backend

Backends of type trust-store-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

NoneNo administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.TrustStoreBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file that stores the trust information. It may be an absolute path, or a path that is relative to the OpenDJ instance root.

Default Value

config/ads-truststore

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the

clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well.

Default Value

The JVM default value is used.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect the next time that the key manager is accessed.

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-backend-vlv-index-prop(1)

Name

dsconfig set-backend-vlv-index-prop - Modifies Backend VLV Index properties

Synopsis

`dsconfig set-backend-vlv-index-prop` {options}

Description

Modifies Backend VLV Index properties.

Options

The `dsconfig set-backend-vlv-index-prop` command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default {name}: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

`--index-name {name}`

The name of the Backend VLV Index.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

`backend-vlv-index`

Default {name}: Backend VLV Index

Enabled by default: false

See Backend VLV Index for the properties of this Backend VLV Index type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the `--index-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the `--index-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the `--index-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the `--index-name {name}` option.

Backend VLV Index

Backend VLV Indexes of type backend-vlv-index have the following properties:

base-dn

Description

Specifies the base DN used in the search query that is being indexed.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

filter

Description

Specifies the LDAP filter used in the query that is being indexed.

Default Value

None

Allowed Values

A valid LDAP search filter.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

name

Description

Specifies a unique name for this VLV index.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

NoneThe VLV index name cannot be altered after the index is created.

Advanced Property

No

Read-only

Yes

scope

Description

Specifies the LDAP scope of the query that is being indexed.

Default Value

None

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

sort-order

Description

Specifies the names of the attributes that are used to sort the entries for the query being indexed. Multiple attributes can be used to determine the sort order by listing the attribute names from highest to lowest precedence. Optionally, + or - can be prefixed to the attribute name to sort the attribute in ascending order or descending order respectively.

Default Value

None

Allowed Values

Valid attribute types defined in the schema, separated by a space and optionally prefixed by + or -.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

dsconfig set-certificate-mapper-prop(1)

Name

dsconfig set-certificate-mapper-prop - Modifies Certificate Mapper properties

Synopsis

`dsconfig set-certificate-mapper-prop` {options}

Description

Modifies Certificate Mapper properties.

Options

The `dsconfig set-certificate-mapper-prop` command takes the following options:

`--mapper-name {name}`

The name of the Certificate Mapper.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

`fingerprint-certificate-mapper`

Default {name}: Fingerprint Certificate Mapper

Enabled by default: true

See Fingerprint Certificate Mapper for the properties of this Certificate Mapper type.

`subject-attribute-to-user-attribute-certificate-mapper`

Default {name}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See Subject Attribute To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-dn-to-user-attribute-certificate-mapper`

Default {name}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See Subject DN To User Attribute Certificate Mapper for the properties of this Certificate Mapper type.

`subject-equals-dn-certificate-mapper`

Default {name}: Subject Equals DN Certificate Mapper

Enabled by default: true

See Subject Equals DN Certificate Mapper for the properties of this Certificate Mapper type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the `--mapper-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the `--mapper-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the `--mapper-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the `--mapper-name {name}` option.

Fingerprint Certificate Mapper

Certificate Mappers of type fingerprint-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-algorithm

Description

Specifies the name of the digest algorithm to compute the fingerprint of client certificates.

Default Value

None

Allowed Values

md5

Use the MD5 digest algorithm to compute certificate fingerprints.

sha1

Use the SHA-1 digest algorithm to compute certificate fingerprints.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-attribute

Description

Specifies the attribute in which to look for the fingerprint. Values of the fingerprint attribute should exactly match the MD5 or SHA1 representation of the certificate fingerprint.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fingerprint Certificate Mapper implementation.

Default Value

org.opends.server.extensions.FingerprintCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs are used when performing searches to map the client certificates to a user entry.

Default Value

The server performs the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subject Attribute To User Attribute Certificate Mapper

Certificate Mappers of type subject-attribute-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Attribute To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectAttributeToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute-mapping

Description

Specifies a mapping between certificate attributes and user attributes. Each value should be in the form "certattr:userattr" where certattr is the name of the attribute in the certificate subject and userattr is the name of the corresponding attribute in user entries. There may be multiple mappings defined, and when performing the mapping values for all attributes present in the certificate subject that have mappings defined must be present in the corresponding user entries.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subject DN To User Attribute Certificate Mapper

Certificate Mappers of type subject-dn-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject DN To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectDNToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute

Description

Specifies the name or OID of the attribute whose value should exactly match the certificate subject DN.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subject Equals DN Certificate Mapper

Certificate Mappers of type subject-equals-dn-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Equals DN Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectEqualsDNCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-connection-handler-prop(1)

Name

dsconfig set-connection-handler-prop - Modifies Connection Handler properties

Synopsis

`dsconfig set-connection-handler-prop` {options}

Description

Modifies Connection Handler properties.

Options

The `dsconfig set-connection-handler-prop` command takes the following options:

`--handler-name {name}`

The name of the Connection Handler.

Connection Handler properties depend on the Connection Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

`http-connection-handler`

Default {name}: HTTP Connection Handler

Enabled by default: true

See HTTP Connection Handler for the properties of this Connection Handler type.

`jmx-connection-handler`

Default {name}: JMX Connection Handler

Enabled by default: true

See JMX Connection Handler for the properties of this Connection Handler type.

`ldap-connection-handler`

Default {name}: LDAP Connection Handler

Enabled by default: true

See LDAP Connection Handler for the properties of this Connection Handler type.

`ldif-connection-handler`

Default {name}: LDIF Connection Handler

Enabled by default: true

See LDIF Connection Handler for the properties of this Connection Handler type.

`snmp-connection-handler`

Default {name}: SNMP Connection Handler

Enabled by default: true

See SNMP Connection Handler for the properties of this Connection Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Connection Handler properties depend on the Connection Handler type, which depends on the `--handler-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Connection Handler properties depend on the Connection Handler type, which depends on the `--handler-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Connection Handler properties depend on the Connection Handler type, which depends on the `--handler-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Connection Handler properties depend on the Connection Handler type, which depends on the `--handler-name {name}` option.

HTTP Connection Handler

Connection Handlers of type http-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the HTTP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the HTTP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer HTTP

response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that

may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Connection Handler implementation.

Default Value

org.opends.server.protocols.http.HTTPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the HTTP Connection Handler should keep statistics. If enabled, the HTTP Connection Handler maintains statistics about the number and types of operations requested over HTTP and the amount of data sent and received.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this HTTP Connection Handler should listen for connections from HTTP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the HTTP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the HTTP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to HTTP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-concurrent-ops-per-connection

Description

Specifies the maximum number of internal operations that each HTTP client connection can execute concurrently. This property allow to limit the impact that each HTTP request can have on the whole server by limiting the number of internal operations that each HTTP request can execute concurrently. A value of 0 means that no limit is enforced.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest HTTP request message that will be allowed by the HTTP Connection Handler. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The HTTP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the HTTP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the HTTP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the HTTP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the HTTP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the HTTP Connection Handler should use SSL. If enabled, the HTTP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the HTTP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle

client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the HTTP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

JMX Connection Handler

Connection Handlers of type jmx-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any

client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Connection Handler implementation.

Default Value

org.opends.server.protocols.jmx.JmxConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this JMX Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the JMX Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address on which this JMX Connection Handler should listen for connections from JMX clients. If no value is provided, then the JMX Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the JMX Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

rmi-port

Description

Specifies the port number on which the JMX RMI service will listen for connections from clients. A value of 0 indicates the service to choose a port of its own. If the value provided is different than 0, the value will be used as the RMI port. Otherwise, the RMI service will choose a port of its own.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the JMX Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the JMX Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the JMX Connection Handler should use SSL. If enabled, the JMX Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

LDAP Connection Handler

Connection Handlers of type ldap-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-ldap-v2

Description

Indicates whether connections from LDAPv2 clients are allowed. If LDAPv2 clients are allowed, then only a minimal degree of special support are provided for them to ensure that LDAPv3-specific protocol elements (for example, Configuration Guide 25 controls, extended response messages, intermediate response messages, referrals) are not sent to an LDAPv2 client.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-start-tls

Description

Indicates whether clients are allowed to use StartTLS. If enabled, the LDAP Connection Handler allows clients to use the StartTLS extended operation to initiate secure communication over an otherwise insecure channel. Note that this is only allowed if the LDAP Connection Handler is not configured to use SSL, and if the server is configured with a valid key manager provider and a valid trust manager provider.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the LDAP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully

qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the LDAP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer LDAP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDAP Connection Handler implementation.

Default Value

org.opends.server.protocols.ldap.LDAPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the LDAP Connection Handler should keep statistics. If enabled, the LDAP Connection Handler maintains statistics about the number and types of operations requested over LDAP and the amount of data sent and received.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this LDAP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this LDAP Connection Handler should listen for connections from LDAP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the LDAP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the LDAP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to LDAP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest LDAP request message that will be allowed by this LDAP

Connection handler. This property is analogous to the maxBERSize configuration attribute of the Sun Java System Directory Server. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The LDAP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-rejection-notice

Description

Indicates whether the LDAP Connection Handler should send a notice of disconnection extended response message to the client if a new connection is rejected for some reason. The extended response message may provide an explanation indicating the reason that the connection was rejected.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the LDAP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to

retrieve both the public key and the private key. This is only applicable when the LDAP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the LDAP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or StartTLS

communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the LDAP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Connection Handler should use SSL. If enabled, the LDAP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the LDAP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the LDAP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

LDIF Connection Handler

Connection Handlers of type ldif-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDIF Connection Handler implementation.

Default Value

org.opends.server.protocols.LDIFConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-directory

Description

Specifies the path to the directory in which the LDIF files should be placed.

Default Value

config/auto-process-ldif

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

poll-interval

Description

Specifies how frequently the LDIF connection handler should check the LDIF directory to determine whether a new LDIF file has been added.

Default Value

5 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

SNMP Connection Handler

Connection Handlers of type snmp-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

allowed-manager

Description

Specifies the hosts of the managers to be granted the access rights. This property is required for SNMP v1 and v2 security configuration. An asterisk (*) opens access to all managers.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

allowed-user

Description

Specifies the users to be granted the access rights. This property is required for SNMP v3 security

configuration. An asterisk (*) opens access to all users.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

community

Description

Specifies the v1,v2 community or the v3 context name allowed to access the MIB 2605 monitoring information or the USM MIB. The mapping between "community" and "context name" is set.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SNMP Connection Handler implementation.

Default Value

org.opends.server.snmp.SNMPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this SNMP Connection Handler should listen for connections from SNMP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the SNMP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

Yes

listen-port

Description

Specifies the port number on which the SNMP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

opendmk-jarfile

Description

Indicates the OpenDMK runtime jar file location

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

registered-mbean

Description

Indicates whether the SNMP objects have to be registered in the directory server MBeanServer or not allowing to access SNMP Objects with RMI connector if enabled.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-agent-file

Description

Specifies the USM security configuration to receive authenticated only SNMP requests.

Default Value

config/snmp/security/opendj-snmp.security

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-level

Description

Specifies the type of security level : NoAuthNoPriv : No security mechanisms activated, AuthNoPriv : Authentication activated with no privacy, AuthPriv : Authentication with privacy activated. This property is required for SNMP V3 security configuration.

Default Value

authnopriv

Allowed Values

authnopriv

Authentication activated with no privacy.

authpriv

Authentication with privacy activated.

noauthnopriv

No security mechanisms activated.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trap-port

Description

Specifies the port to use to send SNMP Traps.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take

effect

Advanced Property

No

Read-only

No

traps-community

Description

Specifies the community string that must be included in the traps sent to define managers (trap-destinations). This property is used in the context of SNMP v1, v2 and v3.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-destination

Description

Specifies the hosts to which V1 traps will be sent. V1 Traps are sent to every host listed. If this list is empty, V1 traps are sent to "localhost". Each host in the list must be identifed by its name or complete IP Addess.

Default Value

If the list is empty, V1 traps are sent to "localhost".

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig set-crypto-manager-prop(1)

Name

dsconfig set-crypto-manager-prop - Modifies Crypto Manager properties

Synopsis

`dsconfig set-crypto-manager-prop` {options}

Description

Modifies Crypto Manager properties.

Options

The `dsconfig set-crypto-manager-prop` command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Crypto Manager properties depend on the Crypto Manager type, which depends on the null option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Crypto Manager properties depend on the Crypto Manager type, which depends on the null option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Crypto Manager properties depend on the Crypto Manager type, which depends on the null option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Crypto Manager properties depend on the Crypto Manager type, which depends on the null option.

Crypto Manager

Crypto Managers of type crypto-manager have the following properties:

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server using the syntax algorithm/mode/padding. The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

digest-algorithm

Description

Specifies the preferred message digest algorithm for the directory server.

Default Value

SHA-256

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately and only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-wrapping-transformation

Description

The preferred key wrapping transformation for the directory server. This value must be the same for all server instances in a replication topology.

Default Value

RSA/ECB/OAEPWITHSHA-1ANDMGF1PADDING

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect immediately but will only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

mac-algorithm

Description

Specifies the preferred MAC algorithm for the directory server.

Default Value

HmacSHA256

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

mac-key-length

Description

Specifies the key length in bits for the preferred MAC algorithm.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Crypto Manager should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Crypto Manager is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Crypto Manager must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL or TLS communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-encryption

Description

Specifies whether SSL/TLS is used to provide encrypted communication between two OpenDJ server components.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or TLS communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

dsconfig set-debug-target-prop(1)

Name

dsconfig set-debug-target-prop - Modifies Debug Target properties

Synopsis

`dsconfig set-debug-target-prop` {options}

Description

Modifies Debug Target properties.

Options

The `dsconfig set-debug-target-prop` command takes the following options:

`--publisher-name {name}`

The name of the Debug Log Publisher.

Debug Target properties depend on the Debug Target type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default {name}: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

`--target-name {name}`

The name of the Debug Target.

Debug Target properties depend on the Debug Target type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

`debug-target`

Default {name}: Debug Target

Enabled by default: true

See Debug Target for the properties of this Debug Target type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Debug Target properties depend on the Debug Target type, which depends on the `--target-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Debug Target properties depend on the Debug Target type, which depends on the `--target-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Debug Target properties depend on the Debug Target type, which depends on the `--target-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Debug Target properties depend on the Debug Target type, which depends on the `--target-name {name}` option.

Debug Target

Debug Targets of type debug-target have the following properties:

debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

debug-scope

Description

Specifies the fully-qualified OpenDJ Java package, class, or method affected by the settings in this target definition. Use the number character (#) to separate the class name and the method name (that is, org.opends.server.core.DirectoryServer#startUp).

Default Value

None

Allowed Values

The fully-qualified OpenDJ Java package, class, or method name.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the Debug Target is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

include-throwable-cause

Description

Specifies the property to indicate whether to include the cause of exceptions in exception thrown and caught messages.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-entry-arguments

Description

Specifies the property to indicate whether to include method arguments in debug messages.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-return-value

Description

Specifies the property to indicate whether to include the return value in debug messages.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

throwable-stack-frames

Description

Specifies the property to indicate the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

0

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-entry-cache-prop(1)

Name

dsconfig set-entry-cache-prop - Modifies Entry Cache properties

Synopsis

`dsconfig set-entry-cache-prop` {options}

Description

Modifies Entry Cache properties.

Options

The `dsconfig set-entry-cache-prop` command takes the following options:

`--cache-name {name}`

The name of the Entry Cache.

Entry Cache properties depend on the Entry Cache type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

`fifo-entry-cache`

Default {name}: FIFO Entry Cache

Enabled by default: true

See FIFO Entry Cache for the properties of this Entry Cache type.

`soft-reference-entry-cache`

Default {name}: Soft Reference Entry Cache

Enabled by default: true

See Soft Reference Entry Cache for the properties of this Entry Cache type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Entry Cache properties depend on the Entry Cache type, which depends on the `--cache-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Entry Cache properties depend on the Entry Cache type, which depends on the `--cache-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Entry Cache properties depend on the Entry Cache type, which depends on the `--cache-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Entry Cache properties depend on the Entry Cache type, which depends on the `--cache-name {name}` option.

FIFO Entry Cache

Entry Caches of type fifo-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the FIFO Entry Cache implementation.

Default Value

org.opends.server.extensions.FIFOEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time to wait while attempting to acquire a read or write lock.

Default Value

2000.0ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-entries

Description

Specifies the maximum number of entries that we will allow in the cache.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-memory-percent

Description

Specifies the maximum percentage of JVM memory used by the server before the entry caches stops caching and begins purging itself. Very low settings such as 10 or 20 (percent) can prevent this entry cache from having enough space to hold any of the entries to cache, making it appear that the server is ignoring or skipping the entry cache entirely.

Default Value

90

Allowed Values

An integer value. Lower value is 1. Upper value is 100.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Soft Reference Entry Cache

Entry Caches of type soft-reference-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Soft Reference Entry Cache implementation.

Default Value

org.opends.server.extensions.SoftReferenceEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time in milliseconds to wait while attempting to acquire a read or write lock.

Default Value

3000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-extended-operation-handler-prop(1)

Name

dsconfig set-extended-operation-handler-prop - Modifies Extended Operation Handler properties

Synopsis

`dsconfig set-extended-operation-handler-prop` {options}

Description

Modifies Extended Operation Handler properties.

Options

The `dsconfig set-extended-operation-handler-prop` command takes the following options:

`--handler-name {name}`

The name of the Extended Operation Handler.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

`cancel-extended-operation-handler`

Default {name}: Cancel Extended Operation Handler

Enabled by default: true

See Cancel Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-connection-id-extended-operation-handler`

Default {name}: Get Connection Id Extended Operation Handler

Enabled by default: true

See Get Connection Id Extended Operation Handler for the properties of this Extended Operation Handler type.

`get-symmetric-key-extended-operation-handler`

Default {name}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See Get Symmetric Key Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-modify-extended-operation-handler`

Default {name}: Password Modify Extended Operation Handler

Enabled by default: true

See Password Modify Extended Operation Handler for the properties of this Extended Operation Handler type.

`password-policy-state-extended-operation-handler`

Default {name}: Password Policy State Extended Operation Handler

Enabled by default: true

See Password Policy State Extended Operation Handler for the properties of this Extended Operation Handler type.

`start-tls-extended-operation-handler`

Default {name}: Start TLS Extended Operation Handler

Enabled by default: true

See Start TLS Extended Operation Handler for the properties of this Extended Operation Handler type.

`who-am-i-extended-operation-handler`

Default {name}: Who Am I Extended Operation Handler

Enabled by default: true

See Who Am I Extended Operation Handler for the properties of this Extended Operation Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the `--handler-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the `--handler-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the `--handler-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the `--handler-name {name}` option.

Cancel Extended Operation Handler

Extended Operation Handlers of type cancel-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Cancel Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.CancelExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Get Connection Id Extended Operation Handler

Extended Operation Handlers of type get-connection-id-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Connection Id Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.GetConnectionIDExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Get Symmetric Key Extended Operation Handler

Extended Operation Handlers of type get-symmetric-key-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Symmetric Key Extended Operation Handler implementation.

Default Value

org.opends.server.crypto.GetSymmetricKeyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Modify Extended Operation Handler

Extended Operation Handlers of type password-modify-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that should be used in conjunction with the password modify extended operation. This property is used to identify a user based on an authorization ID in the 'u:' form. Changes to this property take effect immediately.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Password Modify Extended Operation Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Modify Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordModifyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Policy State Extended Operation Handler

Extended Operation Handlers of type password-policy-state-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Policy State Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordPolicyStateExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Start TLS Extended Operation Handler

Extended Operation Handlers of type start-tls-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Start TLS Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.StartTLSExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Who Am I Extended Operation Handler

Extended Operation Handlers of type who-am-i-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Who Am I Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.WhoAmIExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-external-changelog-domain-prop(1)

Name

dsconfig set-external-changelog-domain-prop - Modifies External Changelog Domain properties

Synopsis

`dsconfig set-external-changelog-domain-prop` {options}

Description

Modifies External Changelog Domain properties.

Options

The `dsconfig set-external-changelog-domain-prop` command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following External Changelog Domain types:

`external-changelog-domain`

Default {name}: External Changelog Domain

Enabled by default: true

See External Changelog Domain for the properties of this External Changelog Domain type.

`--domain-name {name}`

The name of the Replication Domain.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following External Changelog Domain types:

`external-changelog-domain`

Default {name}: External Changelog Domain

Enabled by default: true

See External Changelog Domain for the properties of this External Changelog Domain type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the `--domain-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the `--domain-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the `--domain-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the `--domain-name {name}` option.

External Changelog Domain

External Changelog Domains of type external-changelog-domain have the following properties:

ecl-include

Description

Specifies a list of attributes which should be published with every change log entry, regardless of whether the attribute itself has changed. The list of attributes may include wild cards such as "*" and "+" as well as object class references prefixed with an ampersand, for example "@person". The included attributes will be published using the "includedAttributes" operational attribute as a single LDIF value rather like the "changes" attribute. For modify and modifyDN operations the included attributes will be taken from the entry before any changes were applied.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ecl-include-for-deletes

Description

Specifies a list of attributes which should be published with every delete operation change log entry, in addition to those specified by the "ecl-include" property. This property provides a means for applications to archive entries after they have been deleted. See the description of the "ecl-include" property for further information about how the included attributes are published.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the External Changelog Domain is enabled. To enable computing the change

numbers, set the Replication Server's "ds-cfg-compute-change-number" property to true.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-global-configuration-prop(1)

Name

dsconfig set-global-configuration-prop - Modifies Global Configuration properties

Synopsis

`dsconfig set-global-configuration-prop` {options}

Description

Modifies Global Configuration properties.

Options

The `dsconfig set-global-configuration-prop` command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Global Configuration properties depend on the Global Configuration type, which depends on the null option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Global Configuration properties depend on the Global Configuration type, which depends on the null option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Global Configuration properties depend on the Global Configuration type, which depends on the null option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Global Configuration properties depend on the Global Configuration type, which depends on the null option.

Global Configuration

Global Configurations of type global have the following properties:

add-missing-rdn-attributes

Description

Indicates whether the directory server should automatically add any attribute values contained in the entry's RDN into that entry when processing an add request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-attribute-name-exceptions

Description

Indicates whether the directory server should allow underscores in attribute names and allow attribute names to begin with numeric digits (both of which are violations of the LDAP standards).

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-task

Description

Specifies the fully-qualified name of a Java class that may be invoked in the server. Any attempt to invoke a task not included in the list of allowed tasks is rejected.

Default Value

If no values are defined, then the server does not allow any tasks to be invoked.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

bind-with-dn-requires-password

Description

Indicates whether the directory server should reject any simple bind request that contains a DN but no password. Although such bind requests are technically allowed by the LDAPv3 specification (and should be treated as anonymous simple authentication), they may introduce security problems in applications that do not verify that the client actually provided a password.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-schema

Description

Indicates whether schema enforcement is active. When schema enforcement is activated, the directory server ensures that all operations result in entries are valid according to the defined server schema. It is strongly recommended that this option be left enabled to prevent the inadvertent addition of invalid data into the server.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-password-policy

Description

Specifies the name of the password policy that is in effect for users whose entries do not specify an alternate password policy (either via a real or virtual attribute). In addition, the default password policy will be used for providing default parameters for sub-entry based password policies when not provided or supported by the sub-entry itself. This property must reference a password policy and no other type of authentication policy.

Default Value

None

Allowed Values

The DN of any Password Policy.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

disabled-privilege

Description

Specifies the name of a privilege that should not be evaluated by the server. If a privilege is disabled, then it is assumed that all clients (including unauthenticated clients) have that privilege.

Default Value

If no values are defined, then the server enforces all privileges.

Allowed Values

backend-backup

Allows the user to request that the server process backup tasks.

backend-restore

Allows the user to request that the server process restore tasks.

bypass-acl

Allows the associated user to bypass access control checks performed by the server.

bypass-lockdown

Allows the associated user to bypass server lockdown mode.

cancel-request

Allows the user to cancel operations in progress on other client connections.

changelog-read

The privilege that provides the ability to perform read operations on the changelog

config-read

Allows the associated user to read the server configuration.

config-write

Allows the associated user to update the server configuration. The config-read privilege is also required.

data-sync

Allows the user to participate in data synchronization.

disconnect-client

Allows the user to terminate other client connections.

jmx-notify

Allows the associated user to subscribe to receive JMX notifications.

jmx-read

Allows the associated user to perform JMX read operations.

jmx-write

Allows the associated user to perform JMX write operations.

ldif-export

Allows the user to request that the server process LDIF export tasks.

ldif-import

Allows the user to request that the server process LDIF import tasks.

modify-acl

Allows the associated user to modify the server's access control configuration.

password-reset

Allows the user to reset user passwords.

privilege-change

Allows the user to make changes to the set of defined root privileges, as well as to grant and revoke privileges for users.

proxied-auth

Allows the user to use the proxied authorization control, or to perform a bind that specifies an alternate authorization identity.

server-lockdown

Allows the user to place and bring the server of lockdown mode.

server-restart

Allows the user to request that the server perform an in-core restart.

server-shutdown

Allows the user to request that the server shut down.

subentry-write

Allows the associated user to perform LDAP subentry write operations.

unindexed-search

Allows the user to request that the server process a search that cannot be optimized using server indexes.

update-schema

Allows the user to make changes to the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

etime-resolution

Description

Specifies the resolution to use for operation elapsed processing time (etime) measurements.

Default Value

milliseconds

Allowed Values

milliseconds

Use millisecond resolution.

nanoseconds

Use nanosecond resolution.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

idle-time-limit

Description

Specifies the maximum length of time that a client connection may remain established since its last completed operation. A value of "0 seconds" indicates that no idle time limit is enforced.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

invalid-attribute-syntax-behavior

Description

Specifies how the directory server should handle operations whenever an attribute value violates the associated attribute syntax.

Default Value

reject

Allowed Values

accept

The directory server silently accepts attribute values that are invalid according to their associated syntax. Matching operations targeting those values may not behave as expected.

reject

The directory server rejects attribute values that are invalid according to their associated syntax.

warn

The directory server accepts attribute values that are invalid according to their associated syntax, but also logs a warning message to the error log. Matching operations targeting those values may not behave as expected.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lookthrough-limit

Description

Specifies the maximum number of entries that the directory server should "look through" in the course of processing a search request. This includes any entry that the server must examine in the course of processing the request, regardless of whether it actually matches the search criteria. A value of 0 indicates that no lookthrough limit is enforced. Note that this is the default server-wide limit, but it may be overridden on a per-user basis using the ds-rlim-lookthrough-

limit operational attribute.

Default Value

5000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-allowed-client-connections

Description

Specifies the maximum number of client connections that may be established at any given time A value of 0 indicates that unlimited client connection is allowed.

Default Value

0

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-internal-buffer-size

Description

The threshold capacity beyond which internal cached buffers used for encoding and decoding entries and protocol messages will be trimmed after use. Individual buffers may grow very large when encoding and decoding large entries and protocol messages and should be reduced in size when they are no longer needed. This setting specifies the threshold at which a buffer is determined to have grown too big and should be trimmed down after use.

Default Value

32 KB

Allowed Values

Lower value is 512.Upper value is 1000000000.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-psearches

Description

Defines the maximum number of concurrent persistent searches that can be performed on directory server The persistent search mechanism provides an active channel through which entries that change, and information about the changes that occur, can be communicated. Because each persistent search operation consumes resources, limiting the number of simultaneous persistent searches keeps the performance impact minimal. A value of -1 indicates that there is no limit on the persistent searches.

Default Value

-1

Allowed Values

An integer value. Lower value is 0. A value of "-1" or "unlimited" for no limit.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

notify-abandoned-operations

Description

Indicates whether the directory server should send a response to any operation that is interrupted via an abandon request. The LDAP specification states that abandoned operations should not receive any response, but this may cause problems with client applications that always expect to receive a response to each request.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

proxied-authorization-identity-mapper

Description

Specifies the name of the identity mapper to map authorization ID values (using the "u:" form)

provided in the proxied authorization control to the corresponding user entry.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

reject-unauthenticated-requests

Description

Indicates whether the directory server should reject any request (other than bind or StartTLS requests) received from a client that has not yet been authenticated, whose last authentication attempt was unsuccessful, or whose last authentication attempt used anonymous authentication.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

return-bind-error-messages

Description

Indicates whether responses for failed bind operations should include a message string providing the reason for the authentication failure. Note that these messages may include information that could potentially be used by an attacker. If this option is disabled, then these messages appears only in the server's access log.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

save-config-on-successful-startup

Description

Indicates whether the directory server should save a copy of its configuration whenever the startup process completes successfully. This ensures that the server provides a "last known good" configuration, which can be used as a reference (or copied into the active config) if the server fails to start with the current "active" configuration.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-error-result-code

Description

Specifies the numeric value of the result code when request processing fails due to an internal server error.

Default Value

80

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

single-structural-objectclass-behavior

Description

Specifies how the directory server should handle operations an entry does not contain a structural object class or contains multiple structural classes.

Default Value

reject

Allowed Values

accept

The directory server silently accepts entries that do not contain exactly one structural object class. Certain schema features that depend on the entry's structural class may not behave as expected.

reject

The directory server rejects entries that do not contain exactly one structural object class.

warn

The directory server accepts entries that do not contain exactly one structural object class, but also logs a warning message to the error log. Certain schema features that depend on the entry's structural class may not behave as expected.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

size-limit

Description

Specifies the maximum number of entries that can be returned to the client during a single search operation. A value of 0 indicates that no size limit is enforced. Note that this is the default server-wide limit, but it may be overridden on a per-user basis using the ds-rlim-size-limit operational attribute.

Default Value

1000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

smtp-server

Description

Specifies the address (and optional port number) for a mail server that can be used to send email messages via SMTP. It may be an IP address or resolvable hostname, optionally followed by a colon and a port number.

Default Value

If no values are defined, then the server cannot send email via SMTP.

Allowed Values

A hostname, optionally followed by a ":" followed by a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

subordinate-base-dn

Description

Specifies the set of base DNs used for singleLevel, wholeSubtree, and subordinateSubtree searches based at the root DSE.

Default Value

The set of all user-defined suffixes is used.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-limit

Description

Specifies the maximum length of time that should be spent processing a single search operation. A value of 0 seconds indicates that no time limit is enforced. Note that this is the default server-wide time limit, but it may be overridden on a per-user basis using the ds-rlim-time-limit operational attribute.

Default Value

60 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-transaction-ids

Description

Indicates whether the directory server should trust the transaction ids that may be received

from requests, either through a LDAP control or through a HTTP header.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the kinds of write operations the directory server can process.

Default Value

enabled

Allowed Values

disabled

The directory server rejects all write operations that are requested of it, regardless of their origin.

enabled

The directory server attempts to process all write operations that are requested of it, regardless of their origin.

internal-only

The directory server attempts to process write operations requested as internal operations or through synchronization, but rejects any such operations requested from external clients.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-group-implementation-prop(1)

Name

dsconfig set-group-implementation-prop - Modifies Group Implementation properties

Synopsis

`dsconfig set-group-implementation-prop` {options}

Description

Modifies Group Implementation properties.

Options

The `dsconfig set-group-implementation-prop` command takes the following options:

`--implementation-name {name}`

The name of the Group Implementation.

Group Implementation properties depend on the Group Implementation type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

`dynamic-group-implementation`

Default {name}: Dynamic Group Implementation

Enabled by default: true

See Dynamic Group Implementation for the properties of this Group Implementation type.

`static-group-implementation`

Default {name}: Static Group Implementation

Enabled by default: true

See Static Group Implementation for the properties of this Group Implementation type.

`virtual-static-group-implementation`

Default {name}: Virtual Static Group Implementation

Enabled by default: true

See Virtual Static Group Implementation for the properties of this Group Implementation type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Group Implementation properties depend on the Group Implementation type, which depends on the `--implementation-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Group Implementation properties depend on the Group Implementation type, which depends on the `--implementation-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Group Implementation properties depend on the Group Implementation type, which depends on the `--implementation-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Group Implementation properties depend on the Group Implementation type, which depends on the `--implementation-name {name}` option.

Dynamic Group Implementation

Group Implementations of type dynamic-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Dynamic Group Implementation implementation.

Default Value

org.opends.server.extensions.DynamicGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Static Group Implementation

Group Implementations of type static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Group Implementation implementation.

Default Value

org.opends.server.extensions.StaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Virtual Static Group Implementation

Group Implementations of type virtual-static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Virtual Static Group Implementation implementation.

Default Value

org.opends.server.extensions.VirtualStaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-http-authorization-mechanism-prop(1)

Name

dsconfig set-http-authorization-mechanism-prop - Modifies HTTP Authorization Mechanism properties

Synopsis

`dsconfig set-http-authorization-mechanism-prop` {options}

Description

Modifies HTTP Authorization Mechanism properties.

Options

The `dsconfig set-http-authorization-mechanism-prop` command takes the following options:

`--mechanism-name {name}`

The name of the HTTP Authorization Mechanism.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

`http-anonymous-authorization-mechanism`

Default {name}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See HTTP Anonymous Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-basic-authorization-mechanism`

Default {name}: HTTP Basic Authorization Mechanism

Enabled by default: true

See HTTP Basic Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-cts-authorization-mechanism`

Default {name}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Cts Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-file-authorization-mechanism`

Default {name}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 File Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-openam-authorization-mechanism`

Default {name}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Openam Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`http-oauth2-token-introspection-authorization-mechanism`

Default {name}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See HTTP Oauth2 Token Introspection Authorization Mechanism for the properties of this HTTP Authorization Mechanism type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the `--mechanism-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the `--mechanism-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the `--mechanism-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the `--mechanism-name {name}` option.

HTTP Anonymous Authorization Mechanism

HTTP Authorization Mechanisms of type http-anonymous-authorization-mechanism have the following properties:

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Anonymous Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpAnonymousAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-dn

Description

The authorization DN which will be used for performing anonymous operations.

Default Value

By default, operations will be performed using an anonymously bound connection.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

HTTP Basic Authorization Mechanism

HTTP Authorization Mechanisms of type http-basic-authorization-mechanism have the following properties:

alt-authentication-enabled

Description

Specifies whether user credentials may be provided using alternative headers to the standard 'Authorize' header.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-password-header

Description

Alternate HTTP headers to get the user's password from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-username-header

Description

Alternate HTTP headers to get the user's name from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper used to get the user's entry corresponding to the user-id provided in the HTTP authentication header.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Basic Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Basic Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpBasicAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

HTTP Oauth2 Cts Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-cts-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

The base DN of the Core Token Service where access token are stored. (example: ou=famrecords,ou=openam-session,ou=tokens,dc=example,dc=com)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Cts Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2CtsAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

HTTP Oauth2 File Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-file-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-directory

Description

Directory containing token files. File names must be equal to the token strings. The file content must a JSON object with the following attributes: 'scope', 'expireTime' and all the field(s) needed to resolve the authzIdTemplate.

Default Value

oauth2-demo/

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 File Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2FileAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

HTTP Oauth2 Openam Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-openam-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Openam Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2OpenAmAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Openam Authorization Mechanism .

Default Value

By default the system key manager(s) will be used.

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-info-url

Description

Defines the OpenAM endpoint URL where the access-token resolution request should be sent.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

HTTP Oauth2 Token Introspection Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-token-introspection-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-id

Description

Client's ID to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-secret

Description

Client's secret to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Token Introspection Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2TokenIntrospectionAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Token Introspection Authorization Mechanism .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-introspection-url

Description

Defines the token introspection endpoint URL where the access-token resolution request should be sent. (example: http://example.com/introspect)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

dsconfig set-http-endpoint-prop(1)

Name

dsconfig set-http-endpoint-prop - Modifies HTTP Endpoint properties

Synopsis

`dsconfig set-http-endpoint-prop` {options}

Description

Modifies HTTP Endpoint properties.

Options

The `dsconfig set-http-endpoint-prop` command takes the following options:

`--endpoint-name {name}`

The name of the HTTP Endpoint.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

`admin-endpoint`

Default {name}: Admin Endpoint

Enabled by default: true

See Admin Endpoint for the properties of this HTTP Endpoint type.

`rest2ldap-endpoint`

Default {name}: Rest2ldap Endpoint

Enabled by default: true

See Rest2ldap Endpoint for the properties of this HTTP Endpoint type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the `--endpoint-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the `--endpoint-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the `--endpoint-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the `--endpoint-name {name}` option.

Admin Endpoint

HTTP Endpoints of type admin-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Admin Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.AdminEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Rest2ldap Endpoint

HTTP Endpoints of type rest2ldap-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

config-directory

Description

The directory containing the Rest2Ldap configuration file(s) for this specific endpoint. The directory must be readable by the server and may contain multiple configuration files, one for each supported version of the REST endpoint. If a relative path is used then it will be resolved against the server's instance directory.

Default Value

None

Allowed Values

A directory that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Rest2ldap Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.Rest2LdapEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-identity-mapper-prop(1)

Name

dsconfig set-identity-mapper-prop - Modifies Identity Mapper properties

Synopsis

`dsconfig set-identity-mapper-prop` {options}

Description

Modifies Identity Mapper properties.

Options

The `dsconfig set-identity-mapper-prop` command takes the following options:

`--mapper-name {name}`

The name of the Identity Mapper.

Identity Mapper properties depend on the Identity Mapper type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

`exact-match-identity-mapper`

Default {name}: Exact Match Identity Mapper

Enabled by default: true

See Exact Match Identity Mapper for the properties of this Identity Mapper type.

`regular-expression-identity-mapper`

Default {name}: Regular Expression Identity Mapper

Enabled by default: true

See Regular Expression Identity Mapper for the properties of this Identity Mapper type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Identity Mapper properties depend on the Identity Mapper type, which depends on the `--mapper-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Identity Mapper properties depend on the Identity Mapper type, which depends on the `--mapper-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Identity Mapper properties depend on the Identity Mapper type, which depends on the `--mapper-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Identity Mapper properties depend on the Identity Mapper type, which depends on the `--mapper-name {name}` option.

Exact Match Identity Mapper

Identity Mappers of type exact-match-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Exact Match Identity Mapper implementation.

Default Value

org.opends.server.extensions.ExactMatchIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the attribute whose value should exactly match the ID string provided to this identity mapper. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry. The internal search performed includes a logical OR across all of these values.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs will be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Regular Expression Identity Mapper

Identity Mappers of type regular-expression-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Regular Expression Identity Mapper implementation.

Default Value

org.opends.server.extensions.RegularExpressionIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name or OID of the attribute whose value should match the provided identifier string after it has been processed by the associated regular expression. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the base DN(s) that should be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all the specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

match-pattern

Description

Specifies the regular expression pattern that is used to identify portions of the ID string that will be replaced. Any portion of the ID string that matches this pattern is replaced in accordance with the provided replace pattern (or is removed if no replace pattern is specified). If multiple substrings within the given ID string match this pattern, all occurrences are replaced. If no part of the given ID string matches this pattern, the ID string is not altered. Exactly one match pattern value must be provided, and it must be a valid regular expression as described in the API documentation for the java.util.regex.Pattern class, including support for capturing groups.

Default Value

None

Allowed Values

Any valid regular expression pattern which is supported by the javax.util.regex.Pattern class (see http://download.oracle.com/docs/cd/E17409_01/javase/6/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 6).

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replace-pattern

Description

Specifies the replacement pattern that should be used for substrings in the ID string that match the provided regular expression pattern. If no replacement pattern is provided, then any

matching portions of the ID string will be removed (i.e., replaced with an empty string). The replacement pattern may include a string from a capturing group by using a dollar sign ($) followed by an integer value that indicates which capturing group should be used.

Default Value

The replace pattern will be the empty string.

Allowed Values

Any valid replacement string that is allowed by the javax.util.regex.Matcher class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-key-manager-provider-prop(1)

Name

dsconfig set-key-manager-provider-prop - Modifies Key Manager Provider properties

Synopsis

`dsconfig set-key-manager-provider-prop` {options}

Description

Modifies Key Manager Provider properties.

Options

The `dsconfig set-key-manager-provider-prop` command takes the following options:

`--provider-name {name}`

The name of the Key Manager Provider.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

`file-based-key-manager-provider`

Default {name}: File Based Key Manager Provider

Enabled by default: true

See File Based Key Manager Provider for the properties of this Key Manager Provider type.

`ldap-key-manager-provider`

Default {name}: LDAP Key Manager Provider

Enabled by default: true

See LDAP Key Manager Provider for the properties of this Key Manager Provider type.

`pkcs11-key-manager-provider`

Default {name}: PKCS11 Key Manager Provider

Enabled by default: true

See PKCS11 Key Manager Provider for the properties of this Key Manager Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the `--provider-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the `--provider-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the `--provider-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the `--provider-name {name}` option.

File Based Key Manager Provider

Key Manager Providers of type file-based-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Key Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well. If no value is provided, the JVM-default value is used. Changes to this configuration attribute will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

LDAP Key Manager Provider

Key Manager Providers of type ldap-key-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Key Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

PKCS11 Key Manager Provider

Key Manager Providers of type pkcs11-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Key Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11KeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig set-log-publisher-prop(1)

Name

dsconfig set-log-publisher-prop - Modifies Log Publisher properties

Synopsis

`dsconfig set-log-publisher-prop` {options}

Description

Modifies Log Publisher properties.

Options

The `dsconfig set-log-publisher-prop` command takes the following options:

`--publisher-name {name}`

The name of the Log Publisher.

Log Publisher properties depend on the Log Publisher type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

`csv-file-access-log-publisher`

Default {name}: Csv File Access Log Publisher

Enabled by default: true

See Csv File Access Log Publisher for the properties of this Log Publisher type.

`csv-file-http-access-log-publisher`

Default {name}: Csv File HTTP Access Log Publisher

Enabled by default: true

See Csv File HTTP Access Log Publisher for the properties of this Log Publisher type.

`external-access-log-publisher`

Default {name}: External Access Log Publisher

Enabled by default: true

See External Access Log Publisher for the properties of this Log Publisher type.

`external-http-access-log-publisher`

Default {name}: External HTTP Access Log Publisher

Enabled by default: true

See External HTTP Access Log Publisher for the properties of this Log Publisher type.

`file-based-access-log-publisher`

Default {name}: File Based Access Log Publisher

Enabled by default: true

See File Based Access Log Publisher for the properties of this Log Publisher type.

`file-based-audit-log-publisher`

Default {name}: File Based Audit Log Publisher

Enabled by default: true

See File Based Audit Log Publisher for the properties of this Log Publisher type.

`file-based-debug-log-publisher`

Default {name}: File Based Debug Log Publisher

Enabled by default: true

See File Based Debug Log Publisher for the properties of this Log Publisher type.

`file-based-error-log-publisher`

Default {name}: File Based Error Log Publisher

Enabled by default: true

See File Based Error Log Publisher for the properties of this Log Publisher type.

`file-based-http-access-log-publisher`

Default {name}: File Based HTTP Access Log Publisher

Enabled by default: true

See File Based HTTP Access Log Publisher for the properties of this Log Publisher type.

`json-file-access-log-publisher`

Default {name}: Json File Access Log Publisher

Enabled by default: true

See Json File Access Log Publisher for the properties of this Log Publisher type.

`json-file-http-access-log-publisher`

Default {name}: Json File HTTP Access Log Publisher

Enabled by default: true

See Json File HTTP Access Log Publisher for the properties of this Log Publisher type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Log Publisher properties depend on the Log Publisher type, which depends on the `--publisher-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Log Publisher properties depend on the Log Publisher type, which depends on the `--publisher-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Log Publisher properties depend on the Log Publisher type, which depends on the `--publisher-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Log Publisher properties depend on the Log Publisher type, which depends on the `--publisher-name {name}` option.

Csv File Access Log Publisher

Log Publishers of type csv-file-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writting in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CsvFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Csv File Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when the tamper-evident option is enabled.

Default Value

3s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Csv File HTTP Access Log Publisher

Log Publishers of type csv-file-http-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File HTTP Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the Csv File HTTP Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when secure option is enabled.

Default Value

3s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

External Access Log Publisher

Log Publishers of type external-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External Access Log Publisher implementation.

Default Value

org.opends.server.loggers.ExternalAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

External HTTP Access Log Publisher

Log Publishers of type external-http-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External HTTP Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Access Log Publisher

Log Publishers of type file-based-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the access log.

Default Value

multi-line

Allowed Values

combined

Combine log records for operation requests and responses into a single record. This format should be used when log records are to be filtered based on response criteria (e.g. result code).

multi-line

Outputs separate log records for operation requests and responses.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Audit Log Publisher

Log Publishers of type file-based-audit-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Audit Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Audit Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAuditLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Audit Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Audit Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Audit Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Audit Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Debug Log Publisher

Log Publishers of type file-based-debug-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Debug Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-include-throwable-cause

Description

Indicates whether to include the cause of exceptions in exception thrown and caught messages logged by default.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-entry-arguments

Description

Indicates whether to include method arguments in debug messages logged by default.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-return-value

Description

Indicates whether to include the return value in debug messages logged by default.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-throwable-stack-frames

Description

Indicates the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Debug Log Publisher implementation.

Default Value

org.opends.server.loggers.TextDebugLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Debug Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Debug Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Debug Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Debug Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Error Log Publisher

Log Publishers of type file-based-error-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Error Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer will be flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-severity

Description

Specifies the default severity levels for the logger.

Default Value

error warning

Allowed Values

all

Messages of all severity levels are logged.

debug

The error log severity that is used for messages that provide debugging information triggered during processing.

error

The error log severity that is used for messages that provide information about errors which may force the server to shut down or operate in a significantly degraded state.

info

The error log severity that is used for messages that provide information about significant events within the server that are not warnings or errors.

none

No messages of any severity are logged by default. This value is intended to be used in conjunction with the override-severity property to define an error logger that will publish no error message beside the errors of a given category.

notice

The error log severity that is used for the most important informational messages (i.e., information that should almost always be logged but is not associated with a warning or error condition).

warning

The error log severity that is used for messages that provide information about warnings triggered during processing.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Error Log Publisher implementation.

Default Value

org.opends.server.loggers.TextErrorLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Error Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Error Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

override-severity

Description

Specifies the override severity levels for the logger based on the category of the messages. Each override severity level should include the category and the severity levels to log for that category, for example, core=error,info,warning. Valid categories are: core, extensions, protocol, config, log, util, schema, plugin, jeb, backend, tools, task, access-control, admin, sync, version, quicksetup, admin-tool, dsconfig, user-defined. Valid severities are: all, error, info, warning, notice, debug.

Default Value

All messages with the default severity levels are logged.

Allowed Values

A string in the form category=severity1,severity2...

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Error Log Publisher . When multiple policies are used, log files will be cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files will never be cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Error Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based HTTP Access Log Publisher

Log Publishers of type file-based-http-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based HTTP Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based HTTP Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the HTTP access log.

Default Value

cs-host c-ip cs-username x-datetime cs-method cs-uri-stem cs-uri-query cs-version sc-status cs(User-Agent) x-connection-id x-etime x-transaction-id

Allowed Values

A space separated list of fields describing the extended log format to be used for logging HTTP accesses. Available values are listed on the W3C working draft http://www.w3.org/TR/WD-logfile.html and Microsoft website http://www.microsoft.com/technet/prodtechnol/

WindowsServer2003/Library/IIS/676400bc-8969-4aa7-851a-9319490a9bbb.mspx?mfr=true
OpenDJ supports the following standard fields: "c-ip", "c-port", "cs-host", "cs-method", "cs-uri", "cs-uri-stem", "cs-uri-query", "cs(User-Agent)", "cs-username", "cs-version", "s-computername", "s-ip", "s-port", "sc-status". OpenDJ supports the following application specific field extensions: "x-connection-id" displays the internal connection ID assigned to the HTTP client connection, "x-datetime" displays the completion date and time for the logged HTTP request and its ouput is controlled by the "ds-cfg-log-record-time-format" property, "x-etime" displays the total execution time for the logged HTTP request, "x-transaction-id" displays the transaction id associated to a request

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Json File Access Log Publisher

Log Publishers of type json-file-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.JsonFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Json File HTTP Access Log Publisher

Log Publishers of type json-file-http-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-log-retention-policy-prop(1)

Name

dsconfig set-log-retention-policy-prop - Modifies Log Retention Policy properties

Synopsis

`dsconfig set-log-retention-policy-prop` {options}

Description

Modifies Log Retention Policy properties.

Options

The `dsconfig set-log-retention-policy-prop` command takes the following options:

`--policy-name {name}`

The name of the Log Retention Policy.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

`file-count-log-retention-policy`

Default {name}: File Count Log Retention Policy

Enabled by default: false

See File Count Log Retention Policy for the properties of this Log Retention Policy type.

`free-disk-space-log-retention-policy`

Default {name}: Free Disk Space Log Retention Policy

Enabled by default: false

See Free Disk Space Log Retention Policy for the properties of this Log Retention Policy type.

`size-limit-log-retention-policy`

Default {name}: Size Limit Log Retention Policy

Enabled by default: false

See Size Limit Log Retention Policy for the properties of this Log Retention Policy type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the `--policy-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the `--policy-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the `--policy-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the `--policy-name {name}` option.

File Count Log Retention Policy

Log Retention Policies of type file-count-log-retention-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the File Count Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FileNumberRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

number-of-files

Description

Specifies the number of archived log files to retain before the oldest ones are cleaned.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Free Disk Space Log Retention Policy

Log Retention Policies of type free-disk-space-log-retention-policy have the following properties:

free-disk-space

Description

Specifies the minimum amount of free disk space that should be available on the file system on which the archived log files are stored.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Free Disk Space Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FreeDiskSpaceRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Size Limit Log Retention Policy

Log Retention Policies of type size-limit-log-retention-policy have the following properties:

disk-space-used

Description

Specifies the maximum total disk space used by the log files.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Retention Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-log-rotation-policy-prop(1)

Name

dsconfig set-log-rotation-policy-prop - Modifies Log Rotation Policy properties

Synopsis

`dsconfig set-log-rotation-policy-prop` {options}

Description

Modifies Log Rotation Policy properties.

Options

The `dsconfig set-log-rotation-policy-prop` command takes the following options:

`--policy-name {name}`

The name of the Log Rotation Policy.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

`fixed-time-log-rotation-policy`

Default {name}: Fixed Time Log Rotation Policy

Enabled by default: false

See Fixed Time Log Rotation Policy for the properties of this Log Rotation Policy type.

`size-limit-log-rotation-policy`

Default {name}: Size Limit Log Rotation Policy

Enabled by default: false

See Size Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`time-limit-log-rotation-policy`

Default {name}: Time Limit Log Rotation Policy

Enabled by default: false

See Time Limit Log Rotation Policy for the properties of this Log Rotation Policy type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the `--policy-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the `--policy-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the `--policy-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the `--policy-name {name}` option.

Fixed Time Log Rotation Policy

Log Rotation Policies of type fixed-time-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fixed Time Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.FixedTimeRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-of-day

Description

Specifies the time of day at which log rotation should occur.

Default Value

None

Allowed Values

24 hour time of day in HHmm format.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Size Limit Log Rotation Policy

Log Rotation Policies of type size-limit-log-rotation-policy have the following properties:

file-size-limit

Description

Specifies the maximum size that a log file can reach before it is rotated.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Time Limit Log Rotation Policy

Log Rotation Policies of type time-limit-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Time Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.TimeLimitRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

rotation-interval

Description

Specifies the time interval between rotations.

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-monitor-provider-prop(1)

Name

dsconfig set-monitor-provider-prop - Modifies Monitor Provider properties

Synopsis

`dsconfig set-monitor-provider-prop` {options}

Description

Modifies Monitor Provider properties.

Options

The `dsconfig set-monitor-provider-prop` command takes the following options:

`--provider-name {name}`

The name of the Monitor Provider.

Monitor Provider properties depend on the Monitor Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

`client-connection-monitor-provider`

Default {name}: Client Connection Monitor Provider

Enabled by default: true

See Client Connection Monitor Provider for the properties of this Monitor Provider type.

`entry-cache-monitor-provider`

Default {name}: Entry Cache Monitor Provider

Enabled by default: true

See Entry Cache Monitor Provider for the properties of this Monitor Provider type.

`memory-usage-monitor-provider`

Default {name}: Memory Usage Monitor Provider

Enabled by default: true

See Memory Usage Monitor Provider for the properties of this Monitor Provider type.

`stack-trace-monitor-provider`

Default {name}: Stack Trace Monitor Provider

Enabled by default: true

See Stack Trace Monitor Provider for the properties of this Monitor Provider type.

`system-info-monitor-provider`

Default {name}: System Info Monitor Provider

Enabled by default: true

See System Info Monitor Provider for the properties of this Monitor Provider type.

`version-monitor-provider`

Default {name}: Version Monitor Provider

Enabled by default: true

See Version Monitor Provider for the properties of this Monitor Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Monitor Provider properties depend on the Monitor Provider type, which depends on the `--provider-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Monitor Provider properties depend on the Monitor Provider type, which depends on the `--provider-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Monitor Provider properties depend on the Monitor Provider type, which depends on the `--provider-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Monitor Provider properties depend on the Monitor Provider type, which depends on the `--provider-name {name}` option.

Client Connection Monitor Provider

Monitor Providers of type client-connection-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Client Connection Monitor Provider implementation.

Default Value

org.opends.server.monitors.ClientConnectionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Entry Cache Monitor Provider

Monitor Providers of type entry-cache-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Entry Cache Monitor Provider implementation.

Default Value

org.opends.server.monitors.EntryCacheMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Memory Usage Monitor Provider

Monitor Providers of type memory-usage-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Memory Usage Monitor Provider implementation.

Default Value

org.opends.server.monitors.MemoryUsageMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Stack Trace Monitor Provider

Monitor Providers of type stack-trace-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Stack Trace Monitor Provider implementation.

Default Value

org.opends.server.monitors.StackTraceMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

System Info Monitor Provider

Monitor Providers of type system-info-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the System Info Monitor Provider implementation.

Default Value

org.opends.server.monitors.SystemInfoMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Version Monitor Provider

Monitor Providers of type version-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Version Monitor Provider implementation.

Default Value

org.opends.server.monitors.VersionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-password-generator-prop(1)

Name

dsconfig set-password-generator-prop - Modifies Password Generator properties

Synopsis

`dsconfig set-password-generator-prop` {options}

Description

Modifies Password Generator properties.

Options

The `dsconfig set-password-generator-prop` command takes the following options:

`--generator-name {name}`

The name of the Password Generator.

Password Generator properties depend on the Password Generator type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

`random-password-generator`

Default {name}: Random Password Generator

Enabled by default: true

See Random Password Generator for the properties of this Password Generator type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Password Generator properties depend on the Password Generator type, which depends on the `--generator-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Password Generator properties depend on the Password Generator type, which depends on the `--generator-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Password Generator properties depend on the Password Generator type, which depends on the `--generator-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Password Generator properties depend on the Password Generator type, which depends on the `--generator-name {name}` option.

Random Password Generator

Password Generators of type random-password-generator have the following properties:

enabled

Description

Indicates whether the Password Generator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Random Password Generator implementation.

Default Value

org.opends.server.extensions.RandomPasswordGenerator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordGenerator

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

password-character-set

Description

Specifies one or more named character sets. This is a multi-valued property, with each value defining a different character set. The format of the character set is the name of the set followed by a colon and the characters that are in that set. For example, the value "alpha:abcdefghijklmnopqrstuvwxyz" defines a character set named "alpha" containing all of the lower-case ASCII alphabetic characters.

Default Value

None

Allowed Values

A character set name (consisting of ASCII letters) followed by a colon and the set of characters that are included in that character set.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-format

Description

Specifies the format to use for the generated password. The value is a comma-delimited list of elements in which each of those elements is comprised of the name of a character set defined in the password-character-set property, a colon, and the number of characters to include from that set. For example, a value of "alpha:3,numeric:2,alpha:3" generates an 8-character password in which the first three characters are from the "alpha" set, the next two are from the "numeric" set, and the final three are from the "alpha" set.

Default Value

None

Allowed Values

A comma-delimited list whose elements comprise a valid character set name, a colon, and a positive integer indicating the number of characters from that set to be included.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-password-policy-prop(1)

Name

dsconfig set-password-policy-prop - Modifies Authentication Policy properties

Synopsis

`dsconfig set-password-policy-prop` {options}

Description

Modifies Authentication Policy properties.

Options

The `dsconfig set-password-policy-prop` command takes the following options:

`--policy-name {name}`

The name of the Authentication Policy.

Authentication Policy properties depend on the Authentication Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

`ldap-pass-through-authentication-policy`

Default {name}: LDAP Pass Through Authentication Policy

Enabled by default: false

See LDAP Pass Through Authentication Policy for the properties of this Authentication Policy type.

`password-policy`

Default {name}: Password Policy

Enabled by default: false

See Password Policy for the properties of this Authentication Policy type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Authentication Policy properties depend on the Authentication Policy type, which depends on

the `--policy-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Authentication Policy properties depend on the Authentication Policy type, which depends on the `--policy-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Authentication Policy properties depend on the Authentication Policy type, which depends on the `--policy-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Authentication Policy properties depend on the Authentication Policy type, which depends on the `--policy-name {name}` option.

LDAP Pass Through Authentication Policy

Authentication Policies of type ldap-pass-through-authentication-policy have the following properties:

cached-password-storage-scheme

Description

Specifies the name of a password storage scheme which should be used for encoding cached passwords. Changing the password storage scheme will cause all existing cached passwords to be discarded.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cached-password-ttl

Description

Specifies the maximum length of time that a locally cached password may be used for authentication before it is refreshed from the remote LDAP service. This property represents a cache timeout. Increasing the timeout period decreases the frequency that bind operations are delegated to the remote LDAP service, but increases the risk of users authenticating using stale passwords. Note that authentication attempts which fail because the provided password does not match the locally cached password will always be retried against the remote LDAP service.

Default Value

8 hours

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-timeout

Description

Specifies the timeout used when connecting to remote LDAP directory servers, performing SSL negotiation, and for individual search and bind requests. If the timeout expires then the current operation will be aborted and retried against another LDAP server if one is available.

Default Value

3 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the LDAP Pass Through Authentication Policy implementation.

Default Value

org.opends.server.extensions.LDAPPassThroughAuthenticationPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

mapped-attribute

Description

Specifies one or more attributes in the user's entry whose value(s) will determine the bind DN used when authenticating to the remote LDAP directory service. This property is mandatory when using the "mapped-bind" or "mapped-search" mapping policies. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. At least one of the named attributes must exist in a user's local entry in order for authentication to proceed. When multiple attributes or values are found in the user's entry then the behavior is determined by the mapping policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-base-dn

Description

Specifies the set of base DNs below which to search for users in the remote LDAP directory service. This property is mandatory when using the "mapped-search" mapping policy. If multiple values are given, searches are performed below all specified base DNs.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-dn

Description

Specifies the bind DN which should be used to perform user searches in the remote LDAP directory service.

Default Value

Searches will be performed anonymously.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password

Description

Specifies the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-environment-variable

Description

Specifies the name of an environment variable containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-file

Description

Specifies the name of a file containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-property

Description

Specifies the name of a Java property containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-filter-template

Description

If defined, overrides the filter used when searching for the user, substituting %s with the value of the local entry's "mapped-attribute". The filter-template may include ZERO or ONE %s substitutions. If multiple mapped-attributes are configured, multiple renditions of this template will be aggregated into one larger filter using an OR (|) operator. An example use-case for this property would be to use a different attribute type on the mapped search. For example, mapped-attribute could be set to "uid" and filter-template to "(samAccountName=%s)". You can also use the filter to restrict search results. For example: "(&(uid=%s)(objectclass=student))"

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapping-policy

Description

Specifies the mapping algorithm for obtaining the bind DN from the user's entry.

Default Value

unmapped

Allowed Values

mapped-bind

Bind to the remote LDAP directory service using a DN obtained from an attribute in the user's entry. This policy will check each attribute named in the "mapped-attribute" property. If more than one attribute or value is present then the first one will be used.

mapped-search

Bind to the remote LDAP directory service using the DN of an entry obtained using a search

against the remote LDAP directory service. The search filter will comprise of an equality matching filter whose attribute type is the "mapped-attribute" property, and whose assertion value is the attribute value obtained from the user's entry. If more than one attribute or value is present then the filter will be composed of multiple equality filters combined using a logical OR (union).

unmapped

Bind to the remote LDAP directory service using the DN of the user's entry in this directory server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

primary-remote-ldap-server

Description

Specifies the primary list of remote LDAP servers which should be used for pass through authentication. If more than one LDAP server is specified then operations may be distributed across them. If all of the primary LDAP servers are unavailable then operations will fail-over to the set of secondary LDAP servers, if defined.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-remote-ldap-server

Description

Specifies the secondary list of remote LDAP servers which should be used for pass through authentication in the event that the primary LDAP servers are unavailable. If more than one LDAP server is specified then operations may be distributed across them. Operations will be rerouted to the primary LDAP servers as soon as they are determined to be available.

Default Value

No secondary LDAP servers.

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols which are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with remote LDAP directory servers.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

use-password-caching

Description

Indicates whether passwords should be cached locally within the user's entry.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Pass Through Authentication Policy should use SSL. If enabled, the LDAP Pass Through Authentication Policy will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether LDAP connections should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether LDAP connections should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance

and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Policy

Authentication Policies of type password-policy have the following properties:

account-status-notification-handler

Description

Specifies the names of the account status notification handlers that are used with the associated password storage scheme.

Default Value

None

Allowed Values

The DN of any Account Status Notification Handler. The referenced account status notification handlers must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-expired-password-changes

Description

Indicates whether a user whose password is expired is still allowed to change that password using the password modify extended operation.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-multiple-password-values

Description

Indicates whether user entries can have multiple distinct values for the password attribute. This is potentially dangerous because many mechanisms used to change the password do not work well with such a configuration. If multiple password values are allowed, then any of them can be used to authenticate, and they are all subject to the same policy constraints.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-pre-encoded-passwords

Description

Indicates whether users can change their passwords by providing a pre-encoded value. This can cause a security risk because the clear-text version of the password is not known and therefore validation checks cannot be applied to it.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-user-password-changes

Description

Indicates whether users can change their own passwords. This check is made in addition to access control evaluation. Both must allow the password change for it to occur.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-password-storage-scheme

Description

Specifies the names of the password storage schemes that are used to encode clear-text passwords for this password policy.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

deprecated-password-storage-scheme

Description

Specifies the names of the password storage schemes that are considered deprecated for this password policy. If a user with this password policy authenticates to the server and his/her password is encoded with a deprecated scheme, those values are removed and replaced with values encoded using the default password storage scheme(s).

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

expire-passwords-without-warning

Description

Indicates whether the directory server allows a user's password to expire even if that user has never seen an expiration warning notification. If this property is true, accounts always expire when the expiration time arrives. If this property is false or disabled, the user always receives at least one warning notification, and the password expiration is set to the warning time plus the warning interval.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-add

Description

Indicates whether users are forced to change their passwords upon first authenticating to the directory server after their account has been created.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-reset

Description

Indicates whether users are forced to change their passwords if they are reset by an administrator. For this purpose, anyone with permission to change a given user's password other than that user is considered an administrator.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

grace-login-count

Description

Specifies the number of grace logins that a user is allowed after the account has expired to allow that user to choose a new password. A value of 0 indicates that no grace logins are allowed.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

idle-lockout-interval

Description

Specifies the maximum length of time that an account may remain idle (that is, the associated user does not authenticate to the server) before that user is locked out. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that idle accounts are not automatically locked out. This feature is available only if the last login time is maintained.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the Password Policy implementation.

Default Value

org.opends.server.core.PasswordPolicyFactory

Allowed Values

A Java class that implements or extends the class(es):

org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

last-login-time-attribute

Description

Specifies the name or OID of the attribute type that is used to hold the last login time for users with the associated password policy. This attribute type must be defined in the directory server schema and must either be defined as an operational attribute or must be allowed by the set of objectClasses for all users with the associated password policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

last-login-time-format

Description

Specifies the format string that is used to generate the last login time value for users with the associated password policy. This format string conforms to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-duration

Description

Specifies the length of time that an account is locked after too many authentication failures. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the account must remain locked until an administrator resets the password.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-count

Description

Specifies the maximum number of authentication failures that a user is allowed before the account is locked out. A value of 0 indicates that accounts are never locked out due to failed attempts.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-expiration-interval

Description

Specifies the length of time before an authentication failure is no longer counted against a user for the purposes of account lockout. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the authentication failures must never expire. The failure count is always cleared upon a successful authentication.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-age

Description

Specifies the maximum length of time that a user can continue using the same password before it must be changed (that is, the password expiration interval). The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables password expiration.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-reset-age

Description

Specifies the maximum length of time that users have to change passwords after they have been reset by an administrator before they become locked. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables this feature.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-age

Description

Specifies the minimum length of time after a password change before the user is allowed to change the password again. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. This setting can be used to prevent users from changing their passwords repeatedly over a short period of time to flush an old password from the history so that it can be re-used.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-attribute

Description

Specifies the attribute type used to hold user passwords. This attribute type must be defined in the server schema, and it must have either the user password or auth password syntax.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-change-requires-current-password

Description

Indicates whether user password changes must use the password modify extended operation and must include the user's current password before the change is allowed.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-expiration-warning-interval

Description

Specifies the maximum length of time before a user's password actually expires that the server begins to include warning notifications in bind responses for that user. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables the warning interval.

Default Value

5 days

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-generator

Description

Specifies the name of the password generator that is used with the associated password policy. This is used in conjunction with the password modify extended operation to generate a new password for a user when none was provided in the request.

Default Value

None

Allowed Values

The DN of any Password Generator. The referenced password generator must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-count

Description

Specifies the maximum number of former passwords to maintain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero indicates that either no password history is to be maintained (if the password history duration has a value of zero seconds), or that there is no maximum number of passwords to maintain in the history (if the password history duration has a value greater than zero seconds).

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-duration

Description

Specifies the maximum length of time that passwords remain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero seconds indicates that either no password history is to be maintained (if the password history count has a value of zero), or that there is no maximum duration for passwords in the history (if the password history count has a value greater than zero).

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-validator

Description

Specifies the names of the password validators that are used with the associated password storage scheme. The password validators are invoked when a user attempts to provide a new password, to determine whether the new password is acceptable.

Default Value

None

Allowed Values

The DN of any Password Validator. The referenced password validators must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

previous-last-login-time-format

Description

Specifies the format string(s) that might have been used with the last login time at any point in the past for users associated with the password policy. These values are used to make it possible to parse previous values, but are not used to set new values. The format strings conform to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-change-by-time

Description

Specifies the time by which all users with the associated password policy must change their passwords. The value is expressed in a generalized time format. If this time is equal to the current time or is in the past, then all users are required to change their passwords immediately. The behavior of the server in this mode is identical to the behavior observed when users are forced to change their passwords after an administrative reset.

Default Value

None

Allowed Values

A valid timestamp in generalized time form (for example, a value of "20070409185811Z" indicates a value of April 9, 2007 at 6:58:11 pm GMT).

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-authentication

Description

Indicates whether users with the associated password policy are required to authenticate in a secure manner. This might mean either using a secure communication channel between the client and the server, or using a SASL mechanism that does not expose the credentials.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-password-changes

Description

Indicates whether users with the associated password policy are required to change their password in a secure manner that does not expose the credentials.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

skip-validation-for-administrators

Description

Indicates whether passwords set by administrators are allowed to bypass the password validation process that is required for user password changes.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

state-update-failure-policy

Description

Specifies how the server deals with the inability to update password policy state information during an authentication attempt. In particular, this property can be used to control whether an otherwise successful bind operation fails if a failure occurs while attempting to update password policy state information (for example, to clear a record of previous authentication failures or to update the last login time). It can also be used to control whether to reject a bind request if it is known ahead of time that it will not be possible to update the authentication failure times in the event of an unsuccessful bind attempt (for example, if the backend writability mode is disabled).

Default Value

reactive

Allowed Values

ignore

If a bind attempt would otherwise be successful, then do not reject it if a problem occurs while attempting to update the password policy state information for the user.

proactive

Proactively reject any bind attempt if it is known ahead of time that it would not be possible to update the user's password policy state information.

reactive

Even if a bind attempt would otherwise be successful, reject it if a problem occurs while attempting to update the password policy state information for the user.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-password-storage-scheme-prop(1)

Name

dsconfig set-password-storage-scheme-prop - Modifies Password Storage Scheme properties

Synopsis

`dsconfig set-password-storage-scheme-prop` {options}

Description

Modifies Password Storage Scheme properties.

Options

The `dsconfig set-password-storage-scheme-prop` command takes the following options:

`--scheme-name {name}`

The name of the Password Storage Scheme.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

`aes-password-storage-scheme`

Default {name}: AES Password Storage Scheme

Enabled by default: true

See AES Password Storage Scheme for the properties of this Password Storage Scheme type.

`base64-password-storage-scheme`

Default {name}: Base64 Password Storage Scheme

Enabled by default: true

See Base64 Password Storage Scheme for the properties of this Password Storage Scheme type.

`bcrypt-password-storage-scheme`

Default {name}: Bcrypt Password Storage Scheme

Enabled by default: true

See Bcrypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`blowfish-password-storage-scheme`

Default {name}: Blowfish Password Storage Scheme

Enabled by default: true

See Blowfish Password Storage Scheme for the properties of this Password Storage Scheme type.

`clear-password-storage-scheme`

Default {name}: Clear Password Storage Scheme

Enabled by default: true

See Clear Password Storage Scheme for the properties of this Password Storage Scheme type.

`crypt-password-storage-scheme`

Default {name}: Crypt Password Storage Scheme

Enabled by default: true

See Crypt Password Storage Scheme for the properties of this Password Storage Scheme type.

`md5-password-storage-scheme`

Default {name}: MD5 Password Storage Scheme

Enabled by default: true

See MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha256-password-storage-scheme`

Default {name}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pbkdf2-hmac-sha512-password-storage-scheme`

Default {name}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See PBKDF2 Hmac SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`pkcs5s2-password-storage-scheme`

Default {name}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See PKCS5S2 Password Storage Scheme for the properties of this Password Storage Scheme type.

`rc4-password-storage-scheme`

Default {name}: RC4 Password Storage Scheme

Enabled by default: true

See RC4 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-md5-password-storage-scheme`

Default {name}: Salted MD5 Password Storage Scheme

Enabled by default: true

See Salted MD5 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha1-password-storage-scheme`

Default {name}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See Salted SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha256-password-storage-scheme`

Default {name}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See Salted SHA256 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha384-password-storage-scheme`

Default {name}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See Salted SHA384 Password Storage Scheme for the properties of this Password Storage Scheme type.

`salted-sha512-password-storage-scheme`

Default {name}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See Salted SHA512 Password Storage Scheme for the properties of this Password Storage Scheme type.

`sha1-password-storage-scheme`

Default {name}: SHA1 Password Storage Scheme

Enabled by default: true

See SHA1 Password Storage Scheme for the properties of this Password Storage Scheme type.

`triple-des-password-storage-scheme`

Default {name}: Triple DES Password Storage Scheme

Enabled by default: true

See Triple DES Password Storage Scheme for the properties of this Password Storage Scheme type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the `--scheme-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the `--scheme-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the `--scheme-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the `--scheme-name {name}` option.

AES Password Storage Scheme

Password Storage Schemes of type aes-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the AES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.AESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Base64 Password Storage Scheme

Password Storage Schemes of type base64-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Base64 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.Base64PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Bcrypt Password Storage Scheme

Password Storage Schemes of type bcrypt-password-storage-scheme have the following properties:

bcrypt-cost

Description

The cost parameter specifies a key expansion iteration count as a power of two. A default value of 12 (2^12 iterations) is considered in 2016 as a reasonable balance between responsiveness and security for regular users.

Default Value

12

Allowed Values

An integer value. Lower value is 1. Upper value is 30.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Bcrypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BcryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Blowfish Password Storage Scheme

Password Storage Schemes of type blowfish-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Blowfish Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BlowfishPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Clear Password Storage Scheme

Password Storage Schemes of type clear-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Clear Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.ClearPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Crypt Password Storage Scheme

Password Storage Schemes of type crypt-password-storage-scheme have the following properties:

crypt-password-storage-encryption-algorithm

Description

Specifies the algorithm to use to encrypt new passwords. Select the crypt algorithm to use to encrypt new passwords. The value can either be "unix", which means the password is encrypted with the weak Unix crypt algorithm, or "md5" which means the password is encrypted with the BSD MD5 algorithm and has a 1 prefix, or "sha256" which means the password is encrypted with the SHA256 algorithm and has a 5 prefix, or "sha512" which means the password is encrypted with the SHA512 algorithm and has a 6 prefix.

Default Value

unix

Allowed Values

md5

New passwords are encrypted with the BSD MD5 algorithm.

sha256

New passwords are encrypted with the Unix crypt SHA256 algorithm.

sha512

New passwords are encrypted with the Unix crypt SHA512 algorithm.

unix

New passwords are encrypted with the Unix crypt algorithm. Passwords are truncated at 8 characters and the top bit of each character is ignored.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Crypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.CryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

MD5 Password Storage Scheme

Password Storage Schemes of type md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.MD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

PBKDF2 Hmac SHA256 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

PBKDF2 Hmac SHA512 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

PKCS5S2 Password Storage Scheme

Password Storage Schemes of type pkcs5s2-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PKCS5S2 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PKCS5S2PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

RC4 Password Storage Scheme

Password Storage Schemes of type rc4-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the RC4 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.RC4PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted MD5 Password Storage Scheme

Password Storage Schemes of type salted-md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedMD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA1 Password Storage Scheme

Password Storage Schemes of type salted-sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA256 Password Storage Scheme

Password Storage Schemes of type salted-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA384 Password Storage Scheme

Password Storage Schemes of type salted-sha384-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA384 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA384PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Salted SHA512 Password Storage Scheme

Password Storage Schemes of type salted-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

SHA1 Password Storage Scheme

Password Storage Schemes of type sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Triple DES Password Storage Scheme

Password Storage Schemes of type triple-des-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Triple DES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.TripleDESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-password-validator-prop(1)

Name

dsconfig set-password-validator-prop - Modifies Password Validator properties

Synopsis

`dsconfig set-password-validator-prop` {options}

Description

Modifies Password Validator properties.

Options

The `dsconfig set-password-validator-prop` command takes the following options:

`--validator-name {name}`

The name of the Password Validator.

Password Validator properties depend on the Password Validator type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

`attribute-value-password-validator`

Default {name}: Attribute Value Password Validator

Enabled by default: true

See Attribute Value Password Validator for the properties of this Password Validator type.

`character-set-password-validator`

Default {name}: Character Set Password Validator

Enabled by default: true

See Character Set Password Validator for the properties of this Password Validator type.

`dictionary-password-validator`

Default {name}: Dictionary Password Validator

Enabled by default: true

See Dictionary Password Validator for the properties of this Password Validator type.

`length-based-password-validator`

Default {name}: Length Based Password Validator

Enabled by default: true

See Length Based Password Validator for the properties of this Password Validator type.

`repeated-characters-password-validator`

Default {name}: Repeated Characters Password Validator

Enabled by default: true

See Repeated Characters Password Validator for the properties of this Password Validator type.

`similarity-based-password-validator`

Default {name}: Similarity Based Password Validator

Enabled by default: true

See Similarity Based Password Validator for the properties of this Password Validator type.

`unique-characters-password-validator`

Default {name}: Unique Characters Password Validator

Enabled by default: true

See Unique Characters Password Validator for the properties of this Password Validator type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Password Validator properties depend on the Password Validator type, which depends on the `--validator-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Password Validator properties depend on the Password Validator type, which depends on the `--validator-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Password Validator properties depend on the Password Validator type, which depends on the `--validator-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Password Validator properties depend on the Password Validator type, which depends on the `--validator-name {name}` option.

Attribute Value Password Validator

Password Validators of type attribute-value-password-validator have the following properties:

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against attribute values. If "false" then only match the entire password against attribute values otherwise ("true") check whether the password contains attribute values.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.AttributeValuePasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name(s) of the attribute(s) whose values should be checked to determine whether they match the provided password. If no values are provided, then the server checks if the proposed password matches the value of any attribute in the user's entry.

Default Value

All attributes in the user entry will be checked.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator should test the reversed value of the provided password as well as the order in which it was given.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Character Set Password Validator

Password Validators of type character-set-password-validator have the following properties:

allow-unclassified-characters

Description

Indicates whether this password validator allows passwords to contain characters outside of any of the user-defined character sets and ranges. If this is "false", then only those characters in the user-defined character sets and ranges may be used in passwords. Any password containing a character not included in any character set or range will be rejected.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set

Description

Specifies a character set containing characters that a password may contain and a value indicating the minimum number of characters required from that set. Each value must be an integer (indicating the minimum required characters from the set which may be zero, indicating that the character set is optional) followed by a colon and the characters to include in that set (for example, "3:abcdefghijklmnopqrstuvwxyz" indicates that a user password must contain at least three characters from the set of lowercase ASCII letters). Multiple character sets can be defined in separate values, although no character can appear in more than one character set.

Default Value

If no sets are specified, the validator only uses the defined character ranges.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set-ranges

Description

Specifies a character range containing characters that a password may contain and a value indicating the minimum number of characters required from that range. Each value must be an integer (indicating the minimum required characters from the range which may be zero, indicating that the character range is optional) followed by a colon and one or more range specifications. A range specification is 3 characters: the first character allowed, a minus, and the last character allowed. For example, "3:A-Za-z0-9". The ranges in each value should not overlap, and the characters in each range specification should be ordered.

Default Value

If no ranges are specified, the validator only uses the defined character sets.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.CharacterSetPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-character-sets

Description

Specifies the minimum number of character sets and ranges that a password must contain. This property should only be used in conjunction with optional character sets and ranges (those requiring zero characters). Its value must include any mandatory character sets and ranges (those requiring greater than zero characters). This is useful in situations where a password must contain characters from mandatory character sets and ranges, and characters from at least N optional character sets and ranges. For example, it is quite common to require that a password

contains at least one non-alphanumeric character as well as characters from two alphanumeric character sets (lower-case, upper-case, digits). In this case, this property should be set to 3.

Default Value

The password must contain characters from each of the mandatory character sets and ranges and, if there are optional character sets and ranges, at least one character from one of the optional character sets and ranges.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Dictionary Password Validator

Password Validators of type dictionary-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator is to treat password characters in a case-sensitive manner. If it is set to true, then the validator rejects a password only if it appears in the dictionary with exactly the same capitalization as provided by the user.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against dictionary words. If "false" then only match the entire password against words otherwise ("true") check whether the password contains words.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dictionary-file

Description

Specifies the path to the file containing a list of words that cannot be used as passwords. It should be formatted with one word per line. The value can be an absolute path or a path that is relative to the OpenDJ instance root.

Default Value

For Unix and Linux systems: config/wordlist.txt. For Windows systems: config\wordlist.txt

Allowed Values

The path to any text file contained on the system that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.DictionaryPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator is to test the reversed value of the provided password as well as the order in which it was given. For example, if the user provides a new password of "password" and this configuration attribute is set to true, then the value "drowssap" is also tested against attribute values in the user's entry.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Length Based Password Validator

Password Validators of type length-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.LengthBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-password-length

Description

Specifies the maximum number of characters that can be included in a proposed password. A value of zero indicates that there will be no upper bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the

maximum length.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-length

Description

Specifies the minimum number of characters that must be included in a proposed password. A value of zero indicates that there will be no lower bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

6

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Repeated Characters Password Validator

Password Validators of type repeated-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. If the value of this property is false, the validator ignores any differences in capitalization when looking for consecutive characters in the password. If the value is true, the validator considers a character to be repeating only if all consecutive occurrences use the same capitalization.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.RepeatedCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-consecutive-length

Description

Specifies the maximum number of times that any character can appear consecutively in a password value. A value of zero indicates that no maximum limit is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Similarity Based Password Validator

Password Validators of type similarity-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.SimilarityBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-password-difference

Description

Specifies the minimum difference of new and old password. A value of zero indicates that no difference between passwords is acceptable.

Default Value

None

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

Unique Characters Password Validator

Password Validators of type unique-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. A value of true indicates that the validator does not consider a capital letter to be the same as its lower-case counterpart. A value of false indicates that the validator ignores differences in capitalization when looking at the number of unique characters in the password.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.UniqueCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-unique-characters

Description

Specifies the minimum number of unique characters that a password will be allowed to contain. A value of zero indicates that no minimum value is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-plugin-prop(1)

Name

dsconfig set-plugin-prop - Modifies Plugin properties

Synopsis

`dsconfig set-plugin-prop` {options}

Description

Modifies Plugin properties.

Options

The `dsconfig set-plugin-prop` command takes the following options:

`--plugin-name {name}`
: The name of the Plugin.

  Plugin properties depend on the Plugin type, which depends on the {name} you provide.

  By default, OpenDJ directory server supports the following Plugin types:

  `attribute-cleanup-plugin`
  : Default {name}: Attribute Cleanup Plugin

    Enabled by default: true

    See Attribute Cleanup Plugin for the properties of this Plugin type.

  `change-number-control-plugin`
  : Default {name}: Change Number Control Plugin

    Enabled by default: true

    See Change Number Control Plugin for the properties of this Plugin type.

  `entry-uuid-plugin`
  : Default {name}: Entry UUID Plugin

    Enabled by default: true

    See Entry UUID Plugin for the properties of this Plugin type.

  `fractional-ldif-import-plugin`
  : Default {name}: Fractional LDIF Import Plugin

Enabled by default: true

See Fractional LDIF Import Plugin for the properties of this Plugin type.

`last-mod-plugin`

Default {name}: Last Mod Plugin

Enabled by default: true

See Last Mod Plugin for the properties of this Plugin type.

`ldap-attribute-description-list-plugin`

Default {name}: LDAP Attribute Description List Plugin

Enabled by default: true

See LDAP Attribute Description List Plugin for the properties of this Plugin type.

`password-policy-import-plugin`

Default {name}: Password Policy Import Plugin

Enabled by default: true

See Password Policy Import Plugin for the properties of this Plugin type.

`profiler-plugin`

Default {name}: Profiler Plugin

Enabled by default: true

See Profiler Plugin for the properties of this Plugin type.

`referential-integrity-plugin`

Default {name}: Referential Integrity Plugin

Enabled by default: true

See Referential Integrity Plugin for the properties of this Plugin type.

`samba-password-plugin`

Default {name}: Samba Password Plugin

Enabled by default: true

See Samba Password Plugin for the properties of this Plugin type.

`seven-bit-clean-plugin`

Default {name}: Seven Bit Clean Plugin

Enabled by default: true

See Seven Bit Clean Plugin for the properties of this Plugin type.

`unique-attribute-plugin`

Default {name}: Unique Attribute Plugin

Enabled by default: true

See Unique Attribute Plugin for the properties of this Plugin type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Plugin properties depend on the Plugin type, which depends on the `--plugin-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Plugin properties depend on the Plugin type, which depends on the `--plugin-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Plugin properties depend on the Plugin type, which depends on the `--plugin-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Plugin properties depend on the Plugin type, which depends on the `--plugin-name {name}` option.

Attribute Cleanup Plugin

Plugins of type attribute-cleanup-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.AttributeCleanupPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparseadd preparsemodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

remove-inbound-attributes

Description

A list of attributes which should be removed from incoming add or modify requests.

Default Value

No attributes will be removed

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rename-inbound-attributes

Description

A list of attributes which should be renamed in incoming add or modify requests.

Default Value

No attributes will be renamed

Allowed Values

An attribute name mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Change Number Control Plugin

Plugins of type change-number-control-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ChangeNumberControlPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postOperationAdd postOperationDelete postOperationModify postOperationModifyDN

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Entry UUID Plugin

Plugins of type entry-uuid-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.EntryUUIDPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport preoperationadd

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the

client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Fractional LDIF Import Plugin

Plugins of type fractional-ldif-import-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

None

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

None

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

Last Mod Plugin

Plugins of type last-mod-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LastModPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd preoperationmodify preoperationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

LDAP Attribute Description List Plugin

Plugins of type ldap-attribute-description-list-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LDAPADListPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparsesearch

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Password Policy Import Plugin

Plugins of type password-policy-import-plugin have the following properties:

default-auth-password-storage-scheme

Description

Specifies the names of password storage schemes that to be used for encoding passwords contained in attributes with the auth password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy should be used to govern them.

Default Value

If the default password policy uses an attribute with the auth password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes auth password values using the "SHA1" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import plug-in is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-user-password-storage-scheme

Description

Specifies the names of the password storage schemes to be used for encoding passwords contained in attributes with the user password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy is to be used to govern them.

Default Value

If the default password policy uses the attribute with the user password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes user password values using the "SSHA" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import Plugin is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.PasswordPolicyImportPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Profiler Plugin

Plugins of type profiler-plugin have the following properties:

enable-profiling-on-startup

Description

Indicates whether the profiler plug-in is to start collecting data automatically when the directory server is started. This property is read only when the server is started, and any changes take effect on the next restart. This property is typically set to "false" unless startup profiling is required, because otherwise the volume of data that can be collected can cause the server to run out of memory if it is not turned off in a timely manner.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.profiler.ProfilerPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

startup

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

profile-action

Description

Specifies the action that should be taken by the profiler. A value of "start" causes the profiler thread to start collecting data if it is not already active. A value of "stop" causes the profiler thread to stop collecting data and write it to disk, and a value of "cancel" causes the profiler thread to stop collecting data and discard anything that has been captured. These operations occur immediately.

Default Value

none

Allowed Values

cancel

Stop collecting profile data and discard what has been captured.

none

Do not take any action.

start

Start collecting profile data.

stop

Stop collecting profile data and write what has been captured to a file in the profile directory.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-directory

Description

Specifies the path to the directory where profile information is to be written. This path may be either an absolute path or a path that is relative to the root of the OpenDJ directory server instance. The directory must exist and the directory server must have permission to create new files in it.

Default Value

None

Allowed Values

The path to any directory that exists on the filesystem and that can be read and written by the server user.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-sample-interval

Description

Specifies the sample interval in milliseconds to be used when capturing profiling information in the server. When capturing data, the profiler thread sleeps for this length of time between calls to obtain traces for all threads running in the JVM.

Default Value

None

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

NoneChanges to this configuration attribute take effect the next time the profiler is started.

Advanced Property

No

Read-only

No

Referential Integrity Plugin

Plugins of type referential-integrity-plugin have the following properties:

attribute-type

Description

Specifies the attribute types for which referential integrity is to be maintained. At least one attribute type must be specified, and the syntax of any attributes must be either a distinguished name (1.3.6.1.4.1.1466.115.121.1.12) or name and optional UID (1.3.6.1.4.1.1466.115.121.1.34).

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN that limits the scope within which referential integrity is maintained.

Default Value

Referential integrity is maintained in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references

Description

Specifies whether reference attributes must refer to existing entries. When this property is set to true, this plugin will ensure that any new references added as part of an add or modify operation point to existing entries, and that the referenced entries match the filter criteria for the referencing attribute, if specified.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-filter-criteria

Description

Specifies additional filter criteria which will be enforced when checking references. If a reference attribute has filter criteria defined then this plugin will ensure that any new references added as part of an add or modify operation refer to an existing entry which matches the specified filter.

Default Value

None

Allowed Values

An attribute-filter mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-scope-criteria

Description

Specifies whether referenced entries must reside within the same naming context as the entry containing the reference. The reference scope will only be enforced when reference checking is enabled.

Default Value

global

Allowed Values

global

References may refer to existing entries located anywhere in the Directory.

naming-context

References must refer to existing entries located within the same naming context.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ReferentialIntegrityPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

Specifies the log file location where the update records are written when the plug-in is in background-mode processing. The default location is the logs directory of the server instance, using the file name "referint".

Default Value

logs/referint

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postoperationdelete postoperationmodifydn subordinatemodifydn subordinatedelete preoperationadd preoperationmodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

update-interval

Description

Specifies the interval in seconds when referential integrity updates are made. If this value is 0, then the updates are made synchronously in the foreground.

Default Value

0 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Samba Password Plugin

Plugins of type samba-password-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SambaPasswordPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationmodify postoperationextended

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pwd-sync-policy

Description

Specifies which Samba passwords should be kept synchronized.

Default Value

sync-nt-password

Allowed Values

sync-lm-password

Synchronize the LanMan password attribute "sambaLMPassword"

sync-nt-password

Synchronize the NT password attribute "sambaNTPassword"

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

samba-administrator-dn

Description

Specifies the distinguished name of the user which Samba uses to perform Password Modify extended operations against this directory server in order to synchronize the userPassword attribute after the LanMan or NT passwords have been updated. The user must have the 'password-reset' privilege and should not be a root user. This user name can be used in order to identify Samba connections and avoid double re-synchronization of the same password. If this property is left undefined, then no password updates will be skipped.

Default Value

Synchronize all updates to user passwords

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Seven Bit Clean Plugin

Plugins of type seven-bit-clean-plugin have the following properties:

attribute-type

Description

Specifies the name or OID of an attribute type for which values should be checked to ensure that they are 7-bit clean.

Default Value

uid mail userPassword

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN below which the checking is performed. Any attempt to update a value for one of the configured attributes below this base DN must be 7-bit clean for the operation to be allowed.

Default Value

All entries below all public naming contexts will be checked.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SevenBitCleanPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport preparseadd preparsemodify preparsemodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Unique Attribute Plugin

Plugins of type unique-attribute-plugin have the following properties:

base-dn

Description

Specifies a base DN within which the attribute must be unique.

Default Value

The plug-in uses the server's public naming contexts in the searches.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.UniqueAttributePlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd preoperationmodify preoperationmodifydn postoperationadd postoperationmodify postoperationmodifydn postsynchronizationadd postsynchronizationmodify postsynchronizationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

type

Description

Specifies the type of attributes to check for value uniqueness.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-plugin-root-prop(1)

Name

dsconfig set-plugin-root-prop - Modifies Plugin Root properties

Synopsis

`dsconfig set-plugin-root-prop` {options}

Description

Modifies Plugin Root properties.

Options

The `dsconfig set-plugin-root-prop` command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Plugin Root properties depend on the Plugin Root type, which depends on the null option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Plugin Root properties depend on the Plugin Root type, which depends on the null option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Plugin Root properties depend on the Plugin Root type, which depends on the null option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Plugin Root properties depend on the Plugin Root type, which depends on the null option.

Plugin Root

Plugin Roots of type plugin-root have the following properties:

plugin-order-intermediate-response

Description

Specifies the order in which intermediate response plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which intermediate response plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-ldif-export

Description

Specifies the order in which LDIF export plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which LDIF export plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-ldif-import

Description

Specifies the order in which LDIF import plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which LDIF import plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-ldif-import-begin

Description

Specifies the order in which LDIF import begin plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which LDIF import begin plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-ldif-import-end

Description

Specifies the order in which LDIF import end plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which LDIF import end plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-connect

Description

Specifies the order in which post-connect plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-connect plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-disconnect

Description

Specifies the order in which post-disconnect plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-disconnect plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-abandon

Description

Specifies the order in which post-operation abandon plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation abandon plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-add

Description

Specifies the order in which post-operation add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-bind

Description

Specifies the order in which post-operation bind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation bind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-compare

Description

Specifies the order in which post-operation compare plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation compare plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-delete

Description

Specifies the order in which post-operation delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-extended

Description

Specifies the order in which post-operation extended operation plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation extended operation plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-modify

Description

Specifies the order in which post-operation modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-modify-dn

Description

Specifies the order in which post-operation modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-search

Description

Specifies the order in which post-operation search plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation search plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-unbind

Description

Specifies the order in which post-operation unbind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation unbind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-add

Description

Specifies the order in which post-response add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-bind

Description

Specifies the order in which post-response bind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response bind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-compare

Description

Specifies the order in which post-response compare plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response compare plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-delete

Description

Specifies the order in which post-response delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-extended

Description

Specifies the order in which post-response extended operation plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response extended operation plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-modify

Description

Specifies the order in which post-response modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-modify-dn

Description

Specifies the order in which post-response modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-search

Description

Specifies the order in which post-response search plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the

position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response search plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-synchronization-add

Description

Specifies the order in which post-synchronization add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-synchronization add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-synchronization-delete

Description

Specifies the order in which post-synchronization delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-synchronization delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-synchronization-modify

Description

Specifies the order in which post-synchronization modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-synchronization modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-synchronization-modify-dn

Description

Specifies the order in which post-synchronization modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-synchronization modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-add

Description

Specifies the order in which pre-operation add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-bind

Description

Specifies the order in which pre-operation bind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation bind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-compare

Description

Specifies the order in which pre-operation compare plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation compare plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-delete

Description

Specifies the order in which pre-operation delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-extended

Description

Specifies the order in which pre-operation extended operation plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation extended operation plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-modify

Description

Specifies the order in which pre-operation modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-modify-dn

Description

Specifies the order in which pre-operation modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-search

Description

Specifies the order in which pre-operation search plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation searc plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-abandon

Description

Specifies the order in which pre-parse abandon plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse abandon plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-add

Description

Specifies the order in which pre-parse add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-bind

Description

Specifies the order in which pre-parse bind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse bind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-compare

Description

Specifies the order in which pre-parse compare plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse compare plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-delete

Description

Specifies the order in which pre-parse delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-extended

Description

Specifies the order in which pre-parse extended operation plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse extended operation plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-modify

Description

Specifies the order in which pre-parse modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-modify-dn

Description

Specifies the order in which pre-parse modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-search

Description

Specifies the order in which pre-parse search plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse search plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-unbind

Description

Specifies the order in which pre-parse unbind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse unbind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-search-result-entry

Description

Specifies the order in which search result entry plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which search result entry plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-search-result-reference

Description

Specifies the order in which search result reference plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which search result reference plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-shutdown

Description

Specifies the order in which shutdown plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which shutdown plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-startup

Description

Specifies the order in which startup plug-ins are to be loaded and invoked. The value is a

comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which startup plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-subordinate-delete

Description

Specifies the order in which subordinate delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which subordinate delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-subordinate-modify-dn

Description

Specifies the order in which subordinate modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which subordinate modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-replication-domain-prop(1)

Name

dsconfig set-replication-domain-prop - Modifies Replication Domain properties

Synopsis

`dsconfig set-replication-domain-prop` {options}

Description

Modifies Replication Domain properties.

Options

The `dsconfig set-replication-domain-prop` command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default {name}: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

`--domain-name {name}`

The name of the Replication Domain.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

`replication-domain`

Default {name}: Replication Domain

Enabled by default: false

See Replication Domain for the properties of this Replication Domain type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Replication Domain properties depend on the Replication Domain type, which depends on the `--domain-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Replication Domain properties depend on the Replication Domain type, which depends on the `--domain-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Replication Domain properties depend on the Replication Domain type, which depends on the `--domain-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Replication Domain properties depend on the Replication Domain type, which depends on the `--domain-name {name}` option.

Replication Domain

Replication Domains of type replication-domain have the following properties:

assured-sd-level

Description

The level of acknowledgment for Safe Data assured sub mode. When assured replication is configured in Safe Data mode, this value defines the number of replication servers (with the same group ID of the local server) that should acknowledge the sent update before the LDAP client call can return.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-timeout

Description

The timeout value when waiting for assured replication acknowledgments. Defines the amount of milliseconds the server will wait for assured acknowledgments (in either Safe Data or Safe Read assured replication modes) before returning anyway the LDAP client call.

Default Value

2000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-type

Description

Defines the assured replication mode of the replicated domain. The assured replication can be disabled or enabled. When enabled, two modes are available: Safe Data or Safe Read modes.

Default Value

not-assured

Allowed Values

not-assured

Assured replication is not enabled. Updates sent for replication (for being replayed on other LDAP servers in the topology) are sent without waiting for any acknowledgment and the LDAP client call returns immediately.

safe-data

Assured replication is enabled in Safe Data mode: updates sent for replication are subject to acknowledgment from the replication servers that have the same group ID as the local server (defined with the group-id property). The number of acknowledgments to expect is defined by the assured-sd-level property. After acknowledgments are received, LDAP client call returns.

safe-read

Assured replication is enabled in Safe Read mode: updates sent for replication are subject to acknowledgments from the LDAP servers in the topology that have the same group ID as the local server (defined with the group-id property). After acknowledgments are received, LDAP client call returns.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN of the replicated data.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

changetime-heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when sending its local change time to the Replication Server. The directory server sends a regular heart-beat to the Replication within the specified interval. The heart-beat indicates the change time of the directory server to the Replication Server.

Default Value

1000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

conflicts-historical-purge-delay

Description

This delay indicates the time (in minutes) the domain keeps the historical information necessary to solve conflicts.When a change stored in the historical part of the user entry has a date (from its replication ChangeNumber) older than this delay, it is candidate to be purged. The purge is applied on 2 events: modify of the entry, dedicated purge task.

Default Value

1440m

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 minutes.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-exclude

Description

Allows to exclude some attributes to replicate to this server. If fractional-exclude configuration attribute is used, attributes specified in this attribute will be ignored (not added/modified/deleted) when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-include attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be excluded. The object class may be "*" indicating that the attribute type(s) should be excluded regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-include

Description

Allows to include some attributes to replicate to this server. If fractional-include configuration attribute is used, only attributes specified in this attribute will be added/modified/deleted when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-exclude attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be included. The object class may be "*" indicating that the attribute type(s) should be included regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group ID associated with this replicated domain. This value defines the group ID of the replicated domain. The replication system will preferably connect and send updates to replicate to a replication server with the same group ID as its own one (the local server group ID).

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when communicating with Replication Servers. The directory server expects a regular heart-beat coming from the Replication Server within the specified interval. If a heartbeat is not received within the interval, the Directory Server closes its connection and connects to another Replication Server.

Default Value

10000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 100 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

initialization-window-size

Description

Specifies the window size that this directory server may use when communicating with remote Directory Servers for initialization.

Default Value

100

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

isolation-policy

Description

Specifies the behavior of the directory server if a write operation is attempted on the data within the Replication Domain when none of the configured Replication Servers are available.

Default Value

reject-all-updates

Allowed Values

accept-all-updates

Indicates that updates should be accepted even though it is not possible to send them to any Replication Server. Best effort is made to re-send those updates to a Replication Servers when one of them is available, however those changes are at risk because they are only available from the historical information. This mode can also introduce high replication latency.

reject-all-updates

Indicates that all updates attempted on this Replication Domain are rejected when no Replication Server is available.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-changenumber

Description

Indicates if this server logs the ChangeNumber in access log. This boolean indicates if the domain should log the ChangeNumber of replicated operations in the access log.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

referrals-url

Description

The URLs other LDAP servers should use to refer to the local server. URLs used by peer servers in the topology to refer to the local server through LDAP referrals. If this attribute is not defined, every URLs available to access this server will be used. If defined, only URLs specified here will be used.

Default Value

None

Allowed Values

A LDAP URL compliant with RFC 2255.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of the Replication Servers within the Replication Domain to which the directory server should try to connect at startup time. Addresses must be specified using the syntax: hostname:port

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

server-id

Description

Specifies a unique identifier for the directory server within the Replication Domain. Each directory server within the same Replication Domain must have a different server ID. A directory server which is a member of multiple Replication Domains may use the same server ID for each of its Replication Domain configurations.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

solve-conflicts

Description

Indicates if this server solves conflict. This boolean indicates if this domain keeps the historical information necessary to solve conflicts. When set to false the server will not maintain historical information and will therefore not be able to solve conflict. This should therefore be done only if the replication is used in a single master type of deployment.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the directory server will use when communicating with Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-replication-server-prop(1)

Name

dsconfig set-replication-server-prop - Modifies Replication Server properties

Synopsis

`dsconfig set-replication-server-prop` {options}

Description

Modifies Replication Server properties.

Options

The `dsconfig set-replication-server-prop` command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Server properties depend on the Replication Server type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

`replication-server`

Default {name}: Replication Server

Enabled by default: false

See Replication Server for the properties of this Replication Server type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Replication Server properties depend on the Replication Server type, which depends on the `--provider-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Replication Server properties depend on the Replication Server type, which depends on the `--provider-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Replication Server properties depend on the Replication Server type, which depends on the `--provider-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Replication Server properties depend on the Replication Server type, which depends on the `--provider-name {name}` option.

Replication Server

Replication Servers of type replication-server have the following properties:

assured-timeout

Description

The timeout value when waiting for assured mode acknowledgments. Defines the number of milliseconds that the replication server will wait for assured acknowledgments (in either Safe Data or Safe Read assured sub modes) before forgetting them and answer to the entity that sent an update and is waiting for acknowledgment.

Default Value

1000ms

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compute-change-number

Description

Whether the replication server will compute change numbers. This boolean tells the replication server to compute change numbers for each replicated change by maintaining a change number index database. Changenumbers are computed according to http://tools.ietf.org/html/draft-good-ldap-changelog-04. Note this functionality has an impact on CPU, disk accesses and storage. If changenumbers are not required, it is advisable to set this value to false.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the replication change-log should make records readable only by Directory Server. Throughput and disk space are affected by the more expensive operations taking place. Confidentiality is achieved by encrypting records on all domains managed by this replication server. Encrypting the records prevents unauthorized parties from accessing contents of LDAP operations. For complete protection, consider enabling secure communications between servers.

Change number indexing is not affected by the setting.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately but only affect operations performed after the change.

Advanced Property

No

Read-only

No

degraded-status-threshold

Description

The number of pending changes as threshold value for putting a directory server in degraded status. This value represents a number of pending changes a replication server has in queue for sending to a directory server. Once this value is crossed, the matching directory server goes in degraded status. When number of pending changes goes back under this value, the directory server is put back in normal status. 0 means status analyzer is disabled and directory servers are never put in degraded status.

Default Value

5000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group id for the replication server. This value defines the group id of the replication server. The replication system of a LDAP server uses the group id of the replicated domain and tries to connect, if possible, to a replication with the same group id.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

monitoring-period

Description

The period between sending of monitoring messages. Defines the duration that the replication server will wait before sending new monitoring messages to its peers (replication servers and directory servers). Larger values increase the length of time it takes for a directory server to detect and switch to a more suitable replication server, whereas smaller values increase the amount of background network traffic.

Default Value

60s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

Specifies the number of changes that are kept in memory for each directory server in the Replication Domain.

Default Value

10000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

replication-db-directory

Description

The path where the Replication Server stores all persistent information.

Default Value

changelogDb

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

replication-port

Description

The port on which this Replication Server waits for connections from other Replication Servers or Directory Servers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-purge-delay

Description

The time (in seconds) after which the Replication Server erases all persistent information.

Default Value

3 days

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of other Replication Servers to which this Replication Server tries to connect at startup time. Addresses must be specified using the syntax: "hostname:port". If IPv6 addresses are used as the hostname, they must be specified using the syntax "[IPv6Address]:port".

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server-id

Description

Specifies a unique identifier for the Replication Server. Each Replication Server must have a different server ID.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

weight

Description

The weight of the replication server. The weight affected to the replication server. Each replication server of the topology has a weight. When combined together, the weights of the replication servers of a same group can be translated to a percentage that determines the quantity of directory servers of the topology that should be connected to a replication server. For instance imagine a topology with 3 replication servers (with the same group id) with the following weights: RS1=1, RS2=1, RS3=2. This means that RS1 should have 25% of the directory servers connected in the topology, RS2 25%, and RS3 50%. This may be useful if the replication servers of the topology have a different power and one wants to spread the load between the replication servers according to their power.

Default Value

1

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the Replication Server uses when communicating with other Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-root-dn-prop(1)

Name

dsconfig set-root-dn-prop - Modifies Root DN properties

Synopsis

`dsconfig set-root-dn-prop` {options}

Description

Modifies Root DN properties.

Options

The `dsconfig set-root-dn-prop` command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Root DN properties depend on the Root DN type, which depends on the null option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Root DN properties depend on the Root DN type, which depends on the null option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Root DN properties depend on the Root DN type, which depends on the null option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Root DN properties depend on the Root DN type, which depends on the null option.

Root DN

Root Dns of type root-dn have the following properties:

default-root-privilege-name

Description

Specifies the names of the privileges that root users will be granted by default.

Default Value

bypass-lockdown bypass-acl modify-acl config-read config-write ldif-import ldif-export backend-backup backend-restore server-lockdown server-shutdown server-restart disconnect-client cancel-request password-reset update-schema privilege-change unindexed-search subentry-write changelog-read

Allowed Values

backend-backup

Allows the user to request that the server process backup tasks.

backend-restore

Allows the user to request that the server process restore tasks.

bypass-acl

Allows the associated user to bypass access control checks performed by the server.

bypass-lockdown

Allows the associated user to bypass server lockdown mode.

cancel-request

Allows the user to cancel operations in progress on other client connections.

changelog-read

Allows the user to perform read operations on the changelog

config-read

Allows the associated user to read the server configuration.

config-write

Allows the associated user to update the server configuration. The config-read privilege is also required.

data-sync

Allows the user to participate in data synchronization.

disconnect-client

Allows the user to terminate other client connections.

jmx-notify

Allows the associated user to subscribe to receive JMX notifications.

jmx-read

Allows the associated user to perform JMX read operations.

jmx-write

Allows the associated user to perform JMX write operations.

ldif-export

Allows the user to request that the server process LDIF export tasks.

ldif-import

Allows the user to request that the server process LDIF import tasks.

modify-acl

Allows the associated user to modify the server's access control configuration.

password-reset

Allows the user to reset user passwords.

privilege-change

Allows the user to make changes to the set of defined root privileges, as well as to grant and revoke privileges for users.

proxied-auth

Allows the user to use the proxied authorization control, or to perform a bind that specifies an alternate authorization identity.

server-lockdown

Allows the user to place and bring the server of lockdown mode.

server-restart

Allows the user to request that the server perform an in-core restart.

server-shutdown

Allows the user to request that the server shut down.

subentry-write

Allows the associated user to perform LDAP subentry write operations.

unindexed-search

Allows the user to request that the server process a search that cannot be optimized using server indexes.

update-schema

Allows the user to make changes to the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-root-dse-backend-prop(1)

Name

dsconfig set-root-dse-backend-prop - Modifies Root DSE Backend properties

Synopsis

`dsconfig set-root-dse-backend-prop` {options}

Description

Modifies Root DSE Backend properties.

Options

The `dsconfig set-root-dse-backend-prop` command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Root DSE Backend properties depend on the Root DSE Backend type, which depends on the null option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Root DSE Backend properties depend on the Root DSE Backend type, which depends on the null option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Root DSE Backend properties depend on the Root DSE Backend type, which depends on the null option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Root DSE Backend properties depend on the Root DSE Backend type, which depends on the null option.

Root DSE Backend

Root DSE Backends of type root-dse-backend have the following properties:

show-all-attributes

Description

Indicates whether all attributes in the root DSE are to be treated like user attributes (and therefore returned to clients by default) regardless of the directory server schema configuration.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

show-subordinate-naming-contexts

Description

Indicates whether subordinate naming contexts should be visible in the namingContexts attribute of the RootDSE. By default only top level naming contexts are visible

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-sasl-mechanism-handler-prop(1)

Name

dsconfig set-sasl-mechanism-handler-prop - Modifies SASL Mechanism Handler properties

Synopsis

`dsconfig set-sasl-mechanism-handler-prop` {options}

Description

Modifies SASL Mechanism Handler properties.

Options

The `dsconfig set-sasl-mechanism-handler-prop` command takes the following options:

`--handler-name {name}`

The name of the SASL Mechanism Handler.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

`anonymous-sasl-mechanism-handler`

Default {name}: Anonymous SASL Mechanism Handler

Enabled by default: true

See Anonymous SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`cram-md5-sasl-mechanism-handler`

Default {name}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See Cram MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`digest-md5-sasl-mechanism-handler`

Default {name}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See Digest MD5 SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`external-sasl-mechanism-handler`

Default {name}: External SASL Mechanism Handler

Enabled by default: true

See External SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`gssapi-sasl-mechanism-handler`

Default {name}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See GSSAPI SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`plain-sasl-mechanism-handler`

Default {name}: Plain SASL Mechanism Handler

Enabled by default: true

See Plain SASL Mechanism Handler for the properties of this SASL Mechanism Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the `--handler-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the `--handler-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the `--handler-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the `--handler-name {name}` option.

Anonymous SASL Mechanism Handler

SASL Mechanism Handlers of type anonymous-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.AnonymousSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Cram MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type cram-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper used with this SASL mechanism handler to match the authentication ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Cram MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.CRAMMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Digest MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type digest-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Digest MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.DigestMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realms that is to be used by the server for DIGEST-MD5 authentication. If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Default Value

If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Allowed Values

Any realm string that does not contain a comma.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the server that is used when validating the digest-uri parameter during the authentication process. If this configuration attribute is present, then the server expects that clients use a digest-uri equal to "ldap/" followed by the value of this attribute. For example, if the attribute has a value of "directory.example.com", then the server expects clients to use a digest-uri of "ldap/directory.example.com". If no value is provided, then the server does not attempt to validate the digest-uri provided by the client and accepts any value.

Default Value

The server attempts to determine the fully-qualified domain name dynamically.

Allowed Values

The fully-qualified address that is expected for clients to use when connecting to the server and authenticating via DIGEST-MD5.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

External SASL Mechanism Handler

SASL Mechanism Handlers of type external-sasl-mechanism-handler have the following properties:

certificate-attribute

Description

Specifies the name of the attribute to hold user certificates. This property must specify the name of a valid attribute type defined in the server schema.

Default Value

userCertificate

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-mapper

Description

Specifies the name of the certificate mapper that should be used to match client certificates to user entries.

Default Value

None

Allowed Values

The DN of any Certificate Mapper. The referenced certificate mapper must be enabled when the External SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-validation-policy

Description

Indicates whether to attempt to validate the peer certificate against a certificate held in the user's entry.

Default Value

None

Allowed Values

always

Always require the peer certificate to be present in the user’s entry.

ifpresent

If the user’s entry contains one or more certificates, require that one of them match the peer certificate.

never

Do not look for the peer certificate to be present in the user’s entry.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.ExternalSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

GSSAPI SASL Mechanism Handler

SASL Mechanism Handlers of type gssapi-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the Kerberos principal included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the GSSAPI SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.GSSAPISASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

kdc-address

Description

Specifies the address of the KDC that is to be used for Kerberos processing. If provided, this property must be a fully-qualified DNS-resolvable name. If this property is not provided, then the server attempts to determine it from the system-wide Kerberos configuration.

Default Value

The server attempts to determine the KDC address from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

keytab

Description

Specifies the path to the keytab file that should be used for Kerberos processing. If provided, this is either an absolute path or one that is relative to the server instance root.

Default Value

The server attempts to use the system-wide default keytab.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

principal-name

Description

Specifies the principal name. It can either be a simple user name or a service name such as host/example.com. If this property is not provided, then the server attempts to build the principal name by appending the fully qualified domain name to the string "ldap/".

Default Value

The server attempts to determine the principal name from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realm to be used for GSSAPI authentication.

Default Value

The server attempts to determine the realm from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the system.

Default Value

The server attempts to determine the fully-qualified domain name dynamically .

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Plain SASL Mechanism Handler

SASL Mechanism Handlers of type plain-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Plain SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.PlainSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to

take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-schema-provider-prop(1)

Name

dsconfig set-schema-provider-prop - Modifies Schema Provider properties

Synopsis

`dsconfig set-schema-provider-prop` {options}

Description

Modifies Schema Provider properties.

Options

The `dsconfig set-schema-provider-prop` command takes the following options:

`--provider-name {name}`

The name of the Schema Provider.

Schema Provider properties depend on the Schema Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

`core-schema`

Default {name}: Core Schema

Enabled by default: true

See Core Schema for the properties of this Schema Provider type.

`json-schema`

Default {name}: Json Schema

Enabled by default: true

See Json Schema for the properties of this Schema Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Schema Provider properties depend on the Schema Provider type, which depends on the `--provider-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Schema Provider properties depend on the Schema Provider type, which depends on the `--provider-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Schema Provider properties depend on the Schema Provider type, which depends on the `--provider-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Schema Provider properties depend on the Schema Provider type, which depends on the `--provider-name {name}` option.

Core Schema

Schema Providers of type core-schema have the following properties:

allow-attribute-types-with-no-sup-or-syntax

Description

Indicates whether the schema should allow attribute type definitions that do not declare a superior attribute type or syntax When set to true, invalid attribute type definitions will use the default syntax.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-zero-length-values-directory-string

Description

Indicates whether zero-length (that is, an empty string) values are allowed for directory string. This is technically not allowed by the revised LDAPv3 specification, but some environments may require it for backward compatibility with servers that do allow it.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disabled-matching-rule

Description

The set of disabled matching rules. Matching rules must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled matching rule.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

disabled-syntax

Description

The set of disabled syntaxes. Syntaxes must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled syntax, or NONE

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Core Schema implementation.

Default Value

org.opends.server.schema.CoreSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

json-validation-policy

Description

Specifies the policy that will be used when validating JSON syntax values.

Default Value

strict

Allowed Values

disabled

JSON syntax values will not be validated and, as a result any sequence of bytes will be acceptable.

lenient

JSON syntax values must comply with RFC 7159 except: 1) comments are allowed, 2) single quotes may be used instead of double quotes, and 3) unquoted control characters are allowed in strings.

strict

JSON syntax values must strictly conform to RFC 7159.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-certificates

Description

Indicates whether X.509 Certificate values are required to strictly comply with the standard definition for this syntax. When set to false, certificates will not be validated and, as a result any sequence of bytes will be acceptable.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-country-string

Description

Indicates whether country code values are required to strictly comply with the standard definition for this syntax. When set to false, country codes will not be validated and, as a result any string containing 2 characters will be acceptable.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-jpeg-photos

Description

Indicates whether to require JPEG values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-telephone-numbers

Description

Indicates whether to require telephone number values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strip-syntax-min-upper-bound-attribute-type-description

Description

Indicates whether the suggested minimum upper bound appended to an attribute's syntax OID in it's schema definition Attribute Type Description is stripped off. When retrieving the server's schema, some APIs (JNDI) fail in their syntax lookup methods, because they do not parse this value correctly. This configuration option allows the server to be configured to provide schema definitions these APIs can parse correctly.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

Json Schema

Schema Providers of type json-schema have the following properties:

case-sensitive-strings

Description

Indicates whether JSON string comparisons should be case-sensitive.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ignore-white-space

Description

Indicates whether JSON string comparisons should ignore white-space. When enabled all leading and trailing white space will be removed and intermediate white space will be reduced to a single character.

Default Value

true

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

indexed-field

Description

Specifies which JSON fields should be indexed. A field will be indexed if it matches any of the configured field patterns.

Default Value

All JSON fields will be indexed.

Allowed Values

A JSON pointer which may include wild-cards. A single '**' wild-card matches at most a single path element, whereas a double '*' matches zero or more path elements.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Json Schema implementation.

Default Value

org.opends.server.schema.JsonSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

matching-rule-name

Description

The name of the custom JSON matching rule.

Default Value

The matching rule will not have a name.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

matching-rule-oid

Description

The numeric OID of the custom JSON matching rule.

Default Value

None

Allowed Values

The OID of the matching rule.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-service-discovery-mechanism-prop(1)

Name

dsconfig set-service-discovery-mechanism-prop - Modifies Service Discovery Mechanism properties

Synopsis

`dsconfig set-service-discovery-mechanism-prop` {options}

Description

Modifies Service Discovery Mechanism properties.

Options

The `dsconfig set-service-discovery-mechanism-prop` command takes the following options:

`--mechanism-name {name}`

The name of the Service Discovery Mechanism.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

`replication-service-discovery-mechanism`

Default {name}: Replication Service Discovery Mechanism

Enabled by default: false

See Replication Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`static-service-discovery-mechanism`

Default {name}: Static Service Discovery Mechanism

Enabled by default: false

See Static Service Discovery Mechanism for the properties of this Service Discovery Mechanism type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one

value to it.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the `--mechanism-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the `--mechanism-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the `--mechanism-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the `--mechanism-name {name}` option.

Replication Service Discovery Mechanism

Service Discovery Mechanisms of type replication-service-discovery-mechanism have the following properties:

bind-dn

Description

The bind DN for periodically reading replication server configurations The bind DN must be present on all replication servers and directory servers, it must be able to read the server configuration.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

bind-password

Description

The bind password for periodically reading replication server configurations The bind password must be the same on all replication and directory servers

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

discovery-interval

Description

Interval between two replication server configuration discovery queries. Specifies how frequently to query a replication server configuration in order to discover information about available directory server replicas.

Default Value

60s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.ReplicationServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery

Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-group-id

Description

Replication domain group ID of preferred directory server replicas. Directory server replicas with this replication domain group ID will be preferred over other directory server replicas. Secondary server replicas will only be used when all primary server replicas become unavailable.

Default Value

All the server replicas will be treated the same.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the list of replication servers to contact periodically when discovering server replicas.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to

take effect

Advanced Property

No

Read-only

No

Static Service Discovery Mechanism

Service Discovery Mechanisms of type static-service-discovery-mechanism have the following properties:

discovery-interval

Description

Interval between two server configuration discovery executions. Specifies how frequently to read the configuration of the servers in order to discover their new information.

Default Value

60s

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.StaticServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-server

Description

Specifies a list of servers that will be used in preference to secondary servers when available.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-server

Description

Specifies a list of servers that will be used in place of primary servers when all primary servers are unavailable.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig set-synchronization-provider-prop(1)

Name

dsconfig set-synchronization-provider-prop - Modifies Synchronization Provider properties

Synopsis

`dsconfig set-synchronization-provider-prop` {options}

Description

Modifies Synchronization Provider properties.

Options

The `dsconfig set-synchronization-provider-prop` command takes the following options:

`--provider-name {name}`

The name of the Synchronization Provider.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

`replication-synchronization-provider`

Default {name}: Replication Synchronization Provider

Enabled by default: true

See Replication Synchronization Provider for the properties of this Synchronization Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the `--provider-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the `--provider-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the `--provider-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the `--provider-name {name}` option.

Replication Synchronization Provider

Synchronization Providers of type replication-synchronization-provider have the following properties:

connection-timeout

Description

Specifies the timeout used when connecting to peers and when performing SSL negotiation.

Default Value

5 seconds

Allowed Values

<xinclude:include href="itemizedlist-duration.xml" /> Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Synchronization Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Synchronization Provider implementation.

Default Value

org.opends.server.replication.plugin.MultimasterReplication

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SynchronizationProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-update-replay-threads

Description

Specifies the number of update replay threads. This value is the number of threads created for replaying every updates received for all the replication domains.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-trust-manager-provider-prop(1)

Name

dsconfig set-trust-manager-provider-prop - Modifies Trust Manager Provider properties

Synopsis

`dsconfig set-trust-manager-provider-prop` {options}

Description

Modifies Trust Manager Provider properties.

Options

The `dsconfig set-trust-manager-provider-prop` command takes the following options:

`--provider-name {name}`

The name of the Trust Manager Provider.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

`blind-trust-manager-provider`

Default {name}: Blind Trust Manager Provider

Enabled by default: true

See Blind Trust Manager Provider for the properties of this Trust Manager Provider type.

`file-based-trust-manager-provider`

Default {name}: File Based Trust Manager Provider

Enabled by default: true

See File Based Trust Manager Provider for the properties of this Trust Manager Provider type.

`ldap-trust-manager-provider`

Default {name}: LDAP Trust Manager Provider

Enabled by default: true

See LDAP Trust Manager Provider for the properties of this Trust Manager Provider type.

`pkcs11-trust-manager-provider`

Default {name}: PKCS11 Trust Manager Provider

Enabled by default: true

See PKCS11 Trust Manager Provider for the properties of this Trust Manager Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the `--provider-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the `--provider-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the `--provider-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the `--provider-name {name}` option.

Blind Trust Manager Provider

Trust Manager Providers of type blind-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Blind Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.BlindTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

File Based Trust Manager Provider

Trust Manager Providers of type file-based-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file containing the trust information. It can be an absolute path or a path that is relative to the OpenDJ instance root. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

An absolute path or a path that is relative to the OpenDJ directory server instance root.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the trust store file. Valid values always include 'JKS' and 'PKCS12', but different implementations can allow other values as well. If no value is provided, then the JVM default value is used. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment. The "JKS" and "PKCS12" formats are typically available in Java environments.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

LDAP Trust Manager Provider

Trust Manager Providers of type ldap-trust-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

PKCS11 Trust Manager Provider

Trust Manager Providers of type pkcs11-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11TrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

NoneChanges to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig set-virtual-attribute-prop(1)

Name

dsconfig set-virtual-attribute-prop - Modifies Virtual Attribute properties

Synopsis

`dsconfig set-virtual-attribute-prop` {options}

Description

Modifies Virtual Attribute properties.

Options

The `dsconfig set-virtual-attribute-prop` command takes the following options:

`--name {name}`

The name of the Virtual Attribute.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

`collective-attribute-subentries-virtual-attribute`

Default {name}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See Collective Attribute Subentries Virtual Attribute for the properties of this Virtual Attribute type.

`entity-tag-virtual-attribute`

Default {name}: Entity Tag Virtual Attribute

Enabled by default: true

See Entity Tag Virtual Attribute for the properties of this Virtual Attribute type.

`entry-dn-virtual-attribute`

Default {name}: Entry DN Virtual Attribute

Enabled by default: true

See Entry DN Virtual Attribute for the properties of this Virtual Attribute type.

`entry-uuid-virtual-attribute`

Default {name}: Entry UUID Virtual Attribute

Enabled by default: true

See Entry UUID Virtual Attribute for the properties of this Virtual Attribute type.

`governing-structure-rule-virtual-attribute`

Default {name}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See Governing Structure Rule Virtual Attribute for the properties of this Virtual Attribute type.

`has-subordinates-virtual-attribute`

Default {name}: Has Subordinates Virtual Attribute

Enabled by default: true

See Has Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`is-member-of-virtual-attribute`

Default {name}: Is Member Of Virtual Attribute

Enabled by default: true

See Is Member Of Virtual Attribute for the properties of this Virtual Attribute type.

`member-virtual-attribute`

Default {name}: Member Virtual Attribute

Enabled by default: true

See Member Virtual Attribute for the properties of this Virtual Attribute type.

`num-subordinates-virtual-attribute`

Default {name}: Num Subordinates Virtual Attribute

Enabled by default: true

See Num Subordinates Virtual Attribute for the properties of this Virtual Attribute type.

`password-expiration-time-virtual-attribute`

Default {name}: Password Expiration Time Virtual Attribute

Enabled by default: true

See Password Expiration Time Virtual Attribute for the properties of this Virtual Attribute type.

`password-policy-subentry-virtual-attribute`

Default {name}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See Password Policy Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`structural-object-class-virtual-attribute`

Default {name}: Structural Object Class Virtual Attribute

Enabled by default: true

See Structural Object Class Virtual Attribute for the properties of this Virtual Attribute type.

`subschema-subentry-virtual-attribute`

Default {name}: Subschema Subentry Virtual Attribute

Enabled by default: true

See Subschema Subentry Virtual Attribute for the properties of this Virtual Attribute type.

`user-defined-virtual-attribute`

Default {name}: User Defined Virtual Attribute

Enabled by default: true

See User Defined Virtual Attribute for the properties of this Virtual Attribute type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the `--name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the `--name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the `--name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the `--name {name}` option.

Collective Attribute Subentries Virtual Attribute

Virtual Attributes of type collective-attribute-subentries-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

collectiveAttributeSubentries

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an

entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.CollectiveAttributeSubentriesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Entity Tag Virtual Attribute

Virtual Attributes of type entity-tag-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

etag

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

checksum-algorithm

Description

The algorithm which should be used for calculating the entity tag checksum value.

Default Value

adler-32

Allowed Values

adler-32

The Adler-32 checksum algorithm which is almost as reliable as a CRC-32 but can be computed much faster.

crc-32

The CRC-32 checksum algorithm.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

excluded-attribute

Description

The list of attributes which should be ignored when calculating the entity tag checksum value. Certain attributes like "ds-sync-hist" may vary between replicas due to different purging schedules and should not be included in the checksum.

Default Value

ds-sync-hist

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntityTagVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Entry DN Virtual Attribute

Virtual Attributes of type entry-dn-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryDN

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more

real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryDNVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Entry UUID Virtual Attribute

Virtual Attributes of type entry-uuid-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryUUID

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryUUIDVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Governing Structure Rule Virtual Attribute

Virtual Attributes of type governing-structure-rule-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

governingStructureRule

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.GoverningSturctureRuleVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Has Subordinates Virtual Attribute

Virtual Attributes of type has-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

hasSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the

server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.HasSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Is Member Of Virtual Attribute

Virtual Attributes of type is-member-of-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

isMemberOf

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.IsMemberOfVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Member Virtual Attribute

Virtual Attributes of type member-virtual-attribute have the following properties:

allow-retrieving-membership

Description

Indicates whether to handle requests that request all values for the virtual attribute. This operation can be very expensive in some cases and is not consistent with the primary function of virtual static groups, which is to make it possible to use static group idioms to determine whether a given user is a member. If this attribute is set to false, attempts to retrieve the entire set of values receive an empty set, and only attempts to determine whether the attribute has a specific value or set of values (which is the primary anticipated use for virtual static groups) are handled properly.

Default Value

false

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry

and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those

filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.MemberVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Num Subordinates Virtual Attribute

Virtual Attributes of type num-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

numSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.NumSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Password Expiration Time Virtual Attribute

Virtual Attributes of type password-expiration-time-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

ds-pwp-password-expiration-time

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no

values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordExpirationTimeVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Password Policy Subentry Virtual Attribute

Virtual Attributes of type password-policy-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

pwdPolicySubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordPolicySubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Structural Object Class Virtual Attribute

Virtual Attributes of type structural-object-class-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

structuralObjectClass

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.StructuralObjectClassVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Subschema Subentry Virtual Attribute

Virtual Attributes of type subschema-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

subschemaSubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry

and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those

filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.SubschemaSubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

User Defined Virtual Attribute

Virtual Attributes of type user-defined-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.UserDefinedVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

value

Description

Specifies the values to be included in the virtual attribute.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-work-queue-prop(1)

Name

dsconfig set-work-queue-prop - Modifies Work Queue properties

Synopsis

`dsconfig set-work-queue-prop` {options}

Description

Modifies Work Queue properties.

Options

The `dsconfig set-work-queue-prop` command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Work Queue properties depend on the Work Queue type, which depends on the null option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Work Queue properties depend on the Work Queue type, which depends on the null option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Work Queue properties depend on the Work Queue type, which depends on the null option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Work Queue properties depend on the Work Queue type, which depends on the null option.

Parallel Work Queue

Work Queues of type parallel-work-queue have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Parallel Work Queue implementation.

Default Value

org.opends.server.extensions.ParallelWorkQueue

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.WorkQueue

Multi-valued

No

Required

Yes

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-worker-threads

Description

Specifies the number of worker threads to be used for processing operations placed in the queue. If the value is increased, the additional worker threads are created immediately. If the value is reduced, the appropriate number of threads are destroyed as operations complete processing.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

Traditional Work Queue

Work Queues of type traditional-work-queue have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Traditional Work Queue implementation.

Default Value

org.opends.server.extensions.TraditionalWorkQueue

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.WorkQueue

Multi-valued

No

Required

Yes

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-work-queue-capacity

Description

Specifies the maximum number of queued operations that can be in the work queue at any given time. If the work queue is already full and additional requests are received by the server, then the server front end, and possibly the client, will be blocked until the work queue has available capacity.

Default Value

1000

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

num-worker-threads

Description

Specifies the number of worker threads to be used for processing operations placed in the queue. If the value is increased, the additional worker threads are created immediately. If the value is reduced, the appropriate number of threads are destroyed as operations complete processing.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

OpenDJ Glossary

Abandon operation

LDAP operation to stop processing of a request in progress, after which the directory server drops the connection without a reply to the client application.

Access control

Control to grant or to deny access to a resource.

Access control instruction (ACI)

Instruction added as a directory entry attribute for fine-grained control over what a given user or group member is authorized to do in terms of LDAP operations and access to user data.

ACIs are implemented independently from privileges, which apply to administrative operations.

See also Privilege.

Access control list (ACL)

An access control list connects a user or group of users to one or more security entitlements. For example, users in group sales are granted the entitlement read-only to some financial data.

access log

Directory server log tracing the operations the server processes including timestamps, connection information, and information about the operation itself.

Account lockout

The act of making an account temporarily or permanently inactive after successive authentication failures.

Active user

A user that has the ability to authenticate and use the services, having valid credentials.

Add operation

LDAP operation to add a new entry or entries to the directory.

Anonymous

A user that does not need to authenticate, and is unknown to the system.

Anonymous bind

A bind operation using simple authentication with an empty DN and an empty password, allowing anonymous access such as reading public information.

Approximate index

Index is used to match values that "sound like" those provided in the filter.

Attribute

Properties of a directory entry, stored as one or more key-value pairs. Typical examples include the common name (`cn`) to store the user's full name and variations of the name, user ID (`uid`) to

store a unique identifier for the entry, and `mail` to store email addresses.

audit log

Type of access log that dumps changes in LDIF.

Authentication

The process of verifying who is requesting access to a resource; the act of confirming the identity of a principal.

Authorization

The process of determining whether access should be granted to an individual based on information about that individual; the act of determining whether to grant or to deny a principal access to a resource.

Backend

Repository that a directory server can access to store data. Different implementations with different capabilities exist.

Binary copy

Binary backup archive of one directory server that can be restored on another directory server.

Bind operation

LDAP authentication operation to determine the client's identity in LDAP terms, the identity which is later used by the server to authorize (or not) access to directory data that the client wants to lookup or change.

Branch

The distinguished name (DN) of a non-leaf entry in the Directory Information Tree (DIT), and also that entry and all its subordinates taken together.

Some administrative operations allow you to include or exclude branches by specifying the DN of the branch.

See also Suffix.

Collective attribute

A standard mechanism for defining attributes that appear on all the entries in a particular subtree.

Compare operation

LDAP operation to compare a specified attribute value with the value stored on an entry in the directory.

Control

Information added to an LDAP message to further specify how an LDAP operation should be processed. OpenDJ supports many LDAP controls.

Database cache

Memory space set aside to hold database content.

debug log

Directory server log tracing details needed to troubleshoot a problem in the server.

Delete operation

LDAP operation to remove an existing entry or entries from the directory.

Directory

A directory is a network service which lists participants in the network such as users, computers, printers, and groups. The directory provides a convenient, centralized, and robust mechanism for publishing and consuming information about network participants.

Directory hierarchy

A directory can be organized into a hierarchy in order to make it easier to browse or manage. Directory hierarchies normally represent something in the physical world, such as organizational hierarchies or physical locations. For example, the top level of a directory may represent a company, the next level down divisions, the next level down departments, and down the hierarchy. Alternately, the top level may represent the world, the next level down countries, next states or provinces, and next cities.

Directory Information Tree (DIT)

A set of directory entries organized hierarchically in a tree structure, where the vertices are the entries and the arcs between vertices define relationships between entries

Directory manager

Default Root DN who has privileges to do full administration of the OpenDJ server, including bypassing access control evaluation, changing access controls, and changing administrative privileges.

See also Root DN.

Directory object

A directory object is an item in a directory. Example objects include users, user groups, computers, and more. Objects may be organized into a hierarchy and contain identifying attributes.

See also Entry.

Directory server

Server application for centralizing information about network participants. A highly available directory service consists of multiple directory servers configured to replicate directory data.

See also Directory, Replication.

Directory Services Markup Language (DSML)

Standard language to access directory services using XML. DMSL v1 defined an XML mapping of LDAP objects, while DSMLv2 maps the LDAP Protocol and data model to XML.

Distinguished name (DN)

Fully qualified name for a directory entry, such as `uid=bjensen,ou=People,dc=example,dc=com`, built by concatenating the entry RDN (`uid=bjensen`) with the DN of the parent entry (`ou=People,dc=example,dc=com`).

Dynamic group

Group that specifies members using LDAP URLs.

Entry

As generic and hierarchical data stores, directories always contain different kinds of entries, either nodes (or containers) or leaf entries. An entry is an object in the directory, defined by one of more object classes and their related attributes. At startup, OpenDJ reports the number of entries contained in each suffix.

Entry cache

Memory space set aside to hold frequently accessed, large entries, such as static groups.

Equality index

Index used to match values that correspond exactly (though generally without case sensitivity) to the value provided in the search filter.

errors log

Directory server log tracing server events, error conditions, and warnings, categorized and identified by severity.

Export

Save directory data in an LDIF file.

Extended operation

Additional LDAP operation not included in the original standards. OpenDJ supports several standard LDAP extended operations.

Extensible match index

Index for a matching rule other than approximate, equality, ordering, presence, substring or VLV, such as an index for generalized time.

External user

An individual that accesses company resources or services but is not working for the company. Typically a customer or partner.

Filter

An LDAP search filter is an expression that the server uses to find entries that match a search request, such as `(mail=*@example.com)` to match all entries having an email address in the example.com domain.

Group

Entry identifying a set of members whose entries are also in the directory.

Idle time limit

Defines how long OpenDJ allows idle connections to remain open.

Import

Read in and index directory data from an LDIF file.

Inactive user

An entry in the directory that once represented a user but which is now no longer able to be authenticated.

Index

Directory server backend feature to allow quick lookup of entries based on their attribute values.

See also Approximate index, Equality index, Extensible match index, Ordering index, Presence index, Substring index, Virtual list view (VLV) index, Index entry limit.

Index entry limit

When the number of entries that an index key points to exceeds the index entry limit, OpenDJ stops maintaining the list of entries for that index key.

Internal user

An individual who works within the company either as an employee or as a contractor.

LDAP Data Interchange Format (LDIF)

Standard, portable, text-based representation of directory content. See RFC 2849.

LDAP URL

LDAP Uniform Resource Locator such as `ldap://directory.example.com:389/dc=example,dc=com??sub?(uid=bjensen)`. See RFC 2255.

LDAPS

LDAP over SSL.

Lightweight Directory Access Protocol (LDAP)

A simple and standardized network protocol used by applications to connect to a directory, search for objects and add, edit or remove objects. See RFC 4510.

Lookthrough limit

Defines the maximum number of candidate entries OpenDJ considers when processing a search.

Matching rule

Defines rules for performing matching operations against assertion values. Matching rules are frequently associated with an attribute syntax and are used to compare values according to that syntax. For example, the `distinguishedNameEqualityMatch` matching rule can be used to determine whether two DNs are equal and can ignore unnecessary spaces around commas and equal signs, differences in capitalization in attribute names, and other discrepancies.

Modify DN operation

LDAP modification operation to request that the server change the distinguished name of an entry.

Modify operation

LDAP modification operation to request that the server change one or more attributes of an entry.

Naming context

Base DN under which client applications can look for user data.

Object class

Identifies entries that share certain characteristics. Most commonly, an entry's object classes define the attributes that must and may be present on the entry. Object classes are stored on entries as values of the `objectClass` attribute. Object classes are defined in the directory schema, and can be abstract (defining characteristics for other object classes to inherit), structural (defining the basic structure of an entry, one structural inheritance per entry), or auxiliary (for decorating entries already having a structural object class with other required and optional attributes).

Object identifier (OID)

String that uniquely identifies an object, such as `0.9.2342.19200300.100.1.1` for the user ID attribute or `1.3.6.1.4.1.1466.115.121.1.15` for `DirectoryString` syntax.

Operational attribute

An attribute that has a special (operational) meaning for the directory server, such as `pwdPolicySubentry` or `modifyTimestamp`.

Ordering index

Index used to match values for a filter that specifies a range.

Password policy

A set of rules regarding what sequence of characters constitutes an acceptable password. Acceptable passwords are generally those that would be too difficult for another user or an automated program to guess and thereby defeat the password mechanism. Password policies may require a minimum length, a mixture of different types of characters (lowercase, uppercase, digits, punctuation marks, and other characters), avoiding dictionary words or passwords based on the user's name, and other attributes. Password policies may also require that users not reuse old passwords and that users change their passwords regularly.

Password reset

Password change performed by a user other than the user who owns the entry.

Password storage scheme

Mechanism for encoding user passwords stored on directory entries. OpenDJ implements a number of password storage schemes.

Password validator

Mechanism for determining whether a proposed password is acceptable for use. OpenDJ implements a number of password validators.

Plugin

Java library with accompanying configuration that implements a feature through processing that is not essential to the core operation of OpenDJ directory server.

As the name indicates, plugins can be plugged in to an installed server for immediate configuration and use without recompiling the server.

OpenDJ directory server invokes plugins at specific points in the lifecycle of a client request. The OpenDJ configuration framework lets directory administrators manage plugins with the same tools used to manage the server.

Presence index

Index used to match the fact that an attribute is present on the entry, regardless of the value.

Principal

Entity that can be authenticated, such as a user, a device, or an application.

Privilege

Server configuration settings controlling access to administrative operations such as exporting and importing data, restarting the server, performing password reset, and changing the server configuration.

Privileges are implemented independently from access control instructions (ACI), which apply to LDAP operations and user data.

See also Access control instruction (ACI).

Referential integrity

Ensuring that group membership remains consistent following changes to member entries.

referint log

Directory server log tracing referential integrity events, with entries similar to the errors log.

Referral

Reference to another directory location, which can be another directory server running elsewhere or another container on the same server, where the current operation can be processed.

Relative distinguished name (RDN)

Initial portion of a DN that distinguishes the entry from all other entries at the same level, such as `uid=bjensen` in `uid=bjensen,ou=People,dc=example,dc=com`.

Replication

Data synchronization that ensures all directory servers participating eventually share a consistent set of directory data.

replication log

Directory server log tracing replication events, with entries similar to the errors log.

Root DN

A directory superuser, whose account is specific to a directory server under `cn=Root DNs,cn=config`.

The default Root DN is Directory Manager. You can create additional Root DN accounts, each with different administrative privileges.

See also Directory manager, Privilege.

Root DSE

The directory entry with distinguished name "" (empty string), where DSE is an acronym for DSA-Specific Entry. DSA is an acronym for Directory Server Agent, a single directory server. The root DSE serves to expose information over LDAP about what the directory server supports in terms of LDAP controls, auth password schemes, SASL mechanisms, LDAP protocol versions, naming contexts, features, LDAP extended operations, and other information.

Schema

LDAP schema defines the object classes, attributes types, attribute value syntaxes, matching rules and other constrains on entries held by the directory server.

Search filter

See Filter.

Search operation

LDAP lookup operation where a client requests that the server return entries based on an LDAP filter and a base DN under which to search.

Simple authentication

Bind operation performed with a user's entry DN and user's password. Use simple authentication only if the network connection is secure.

Size limit

Sets the maximum number of entries returned for a search.

Static group

Group that enumerates member entries.

Subentry

An entry, such as a password policy entry, that resides with the user data but holds operational data, and is not visible in search results unless explicitly requested.

Substring index

Index used to match values specified with wildcards in the filter.

Suffix

The distinguished name (DN) of a root entry in the Directory Information Tree (DIT), and also that entry and all its subordinates taken together as a single object of administrative tasks such as export, import, indexing, and replication.

Task

Mechanism to provide remote access to directory server administrative functions. OpenDJ supports tasks to back up and restore backends, to import and export LDIF files, and to stop and restart the server.

Time limit

Defines the maximum processing time OpenDJ devotes to a search operation.

Unbind operation

LDAP operation to release resources at the end of a session.

Unindexed search

Search operation for which no matching index is available. If no indexes are applicable, then the directory server potentially has to go through all entries to look for candidate matches. For this reason, the `unindexed-search` privilege, which allows users to request searches for which no applicable index exists, is reserved for the directory manager by default.

User

An entry that represents an individual that can be authenticated through credentials contained or referenced by its attributes. A user may represent an internal user or an external user, and may be an active user or an inactive user.

User attribute

An attribute for storing user data on a directory entry such as `mail` or `givenname`.

Virtual attribute

An attribute with dynamically generated values that appear in entries but are not persistently stored in the backend.

Virtual directory

An application that exposes a consolidated view of multiple physical directories over an LDAP interface. Consumers of the directory information connect to the virtual directory's LDAP service. Behind the scenes, requests for information and updates to the directory are sent to one or more physical directories where the actual information resides. Virtual directories enable organizations to create a consolidated view of information that for legal or technical reasons cannot be consolidated into a single physical copy.

Virtual list view (VLV) index

Browsing index designed to help the directory server respond to client applications that need, for example, to browse through a long list of results a page at a time in a GUI.

Virtual static group

OpenDJ group that lets applications see dynamic groups as what appear to be static groups.

X.500

A family of standardized protocols for accessing, browsing and maintaining a directory. X.500 is functionally similar to LDAP, but is generally considered to be more complex, and has consequently not been widely adopted.

Appendix A: REST to LDAP Configuration

OpenDJ offers two alternatives for access to directory data over HTTP:

- OpenDJ directory server has an HTTP connection handler that exposes RESTful APIs to directory data over HTTP (or HTTPS). You configure an OpenDJ directory server HTTP connection handler, and the HTTP endpoints that it serves, by using the `dsconfig` command. For each HTTP endpoint served by an HTTP connection handler that exposes your directory data, you configure mappings between JSON resources and LDAP entries.
- The OpenDJ REST to LDAP gateway runs in a Servlet container independent from the directory service. You configure the gateway to access the directory service by editing configuration files for the gateway web application.

Interface stability: Evolving (See "ForgeRock Product Interface Stability")

NOTE	The configuration changed significantly in OpenDJ 3.5.

The files for configuring the gateway and the JSON resource to LDAP entry mappings are in JSON format.

In an OpenDJ directory server installation, the default location for the configuration files is under `/path/to/opendj/config`.

In a REST to LDAP gateway Servlet, the configuration files are under `WEB-INF/classes`.

The format and relative locations of the mapping files are the same for OpenDJ directory server and OpenDJ REST to LDAP gateway. Only OpenDJ REST to LDAP gateway, however, has files for configuring how the gateway connects to LDAP servers, how user identities extracted from HTTP requests map to LDAP user identities, and what LDAP features the gateway uses. In OpenDJ directory server these capabilities are part of the server configuration.

The following list describes the configuration files, indicated by relative location under the configuration directory:

`config.json` **(gateway only)**

This file defines how the gateway connects to LDAP servers, and how user identities extracted from HTTP requests map to LDAP user identities.

For details, see "Gateway Configuration File".

`rest2ldap/rest2ldap.json` **(gateway only)**

This file defines which LDAP features the gateway uses.

For details, see "Gateway REST2LDAP Configuration File".

`rest2ldap/endpoints/base-path/root-resource.json`

These files define JSON resource to LDAP entry mappings.

For details about the configuration fields, see "Mapping Configuration File".

Gateway Configuration File

The `config.json` file for the REST to LDAP gateway can hold the configuration objects described in this section.

The order of the settings in the JSON file is not meaningful. Here, the order shown is that of the default configuration file:

`security`

Configures security parameters for establishing secure connections between the gateway (as a client) and the servers it contacts, such as LDAP directory servers and OAuth 2.0 authorization servers.

This field has the following properties:

`trustManager` **(optional)**

This setting configures how the servers are trusted. This setting is ignored for connections to LDAP servers if `connectionSecurity` is set to `none`:

- `file` means trust server certificates signed by a CA that is trusted according to the file-based truststore configured with `fileBasedTrustManager*` settings described below.
- `jvm` (default) means trust server certificates signed by a CA trusted by the Java environment.
- `trustAll` means blindly trust all server certificates.

> **CAUTION** This setting is not secure and makes man-in-the-middle attacks possible.

`fileBasedTrustManagerType` **(optional)**

If `trustManager` is set to `file`, then this setting configures the format for the data in the truststore file specified by the `fileBasedTrustManagerFile` setting. Formats include the following, though other implementations might be supported as well, depending on the Java environment:

- `JKS` (default) specifies Java Keystore format.
- `PKCS12` specifies Public-Key Cryptography Standards 12 format.

`fileBasedTrustManagerFile`

If `trustManager` is set to `file`, then this setting must specify the location of the truststore file.

Example: `/path/to/truststore`

`fileBasedTrustManagerPasswordFile` **(optional)**

If `trustManager` is set to `file`, then this setting specifies the file containing the truststore password.

Example: `/path/to/pinfile`

`keyManager` **(optional)**

This setting configures how the keys are managed for the gateway when the gateway is acting as a client of an LDAP server or OAuth 2.0 authorization server. The client keys are used to establish a secure connection to a server when the server requires client authentication.

This field can take the following values:

- `jvm` (default) means look for client keys in the default keystore for the Java environment.
- `file` means look for client keys in the specified keystore file, configured with the `fileBasedKeyManager*` settings.
- `pkcs11` means look for client keys in a PKCS #11 cryptographic token, where the PIN file is configured with the `pkcs11KeyManagerPasswordFile` setting described below.

`fileBasedKeyManagerFile`

If `keyManager` is set to `file`, then this setting must specify the keystore file.

Example: `/path/to/keystore`

`fileBasedKeyManagerPasswordFile` **(optional)**

If `keyManager` is set to `file`, then this setting specifies the file containing the keystore password.

Example: `/path/to/pinfile`

`fileBasedKeyManagerType` **(optional)**

If `keyManager` is set to `file`, then this setting specifies the format of the keystore specified by the `fileBasedKeyManagerFile` setting. Formats include the following, though other implementations might be supported as well, depending on the Java environment:

- `JKS` (default) specifies Java Keystore format.
- `PKCS12` specifies Public-Key Cryptography Standards 12 format.

`pkcs11KeyManagerPasswordFile` **(optional)**

If `keyManager` is set to `pkcs11`, then this setting specifies the file containing the PKCS #11 token password.

Example: `/path/to/pinfile`

`ldapConnectionFactories`

Configures how the gateway connects to LDAP servers. This entire configuration object applies only to the REST to LDAP gateway.

Configures at least a connection factory for unauthenticated connections that are used for bind requests. By default, also configures a factory for authenticated connections that are used for searches during authentication and for proxied authorization operations.

The default configuration is set to connect to a local directory server listening for LDAP connections on port 1389, authenticating as the root DN user `cn=Directory Manager`, with the

password `password`:

`bind`

Configures the unauthenticated connection factory for bind operations:

`connectionSecurity` **(optional)**

Whether connections to LDAP servers should be secured by using SSL or StartTLS. The following values are supported:

- `none` (default) means connections use plain LDAP and are not secured.
- `ssl` means connections are secured using LDAPS.
- `startTLS` means connections are secured using LDAP and StartTLS.

If you set `connectionSecurity`, also review the `trustManager` and `fileBasedTrustManager*` settings in the `security` field.

`sslCertAlias` **(optional)**

If secure connections to LDAP servers require client authentication, this identifies the alias of the certificate to use for client authentication when establishing a secure connection.

If you uses this setting because client authentication is required, make sure the `keyManager` settings in the `security` field are properly configured.

If this field is missing, then the certificate is chosen during the SSL handshake.

Example: `client-cert`

`connectionPoolSize` **(optional)**

The gateway creates connection pools to the primary and secondary LDAP servers. The connection pools maintain up to `connectionPoolSize` connections to the servers.

Default: 24

`heartBeatIntervalSeconds` **(optional)**

The gateway tests its connections every `heartBeatIntervalSeconds` to detect whether the connection is still alive. The first test is performed immediately when the gateway gets a connection. Subsequent tests follow every `heartBeatIntervalSeconds`.

Default: 30 (seconds)

`heartBeatTimeoutMilliSeconds` **(optional)**

When the gateway tests a connection, if the heartbeat does not come back after `heartBeatTimeoutMilliSeconds` the connection is marked as closed.

Default: 500 (milliseconds)

`primaryLdapServers` **(required)**

The gateway accesses this array of LDAP servers before failing over to the secondary LDAP servers. These might be LDAP servers in the same data center, for example:

```
{
    "primaryLdapServers": [
        {
            "hostname": "local1.example.com",
            "port": 1389
        },
        {
            "hostname": "local2.example.com",
            "port": 1389
        }
    ]
}
```

By default, the gateway connects to the directory server listening on port 1389 on the local host.

`secondaryLdapServers` **(optional)**

The gateway accesses this array of LDAP servers if primary LDAP servers cannot be contacted. These might be LDAP servers in the same remote data center, for example:

```
{
    "secondaryLdapServers": [
        {
            "hostname": "remote1.example.com",
            "port": 1389
        },
        {
            "hostname": "remote2.example.com",
            "port": 1389
        }
    ]
}
```

No secondary LDAP servers are configured by default.

`root`

Configures the authenticated connection factory:

`inheritFrom` **(optional)**

Identifies the unauthenticated connection factory to inherit the settings from. If this connection factory does not inherit from another configuration object, then you must specify the configuration here.

Default: `bind`

`authentication` **(required)**

The gateway authenticates by simple bind using the credentials specified:

```
{
    "authentication": {
        "bindDn": "cn=Directory Manager",
        "password": "password"
    }
}
```

If the OAuth 2.0 authorization policy is configured for the gateway, then the directory service must be configured to allow the user configured here to perform proxied authorization.

`authorization`

Configures how authorization is performed for REST operations. This entire configuration object applies only to the REST to LDAP gateway.

The default configuration handles authorization by mapping HTTP Basic authentication credentials to LDAP bind credentials. User entries are `inetOrgPerson` entries expected to have `uid=username`, and expected to be found under `ou=people,dc=example,dc=com`.

The default configuration also allows alternative, HTTP header-based authentication in the style of OpenIDM.

To protect passwords, configure HTTPS for the container where the REST to LDAP gateway runs.

This object has the following configuration fields:

`policies`

Which authorization policies are allowed, where the supported policies include:

- `anonymous`
- `basic` (HTTP Basic)
- `oauth2`

When more than one policy is specified, policies are applied in the following order:

1. If the client request has an `Authorization` header, and policies include `oauth2`, the server attempts to apply the OAuth 2.0 policy.
2. If the client request has an `Authorization` header, or has the custom credentials headers specified in the configuration, and policies includes `basic`, the server attempts to apply the Basic Auth policy.
3. Otherwise, if policies includes `anonymous`, and none of the previous policies apply, the server attempts to apply the policy for anonymous requests.

Default: `[ "basic" ]`

`anonymous`

Configuration for authorization when the HTTP connection to the gateway is not authenticated.

Operations are performed using connections from the specified factory:

`ldapConnectionFactory`

Factor providing LDAP connections to use for anonymous HTTP requests.

In effect, you add `"anonymous"` to the array of policies allowed without otherwise changing the default configuration, anonymous HTTP requests result in LDAP requests performed by Directory Manager. Take care to adjust this setting appropriately when allowing anonymous requests.

Default: `root`

`basic`

Configuration for authorization using HTTP Basic credentials.

The HTTP Basic credentials are mapped to LDAP credentials. The LDAP credentials are then used to bind to the directory service.

This object has the following configuration fields:

`supportAltAuthentication`

Whether to allow alternative, HTTP header-based authentication. If this is set to `true`, then the headers containing credentials are specified as the values for `altAuthenticationUsernameHeader` and `altAuthenticationPasswordHeader`, and the bind DN is resolved using a template.

Default: `true`

`altAuthenticationUsernameHeader`

The HTTP header containing the username for authentication when alternative, HTTP header-based authentication is allowed.

Default: `X-OpenIDM-Username`

`altAuthenticationPasswordHeader`

The HTTP header containing the password for authentication when alternative, HTTP header-based authentication is allowed.

Default: `X-OpenIDM-Password`

`bind`

How HTTP Basic credentials are mapped to LDAP credentials used to bind to the directory service.

The following values are supported:

- `search` (default) means the gateway performs a search based on the HTTP Basic user name to obtain the bind DN.
- `sasl-plain` means the gateway transforms the HTTP Basic user name to an authorization ID (authzid) using a template.

- `simple` means the HTTP Basic user name is the LDAP bind DN.

`simple`

How to reuse HTTP Basic credentials for an LDAP simple bind.

This object has the following configuration fields:

`ldapConnectionFactory`

The factory providing LDAP connections to the directory service.

Default: `bind`

`bindDnTemplate`

The template to produce the bind DN from the HTTP Basic user name.

A single occurrence of the string `{username}` is replaced in the template with the HTTP Basic user name.

For example, if the user name is also the UID of the LDAP entry, use `uid={username},ou=People,dc=example,dc=com`.

Default: `{username}`

`sasl-plain`

How to reuse HTTP Basic credentials for an LDAP SASL plain bind.

This object has the following configuration fields:

`ldapConnectionFactory`

The factory providing LDAP connections to the directory service.

Default: `bind`

`authzIdTemplate`

The template to produce the authorization ID from the HTTP Basic user name.

A single occurrence of the string `{username}` is replaced in the template with the HTTP Basic user name.

If the user name is also the authorization ID, use `u:{username}`.

If the user name is the LDAP bind DN, use `dn:{username}`.

`search`

How to reuse HTTP Basic credentials to find the bind DN for an LDAP simple bind.

This object has the following configuration fields:

`searchLdapConnectionFactory`

The factory providing LDAP connections to the directory service for the LDAP search operation.

Default: `root`

`bindLdapConnectionFactory`

The factory providing LDAP connections to the directory service for the LDAP bind operation that uses the bind DN returned by the search.

Default: `bind`

`baseDn`

The base DN for the LDAP search.

Example: `ou=People,dc=example,dc=com`.

`scope`

The scope for the LDAP search.

Use `sub` for a subtree search, `one` for a one-level search.

`filterTemplate`

The template for the filter of the LDAP search.

A single occurrence of the string `{username}` is replaced in the template with the HTTP Basic user name.

If the user name is also the UID, use `(&(uid={username})(objectClass=inetOrgPerson))`.

`oauth2`

Configuration for authorization based on OAuth 2.0, where the gateway plays the role of resource server.

This object has the following configuration fields:

`realm`

Realm associated with access tokens presented to the gateway.

`requiredScopes`

Array of OAuth 2.0 scopes that are required to allow access.

This array must not be empty.

Example: `[ "read", "write", "uid" ]`

`resolver`

How to resolve OAuth 2.0 access tokens presented to the gateway.

Supported values include the following:

- `cts` to resolve tokens in a directory service acting as a Core Token Service (CTS) store for OpenAM
- `openam` to send requests for token resolution to an OpenAM server

- `rfc7662` to send requests for token resolution to an RFC 7622-compliant server

Each access token resolution mechanism has its own configuration.

`accessTokenCache`

How to cache OAuth 2.0 token information to avoid repeating calls for access token resolution.

This object has the following configuration fields:

`enabled`

Whether to cache access token information obtained from the resolver.

Default: `false`

`cacheExpiration`

How long to cache information for a particular token if caching is enabled.

Default: `5 minutes`

`openam`

Configuration for resolving OAuth 2.0 tokens by a request to OpenAM.

This object has the following configuration fields:

`endpointUrl`

OpenAM URL for requests for token information, which depends on OpenAM's OAuth 2.0 authorization server configuration.

Example: `https://openam.example.com:8443/openam/oauth2/tokeninfo`

`sslCertAlias` **(optional)**

If secure connections to the authorization server require client authentication, this identifies the alias of the certificate to use for client authentication when establishing a secure connection.

If you uses this setting because client authentication is required, make sure the `keyManager` settings in the `security` field are properly configured.

If this field is missing, then the certificate is chosen during the SSL handshake.

Example: `client-cert`

`authzIdTemplate`

The template to produce the authorization ID from OAuth 2.0 token information.

A JSON pointer value in braces is replaced in the template with a field value from the JSON returned during token resolution.

This template must start with `u:` or `dn:`.

For example, if token resolution returns a JSON document where the value of the `uid` field is the UID of the user entry in the directory, you might use `u:{uid}` or `dn:{uid},ou=People,dc=example,dc=com`.

`rfc7662`

Configuration for resolving OAuth 2.0 tokens by a request to an RFC 7662-compliant authorization server.

RFC 7662, OAuth 2.0 Token Introspection, defines a standard method for resolving access tokens.

This object has the following configuration fields:

`endpointUrl`

Authorization server URL for requests for token information with HTTP Basic authentication for OAuth 2.0 clients.

Example: `https://as.example.com/introspect`

`sslCertAlias` **(optional)**

If secure connections to the authorization server require client authentication, this identifies the alias of the certificate to use for client authentication when establishing a secure connection.

If you uses this setting because client authentication is required, make sure the `keyManager` settings in the `security` field are properly configured.

If this field is missing, then the certificate is chosen during the SSL handshake.

Example: `client-cert`

`clientId`

OAuth 2.0 client identifier defined during registration with the authorization server.

`clientSecret`

OAuth 2.0 client secret defined during registration with the authorization server.

`authzIdTemplate`

The template to produce the authorization ID from OAuth 2.0 token information.

A JSON pointer value in braces is replaced in the template with a field value from the JSON returned during token resolution.

This template must start with `u:` or `dn:`.

For example, if token resolution returns a JSON document where the value of the `username` field is the UID of the user entry in the directory, you might use `u:{username}` or `dn:{username},ou=People,dc=example,dc=com`.

`cts`

Configuration for resolving OAuth 2.0 tokens when the directory service acts as OpenAM's CTS store.

OpenAM's CTS store is constrained to a specific layout. The `authzIdTemplate` must therefore use `{userName/0}` for the user identifier.

This mechanism makes it possible to resolve access tokens by making a request to the CTS directory service, without making a request to OpenAM. *This mechanism does not, however, ensure that the token requested will have already been replicated to the directory server where the request is routed.*

This object has the following configuration fields:

`ldapConnectionFactory`

The factory providing LDAP connections used to obtain token information from the CTS directory service.

Default: `root`

`baseDn`

The base DN in the CTS directory service where tokens are found.

If the base DN configured for CTS in OpenAM is `dc=cts,dc=example,dc=com`, then use `ou=famrecords,ou=openam-session,ou=tokens,dc=cts,dc=example,dc=com`.

`authzIdTemplate`

The template to produce the authorization ID from OAuth 2.0 token information.

A JSON pointer value in braces is replaced in the template with a field value from the JSON returned during token resolution.

This template must start with `u:` or `dn:`.

In OpenAM CTS, the user name field is an array. For example, if the user name is the UID of the user entry, the use `u:{userName/0}` or `dn:{userName/0},ou=People,dc=example,dc=com`.

Gateway REST2LDAP Configuration File

The `rest2ldap/rest2ldap.json` for the REST to LDAP gateway can hold the configuration objects described in this section.

The order of the settings in the JSON file is not meaningful. Here, the order shown is that of the default configuration file:

`useMvcc`

Whether the gateway supports multi-version concurrency control (MVCC). If true, also specify an `mvccAttribute` to use for MVCC.

Default: `true`

`mvccAttribute`

The LDAP attribute whose value is used for MVCC. Before performing a write operation, the client application can check, for example, whether it is modifying the correct version of a resource by matching the value of the header `If-Match: value`.

Default: `etag`

`readOnUpdatePolicy`

The policy used to read an entry before it is deleted, or to read an entry after it is added or modified. One of the following:

- `controls`: (default) use RFC 4527 read-entry controls to reflect the state of the resource at the time the update was performed.

  The directory service must support RFC 4527.

- `disabled`: do not read the entry or return the resource on update.
- `search`: perform an LDAP search to retrieve the entry before deletion or after it is added or modified.

  The JSON resource returned might differ from the LDAP entry that was updated.

`useSubtreeDelete`

Whether to use the LDAP Subtree Delete request control (OID: `1.2.840.113556.1.4.805`) for LDAP delete operations resulting from delete operations on resources. Clients applications that request deletes for resources with children must have access to use the control.

If this setting is `true`, REST to LDAP attempts to use the control, but falls back to searching for and deleting children if the server rejects the request, because the control is not supported, for example.

Default: `true`

Set this to `false` if the directory server does not support the control.

`usePermissiveModify`

Whether to use the LDAP Permissive Modify request control (OID: `1.2.840.113556.1.4.1413`) for LDAP modify operations resulting from patch and update operations on resources.

Default: `true`

Set this to `false` when using the gateway if the directory server does not support the control.

Mapping Configuration File

The `rest2ldap/endpoints/base-path/root-resource.json` files define how JSON resources map to LDAP entries.

For each base path exposing a REST API, a *base-path* directory holds one or more *root-resource*.json files. In the OpenDJ directory server configuration, the Rest2ldap endpoint `base-path` must match the *base-path* directory name.

Each *root-resource*.json file defines mappings for a specific version of the API. The *root-resource* in the file name must match the name of the root resource defined in the file.

If there is more than one version of the API, then client applications must select the version by setting a version header:

```
Accept-API-Version: resource=version
```

If more than one version of the API is available, and the client application does not select the version by setting a version header, then the latest version is returned.

Here, *version* is the value of the `version` field in the mapping configuration file.

The file `rest2ldap/endpoints/api/example-v1.json` is delivered as an example mapping. This file has the following basic structure:

```
{
  "version": "1.0",          // Version for this API.
  "resourceTypes": {         // Resources for this API.
    "example-v1": {          // Root resource type. Name matches file basename.
      "subResources": {      // The base resource, at /api, is not defined.
        "users": {},         // The subresources at /api/users/ and
        "groups": {}         // /api/groups are defined, however.
      }
    },

    // In addition to the root resource type,
    // the example defines a number of other resource type schemas.
    // These are used to describe the resources exposed under the root resource.
    // In the example file, you can see how these are used for inheritance.
    "frapi:opendj:rest2ldap:object:1.0": {},    // Parent type of all objects.
    "frapi:opendj:rest2ldap:user:1.0": {},      // Basic user type, parent of
    "frapi:opendj:rest2ldap:posixUser:1.0": {}, // user with uid, gid, home dir.
    "frapi:opendj:rest2ldap:group:1.0": {}      // Basic group type.
  }
}
```

The following list describes the individual fields in more detail.

The order of the settings in the JSON file is not meaningful. Here, the order shown is that of the default example configuration file:

`version` **(optional)**

The version string for the root resource of this API.

Valid values are `*`, *integer*, and `integer.integer`, where *integer* is a positive decimal integer.

If the version is set, and the client application sets the request header `Accept-API-Version: resource=version`, The mapping with the matching *version* value is selected.

If more than one version of the API is available, and the client application does not select the version by setting a version header, then the latest version is returned.

Default: `*` (no version specified)

`resourceTypes` **(required)**

The map of resource type names to resource type definitions for this API.

One of the resource type name must match the basename of the mapping file. This resource is referred to as the *root resource* for this version of the API.

The value of a resource type is an object whose properties are described in "Resource Type Properties".

Resource Type Properties

Property	Description
`resourceTypeProperty` (string, required for inheritance)	Name of the resource type property that specifies the type of this resource. REST to LDAP uses this to determine the resource subtype when creating a resource. This points the mapper to the type of the resource. The specified property must be of type `resourceType`.
`properties` (map, optional)	Map of property names to property definitions. Unlike LDAP entries, JSON resources are not necessarily flat. You can define nested properties of type `object` that have their own properties. For details on properties configuration, see "Properties of Resource Type Properties Objects".

Property	Description
`subResources` (map, optional)	Map of subresource names to subresource definitions. The subresource names are URL templates. A URL template sets the relative URL template beneath which the subresources are located. If empty, the subresources are located directly beneath the parent resource. URL templates can set variables in braces `{}`. Any URL template variables will be substituted into the DN template. For example, suppose LDAP entries for devices are located under the following base DNs: • `ou=others,ou=devices,dc=example,dc=com` • `ou=pcs,ou=devices,dc=example,dc=com` • `ou=phones,ou=devices,dc=example,dc=com` • `ou=tablets,ou=devices,dc=example,dc=com` The subresource name `/{type}` would be substituted in actual paths with `/others`, `/pcs`, `/phones`, and `/tablets`. The DN template for the subresource would specify `ou={type},ou=devices,dc=example,dc=com` in order to locate the entries in the correct LDAP organizational unit. In the example, REST to LDAP substitutes `{type}` in the DN template with the type defined in the request URL path. For details on subresource configuration, see "Sub-Resource Properties".
`isAbstract` (boolean, optional)	Whether this is an abstract resource type used only for inheritance. Default: `false`
`superType` (string, optional)	Name of the resource type that this resource type extends. Resource types that extend another type inherit properties of the extended type, and inherit subresource definitions. Default: none. This resource type does not extend another type.
`objectClasses` (array, optional)	Names of the LDAP object classes that this type corresponds to. When an object of this type is created, these object class names are added to the list of object classes on the LDAP entry. The LDAP object classes are not shown in the JSON resource. `Default: none.`

Property	Description
`supportedActions` (array, optional)	Names of the common REST actions that this resource type supports. The names must match actions allowed on the resource in the underlying implementation. Default: none.
`includeAllUserAttributesByDefault` (boolean, optional)	Whether to include all LDAP user attributes as properties of the JSON resource. If `true`, the property names in the JSON resource match the attribute names in the LDAP entries. Default: `false`
`excludedDefaultUserAttributes` (array, optional)	Names of the LDAP user attributes to exclude from the JSON resource when `includeAllUserAttributesByDefault` is `true`. Default: none.

Properties of Resource Type Properties Objects

Property	Description
`type` (string, required)	Determines the type of the mapping property, and therefore which other properties the object has. The type must be one of the following: **`constant`** The property maps the JSON resource property to a fixed value specified by the `value` property. **`object`** The property value is a JSON object with its own type and mapping specified by the object's `properties`. **`reference`** The property maps a JSON field to an LDAP entry found by reference. This is useful for LDAP attributes that reference other entries, such as `manager`, and (group) `member`. When the type is `reference`, the mapping must have the following required properties. • `baseDn` • `ldapAttribute` • `mapper` • `primaryKey` The mapping may have the following optional properties. • `isMultiValued` • `isRequired` • `searchFilter` • `writability` **`resourceType`** The property value is the name of a resource type defined in this mapping file. The name of the property with this type should match the `resourceTypeProperty` name. For example, if `"resourceTypeProperty": "_schema"` then the following should be specified or inherited: `"_schema": { "type": "resourceType" }`.

Property	Description
`baseDn`	Indicates the base LDAP DN under which to find entries referenced by the JSON resource. For example, a group could reference users and groups under `dc=example,dc=com`.
`defaultJsonValue`	Sets the JSON value if no corresponding LDAP attribute is present. No default is set if this is omitted.
`isBinary`	Whether the underlying LDAP attribute holds a binary value, such as a JPEG photo or a digital certificate. If `true`, the JSON property takes the base64-encoded value. Binary values can also be handled directly as described in "Working With Alternative Content Types" in the *Directory Server Developer's Guide*. Default: `false`.
`isMultiValued`	Whether the JSON resource property can take an array value. Most LDAP attributes can take multiple values. A literal-minded mapping from LDAP to JSON would therefore be full of array properties, many with only one value. To minimize inconvenience, REST to LDAP generally returns single value scalars, even when the underlying LDAP attribute is multi-valued. If this property is omitted or set to `false`, then the JSON resource contains the first value returned for multi-valued LDAP attributes with more than value. If this property is `true`, then if the LDAP attribute only has one value, it is returned as a scalar. If the LDAP attribute has more than one value, the values are returned in an array. Default: `false`
`isRequired`	`true` means the LDAP attribute is mandatory and must be provided to create the resource; `false` means it is optional. Default: `false`.

Property	Description
`ldapAttribute`	Specifies the LDAP attribute in the entry underlying the JSON resource whose value points to the referenced entry. For example, a `manager` attribute value is the DN of the manager's entry. Default: use the name of the JSON property. For example, the JSON property `description` maps to the LDAP attribute `description` by default.
`mapper`	Describes how the referenced entry content maps to the content of this JSON property. A mapper object is a properties object of its own.
`primaryKey`	Indicates which LDAP attribute in the mapper holds the primary key to the referenced entry.
`searchFilter`	Specifies the LDAP filter to use to search for the referenced entry. Default: `"(objectClass=*)"`
`value`	Use with `"type": "constant"` to specify the constant value.
`writability`	Indicates whether the mapping supports updates. The `writability` property takes one of the following values: • `createOnly`: This attribute can be set only when the entry is created. Attempts to update this attribute thereafter result in errors. • `createOnlyDiscardWrites`: This attribute can be set only when the entry is created. Attempts to update this attribute thereafter do not result in errors. Instead the update value is discarded. • `readOnly`: This attribute cannot be written. Attempts to write this attribute result in errors. • `readOnlyDiscardWrites`: This attribute cannot be written. Attempts to write this attribute do not result in errors. Instead the value to write is discarded. • `readWrite`: (default) This attribute can be set at creation and updated thereafter.

Sub-Resource Properties

Property	Description

`type` (string, required)	The type of this subresource, either `collection` or `singleton`.
	
	`A collection subresource is a container for other resources, which can be created, read, updated, deleted, patched, and queried.`
	`A collection definition has the following required properties:`
	
	• `namingStrategy`
	• `resource`
	
	A collection definition has the following optional properties:
	
	• `dnTemplate`
	• `glueObjectClasses`
	• `isReadOnly`
	
	A singleton subresource is a resource with no children. A singleton definition has the following required properties:
	
	• `resource`
	
	A singleton definition has the following optional properties:
	
	• `dnTemplate`
	• `isReadOnly`

`dnTemplate` (string, optional)	Sets the relative DN template beneath which the subresource LDAP entries are located. If this is an empty string, the LDAP entries are located directly beneath the parent LDAP entry. DN templates can use variables in braces `{}`. DN template variables are substituted using values extracted from the URL template. Default: empty string
`glueObjectClasses` (array, required if the DN template contains one or more RDNs)	Specifies one or more LDAP object class names associated with any intermediate "glue" entries forming the DN template. Default: no object classes are specified
`isReadOnly` (boolean, optional)	Whether this resource is read-only. Default: `false`

Property	Description

`namingStrategy` (object, required)	Specifies the approach used to map LDAP entry names to JSON resources.
	
	LDAP entries mapped to JSON resources must be immediate subordinates of the mapping's `baseDn`. The following naming strategies are supported:
	
	• RDN and resource ID are both derived from a single user attribute in the LDAP entry, as in the following example, where the `uid` attribute is the RDN and its value is the JSON resource ID:
	
	`{ "namingStrategy": { "type": "clientDnNaming", "dnAttribute": "uid" } }`
	
	• RDN and resource ID are derived from separate user attributes in the LDAP entry, as in the following example, where the RDN attribute is `uid`, but the JSON resource ID is the value of the `mail` attribute:
	
	`{ "namingStrategy": { "type": "clientNaming", "dnAttribute": "uid", "idAttribute": "mail" } }`
	
	• RDN is derived from a user attribute and the resource ID from an operational attribute in the LDAP entry, as in the following example, where the RDN attribute is `uid`, but the JSON resource ID is the value of the `entryUUID` operational attribute:
	
	`{ "namingStrategy": { "type": "serverNaming", "dnAttribute": "uid", "idAttribute": "entryUUID" } }`

Property	Description
`resource` (string, required)	Specifies the resource type name of the subresource. A collection can contain objects with different subresource types as long as all types inherit from the same super type. In that case, set `resource` to the super type name.

Appendix B: REST to LDAP Configuration (3.0)

NOTE This appendix applies to OpenDJ 3.0. For the version that applies to OpenDJ 3.5 and later, see "REST to LDAP Configuration".

OpenDJ offers two alternatives for RESTful access to directory data:

- OpenDJ directory server has an HTTP connection handler that exposes the RESTful API over HTTP (or HTTPS). You configure the mapping between JSON resources and LDAP entries by editing the configuration file for the HTTP connection handler, by default `/path/to/opendj/config/http-config.json`.
- The OpenDJ REST to LDAP gateway runs as a Servlet independent from your directory service. You configure the gateway to access your directory service by editing `opendj-rest2ldap-servlet.json` where you deploy the gateway web application.

The JSON format configuration can hold the following configuration objects. Some of the configuration settings are available only in the REST LDAP gateway configuration. The order here is the order shown in the default configuration file:

Interface stability: Evolving (See "ForgeRock Product Interface Stability")

"ldapConnectionFactories" (required, gateway only)

Configures how the gateway connects to LDAP servers. This entire configuration object applies only to the REST to LDAP gateway.

Configures at least a connection factory for unauthenticated connections that are used for bind requests. By default, also configures a factory for authenticated connections that are used for searches during authentication and for proxied authorization operations.

The default configuration is set to connect to a local directory server listening for LDAP connections on port 1389, authenticating as the root DN user `cn=Directory Manager`, with the password `password`:

"default"

Configures the unauthenticated connection factory for bind operations:

"connectionPoolSize" (optional)

The gateway creates connection pools to the primary and secondary LDAP servers that maintain up to `connectionPoolSize` connections to the servers.

Default: 24

```
"connectionPoolSize": 24
```

"connectionSecurity" (optional)

Whether connections to LDAP servers should be secured by using SSL or StartTLS. The following values are supported:

- "none" (default) means connections use plain LDAP and are not secured.
- "ssl" means connections are secured using LDAPS.
- "startTLS" means connections are secured using LDAP and StartTLS.

If you set "connectionSecurity", also review the "trustManager" and "fileBasedTrustManager*" settings.

"heartBeatIntervalSeconds" (optional)

The gateway tests its connections every `heartBeatIntervalSeconds` to detect whether the connection is still alive. The first test is performed immediately when the gateway gets a connection. Subsequent tests follow every `heartBeatIntervalSeconds`.

Default: 30 (seconds)

```
"heartBeatIntervalSeconds": 30
```

"heartBeatTimeoutMilliSeconds" (optional)

When the gateway tests a connection, if the heartbeat does not come back after `heartBeatTimeoutMilliSeconds` the connection is marked as closed.

Default: 500 (milliseconds)

```
"heartBeatTimeoutMilliSeconds": 500
```

"fileBasedTrustManagerFile" (optional)

If "trustManager" is set to "file", then this setting configures the location of the truststore file.

Default: "/path/to/truststore"

"fileBasedTrustManagerPassword" (optional)

If "trustManager" is set to "file", then this setting specifies the truststore password.

Default: "password"

"fileBasedTrustManagerType" (optional)

If "trustManager" is set to "file", then this setting configures the format for the data in the truststore file specified by the "fileBasedTrustManagerFile" setting. Formats include the following, though other implementations might be supported as well depending on the

Java environment:

- "JKS" (default) specifies Java Keystore format.
- "PKCS12" specifies Public-Key Cryptography Standards 12 format.

"primaryLDAPServers" (required)

The gateway accesses this array of LDAP servers before failing over to the secondary LDAP servers. These might be LDAP servers in the same data center, for example:

```
{
    "primaryLDAPServers": [
        {
            "hostname": "local1.example.com",
            "port": 1389
        },
        {
            "hostname": "local2.example.com",
            "port": 1389
        }
    ]
}
```

By default, the gateway connects to the directory server listening on port 1389 on the local host.

"secondaryLDAPServers" (optional)

The gateway accesses this array of LDAP servers if primary LDAP servers cannot be contacted. These might be LDAP servers in the same data center, for example:

```
{
    "secondaryLDAPServers": [
        {
            "hostname": "remote1.example.com",
            "port": 1389
        },
        {
            "hostname": "remote2.example.com",
            "port": 1389
        }
    ]
}
```

No secondary LDAP servers are configured by default.

"trustManager" (optional)

If "connectionSecurity" is set to "ssl" or "startTLS", then this setting configures how the LDAP servers are trusted. This setting is ignored if "connectionSecurity" is set to "none":

- "file" means trust the LDAP server certificate if it is signed by a Certificate Authority (CA) trusted according to the file-based truststore configured with the "fileBasedTrustManager*" settings.
- "jvm" means trust the LDAP server certificate if it is signed by a CA trusted by the Java environment.
- "trustAll" (default) means blindly trust all LDAP server certificates.

"root"

Configures the authenticated connection factory:

"inheritFrom" (optional)

Identifies the unauthenticated connection factory from which to inherit settings. If this connection factory does not inherit from another configuration object, then you must specify the configuration here.

Default: "default"

"authentication" (required)

The gateway authenticates by simple bind using the credentials specified:

```
{
    "authentication": {
        "bindDN": "cn=Directory Manager",
        "password": "password"
    }
}
```

"authenticationFilter" (required)

Configures the REST to LDAP authentication filter. If the configuration is not present, the filter is disabled.

The default configuration allows HTTP Basic authentication where user entries are `inetOrgPerson` entries expected to have `uid=username`, and to be found under `ou=people,dc=example,dc=com`. The default configuration also allows alternative, HTTP header based authentication in the style of OpenIDM.

By default, authentication is required both for the gateway and for the HTTP connection handler. When the HTTP connection handler property `authentication-required` is set to `false` (default: `true`), the HTTP connection handler accepts both authenticated and unauthenticated requests. All requests are subject to access control and resource limit settings in the same way as LDAP client requests to the directory server. The `authentication-required` setting can be overridden by the global configuration property `reject-unauthenticated-requests` (default: `false`), described in "Restricting Client Access" in the *Administration Guide*.

To protect passwords, configure HTTPS for the HTTP connection handler or for the container where the REST to LDAP gateway runs.

The filter has the following configuration fields:

"supportHTTPBasicAuthentication"

Whether to support HTTP Basic authentication. If this is set to `true`, then the entry corresponding to the user name is found using the "searchBaseDN", "searchScope", and "searchFilterTemplate" settings.

Default: `true`

"supportAltAuthentication"

Whether to allow alternative, HTTP header based authentication. If this is set to `true`, then the headers to use are specified in the "altAuthenticationUsernameHeader" and "altAuthenticationPasswordHeader" values, and the bind DN is resolved using the "searchFilterTemplate" value.

Default: `true`

"altAuthenticationUsernameHeader"

Specifies the HTTP header containing the username for authentication when alternative, HTTP-header based authentication is allowed.

Default: "X-OpenIDM-Username"

"altAuthenticationPasswordHeader"

Specifies the HTTP header containing the password for authentication when alternative, HTTP-header based authentication is allowed.

Default: "X-OpenIDM-Password"

"reuseAuthenticatedConnection" (gateway only)

Whether to use authenticated LDAP connections for subsequent LDAP operations. If this is set to `true`, the gateway does not need its own connection factory, nor does it need to use proxied authorization for LDAP operations. Instead, it performs the operations as the user on the authenticated connection.

Default: `true`

"method" (gateway only)

Specifies the authentication method used by the gateway. The following values are supported:

- "search-simple" (default) means the user name is resolved to an LDAP bind DN by a search using the "searchFilterTemplate" value.
- "sasl-plain" means the user name is resolved to an authorization ID (authzid) using the "saslAuthzIdTemplate" value.
- "simple" means the user name is the LDAP bind DN.

"bindLDAPConnectionFactory" (gateway only)

Identifies the factory providing connections used for bind operations to authenticate users to LDAP servers.

Default: "default"

"saslAuthzIdTemplate" (gateway only)

Sets how to resolve the authorization ID when the authentication "method" is set to "sasl-plain", substituting `%s` in the template with the user name provided. The user name provided by is DN escaped before the value is returned.

Default: "dn:uid=%s,ou=people,dc=example,dc=com"

"searchLDAPConnectionFactory" (gateway only)

Identifies the factory providing connections used to find user entries in the directory server when the "method" is set to "search-simple".

Default: "root"

"searchBaseDN"

Sets the base DN to search for user entries. For the gateway, this applies when the "method" is set to "search-simple". This always applies for the HTTP connection handler.

Default: "ou=people,dc=example,dc=com"

"searchScope"

Sets the search scope below the base DN such as "sub" (subtree search) or "one" (one-level search) to search for user entries. For the gateway, this applies when the "method" is set to "search-simple". This always applies for the HTTP connection handler.

Default: "sub"

"searchFilterTemplate"

Sets the search filter used to find the user entry, substituting `%s` in the template with the user name provided. The user name provided by is DN escaped before the value is returned. For the gateway, this applies when the "method" is set to "search-simple". This always applies for the HTTP connection handler.

Default: "(&(uid=%s)(objectClass=inetOrgPerson))"

"servlet" (required)

Configures how HTTP resources map to LDAP entries, and for the gateway how to connect to LDAP servers and how to use proxied authorization.

The default gateway configuration tries to reuse authenticated connections for LDAP operations, falling back to a connection authenticated as root DN using proxied authorization for LDAP operations:

"ldapConnectionFactory" (gateway only)

Specifies the connection factory used by the gateway to perform LDAP operations if an authenticated connection is not passed from the authentication filter according to the setting for "reuseAuthenticatedConnection".

Default: "root"

"authorizationPolicy" (gateway only)

Specifies how to handle LDAP authorization. The following values are supported:

- "proxy" (default) means use proxied authorization when no authenticated connection is provided for reuse, resolving the authorization ID according to the setting for "proxyAuthzIdTemplate".
- "none" means do not use proxied authorization and do not reuse authenticated connections, but instead use connections from the factory specified in "ldapConnectionFactory".
- "reuse" means reuse an authenticated connection passed by the filter, and fail if no connection was passed by the filter.

"proxyAuthzIdTemplate" (gateway only)

Specifies the template to derive the authorization ID from the security context created during authentication. Use `{dn}` to indicate the user's bind DN or `{id}` to indicate the user name provided for authentication.

Default: "dn:{dn}"

"mappings"

For each collection URI such as `/users` and `/groups`, you configure a mapping between the JSON resource returned over HTTP, and the LDAP entry returned by the directory service.

Each mapping has a number of configuration elements:

"baseDN" (required)

The base DN where LDAP entries are found for this mapping.

"readOnUpdatePolicy" (optional)

The policy used to read an entry before it is deleted, or to read an entry after it is added or modified. One of the following:

- "controls": (default) use RFC 4527 read-entry controls to reflect the state of the resource at the time the update was performed.

  The directory service must support RFC 4527.

- "disabled": do not read the entry or return the resource on update.
- "search": perform an LDAP search to retrieve the entry before deletion or after it is added or modified.

  The JSON resource returned might differ from the LDAP entry that was updated.

"useSubtreeDelete" (required)

Whether to use the LDAP Subtree Delete request control (OID: `1.2.840.113556.1.4.805`) for LDAP delete operations resulting from delete operations on resources.

Default: `false`. The default configuration uses `false`.

Set this to `true` if you want this behavior, if your directory server supports the control, and if clients that request delete operations have access to use the control.

"usePermissiveModify" (required)

Whether to use the LDAP Permissive Modify request control (OID: `1.2.840.113556.1.4.1413`) for LDAP modify operations resulting from patch and update operations on resources.

Default: `false`. The default configuration uses `true`.

Set this to `false` when using the gateway if your directory server does not support the control.

"etagAttribute" (optional)

The LDAP attribute to use for multi-version concurrency control (MVCC).

Default: "etag"

"namingStrategy" (required)

The approach used to map LDAP entry names to JSON resources.

LDAP entries mapped to JSON resources must be immediate subordinates of the mapping's "baseDN".

The following naming strategies are supported:

- RDN and resource ID are both derived from a single user attribute in the LDAP entry, as in the following example, where the `uid` attribute is the RDN and its value is the JSON resource ID:

```
{
    "namingStrategy": {
        "strategy": "clientDNNaming",
        "dnAttribute": "uid"
    }
}
```

- RDN and resource ID are derived from separate user attributes in the LDAP entry, as in the following example where the RDN attribute is `uid` but the JSON resource ID is the value of the `mail` attribute:

```
{
    "namingStrategy": {
        "strategy": "clientNaming",
        "dnAttribute": "uid",
        "idAttribute": "mail"
    }
}
```

- RDN is derived from a user attribute and the resource ID from an operational attribute in the LDAP entry, as in the following example, where the RDN attribute is `uid` but the JSON resource ID is the value of the `entryUUID` operational attribute:

```
{
    "namingStrategy": {
        "strategy": "serverNaming",
        "dnAttribute": "uid",
        "idAttribute": "entryUUID"
    }
}
```

"additionalLDAPAttributes" (optional, but necessary)

LDAP attributes to include during LDAP add operations as an array of type-value lists, such as the following example:

```
{
    "additionalLDAPAttributes": [
        {
            "type": "objectClass",
            "values": [
                "top",
                "person",
                "organizationalPerson",
                "inetOrgPerson"
            ]
        }
    ]
}
```

This configuration element is useful to set LDAP object classes, for example, which are not present in JSON resources.

"attributes" (required)

How the JSON resource fields map to attributes on LDAP entries, each taking the form "*field-name*": *mapping-object*. A number of *mapping-object*s are supported:

"constant"

Maps a single JSON attribute to a fixed value.

This can be useful as in the default case where each JSON resource "schemas" takes the SCIM URN, and so the value is not related to the underlying LDAP entries:

```
{
    "schemas": {
        "constant": [
            "urn:scim:schemas:core:1.0"
```

```
        ]
    }
}
```

"simple"

Maps a JSON field to an LDAP attribute.

Simple mappings are used where the correspondence between JSON fields and LDAP attributes is one-to-one:

```
{
    "userName": {
        "simple": {
            "ldapAttribute": "mail",
            "isSingleValued": true,
            "writability": "readOnly"
        }
    }
}
```

Simple mappings can take a number of fields:

- (Required) "ldapAttribute": the name of LDAP attribute.
- (Optional) "defaultJSONValue": the JSON value if no LDAP attribute is available on the entry.

  No default is set if this is omitted.

- (Optional) "isBinary": true means the LDAP attribute is binary and the JSON field gets the base64-encoded value.

  Default: `false`

- (Optional) "isRequired": true means the LDAP attribute is mandatory and must be provided to create the resource; false means it is optional.

  Default: `false`

- (Optional) "isSingleValued": true means represent a possibly multi-valued LDAP attribute as a single value; false means represent it as an array of values.

  Default: determine the representation based on the LDAP schema, so SINGLE-VALUE attributes take single values, and multi-valued attributes take arrays.

- (Optional) "writability": indicates whether the LDAP attribute supports updates. This field can take the following values:
  - "createOnly": This attribute can be set only when the entry is created. Attempts to update this attribute thereafter result in errors.

- "createOnlyDiscardWrites": This attribute can be set only when the entry is created. Attempts to update this attribute thereafter do not result in errors. Instead the update value is discarded.
- "readOnly": This attribute cannot be written. Attempts to write this attribute result in errors.
- "readOnlyDiscardWrites": This attribute cannot be written. Attempts to write this attribute do not result in errors. Instead the value to write is discarded.
- "readWrite": (default) This attribute can be set at creation and updated thereafter.

"object"

Maps a JSON object to LDAP attributes.

This mapping lets you create JSON objects whose fields themselves have mappings to LDAP attributes.

"reference"

Maps a JSON field to an LDAP entry found by reference.

This mapping works for LDAP attributes whose values reference other entries. This is shown in the following example from the default configuration. The LDAP `manager` attribute values are user entry DNs. Here, the JSON `manager` field takes the user ID and name from the entry referenced by the LDAP attribute. On updates, changes to the JSON manager `_id` affect which manager entry is referenced, yet any changes to the manager's name are discarded, because changing managers only affects which user entry to point to, not the referenced user's name:

```
{
    "manager": {
        "reference": {
            "ldapAttribute": "manager",
            "baseDN": "ou=people,dc=example,dc=com",
            "primaryKey": "uid",
            "mapper": {
                "object": {
                    "_id": {
                        "simple": {
                            "ldapAttribute": "uid",
                            "isSingleValued": true,
                            "isRequired": true
                        }
                    },
                    "displayName": {
                        "simple": {
                            "ldapAttribute": "cn",
                            "isSingleValued": true,
                            "writability": "readOnlyDiscardWrites"
                        }
```

```
                    }
                }
            }
        }
    }
}
```

Babs Jensen's manager in the sample LDAP data is Torrey Rigden, who has user ID `trigden`. Babs's entry has `manager: uid=trigden,ou=People,dc=example,dc=com`. With this mapping, the resulting JSON field is the following:

```
{
    "manager": [
        {
            "_id": "trigden",
            "displayName": "Torrey Rigden"
        }
    ]
}
```

Reference mapping objects have the following fields:

- (Required) "baseDN": indicates the base LDAP DN under which to find entries referenced by the JSON resource.
- (Required) "ldapAttribute": specifies the LDAP attribute in the entry underlying the JSON resource whose value points to the referenced entry.
- (Required) "mapper": describes how the referenced entry content maps to the content of this JSON field.
- (Required) "primaryKey": indicates which LDAP attribute in the mapper holds the primary key to the referenced entry.
- (Optional) "isRequired": true means the LDAP attribute is mandatory and must be provided to create the resource; false means it is optional.

  Default: `false`

- (Optional) "isSingleValued": true means represent a possibly multi-valued LDAP attribute as a single value; false means represent it as an array of values.

  Default: `false`

- (Optional) "searchFilter": specifies the LDAP filter to use to search for the referenced entry. The default is `"(objectClass=*)"`.
- (Optional) "writability": indicates whether the mapping supports updates, as described above for the simple mapping. The default is "readWrite".

The default mappings expose a SCIM view of user and group data:

```
{
    "/users": {
        "baseDN": "ou=people,dc=example,dc=com",
        "readOnUpdatePolicy": "controls",
        "useSubtreeDelete": false,
        "usePermissiveModify": true,
        "etagAttribute": "etag",
        "namingStrategy": {
            "strategy": "clientDNNaming",
            "dnAttribute": "uid"
        },
        "additionalLDAPAttributes": [
            {
                "type": "objectClass",
                "values": [
                    "top",
                    "person",
                    "organizationalPerson",
                    "inetOrgPerson"
                ]
            }
        ],
        "attributes": {
            "schemas": {
                "constant": [
                    "urn:scim:schemas:core:1.0"
                ]
            },
            "_id": {
                "simple": {
                    "ldapAttribute": "uid",
                    "isSingleValued": true,
                    "isRequired": true,
                    "writability": "createOnly"
                }
            },
            "_rev": {
                "simple": {
                    "ldapAttribute": "etag",
                    "isSingleValued": true,
                    "writability": "readOnly"
                }
            },
            "userName": {
                "simple": {
                    "ldapAttribute": "mail",
                    "isSingleValued": true,
                    "writability": "readOnly"
                }
            },
```

```
            "displayName": {
                "simple": {
                    "ldapAttribute": "cn",
                    "isSingleValued": true,
                    "isRequired": true
                }
            },
            "name": {
                "object": {
                    "givenName": {
                        "simple": {
                            "ldapAttribute": "givenName",
                            "isSingleValued": true
                        }
                    },
                    "familyName": {
                        "simple": {
                            "ldapAttribute": "sn",
                            "isSingleValued": true,
                            "isRequired": true
                        }
                    }
                }
            },
            "manager": {
                "reference": {
                    "ldapAttribute": "manager",
                    "baseDN": "ou=people,dc=example,dc=com",
                    "primaryKey": "uid",
                    "mapper": {
                        "object": {
                            "_id": {
                                "simple": {
                                    "ldapAttribute": "uid",
                                    "isSingleValued": true,
                                    "isRequired": true
                                }
                            },
                            "displayName": {
                                "simple": {
                                    "ldapAttribute": "cn",
                                    "isSingleValued": true,
                                    "writability": "readOnlyDiscardWrites"
                                }
                            }
                        }
                    }
                }
            },
            "groups": {
                "reference": {
```

```
                    "ldapAttribute": "isMemberOf",
                    "baseDN": "ou=groups,dc=example,dc=com",
                    "writability": "readOnly",
                    "primaryKey": "cn",
                    "mapper": {
                        "object": {
                            "_id": {
                                "simple": {
                                    "ldapAttribute": "cn",
                                    "isSingleValued": true
                                }
                            }
                        }
                    }
                }
            },
            "contactInformation": {
                "object": {
                    "telephoneNumber": {
                        "simple": {
                            "ldapAttribute": "telephoneNumber",
                            "isSingleValued": true
                        }
                    },
                    "emailAddress": {
                        "simple": {
                            "ldapAttribute": "mail",
                            "isSingleValued": true
                        }
                    }
                }
            },
            "meta": {
                "object": {
                    "created": {
                        "simple": {
                            "ldapAttribute": "createTimestamp",
                            "isSingleValued": true,
                            "writability": "readOnly"
                        }
                    },
                    "lastModified": {
                        "simple": {
                            "ldapAttribute": "modifyTimestamp",
                            "isSingleValued": true,
                            "writability": "readOnly"
                        }
                    }
                }
            }
        }
```

```
    },
    "/groups": {
        "baseDN": "ou=groups,dc=example,dc=com",
        "readOnUpdatePolicy": "controls",
        "useSubtreeDelete": false,
        "usePermissiveModify": true,
        "etagAttribute": "etag",
        "namingStrategy": {
            "strategy": "clientDNNaming",
            "dnAttribute": "cn"
        },
        "additionalLDAPAttributes": [
            {
                "type": "objectClass",
                "values": [
                    "top",
                    "groupOfUniqueNames"
                ]
            }
        ],
        "attributes": {
            "schemas": {
                "constant": [
                    "urn:scim:schemas:core:1.0"
                ]
            },
            "_id": {
                "simple": {
                    "ldapAttribute": "cn",
                    "isSingleValued": true,
                    "isRequired": true,
                    "writability": "createOnly"
                }
            },
            "_rev": {
                "simple": {
                    "ldapAttribute": "etag",
                    "isSingleValued": true,
                    "writability": "readOnly"
                }
            },
            "displayName": {
                "simple": {
                    "ldapAttribute": "cn",
                    "isSingleValued": true,
                    "isRequired": true,
                    "writability": "readOnly"
                }
            },
            "members": {
                "reference": {
```

```
                    "ldapAttribute": "uniqueMember",
                    "baseDN": "dc=example,dc=com",
                    "primaryKey": "uid",
                    "mapper": {
                        "object": {
                            "_id": {
                                "simple": {
                                    "ldapAttribute": "uid",
                                    "isSingleValued": true,
                                    "isRequired": true
                                }
                            },
                            "displayName": {
                                "simple": {
                                    "ldapAttribute": "cn",
                                    "isSingleValued": true,
                                    "writability": "readOnlyDiscardWrites"
                                }
                            }
                        }
                    }
                }
            },
            "meta": {
                "object": {
                    "created": {
                        "simple": {
                            "ldapAttribute": "createTimestamp",
                            "isSingleValued": true,
                            "writability": "readOnly"
                        }
                    },
                    "lastModified": {
                        "simple": {
                            "ldapAttribute": "modifyTimestamp",
                            "isSingleValued": true,
                            "writability": "readOnly"
                        }
                    }
                }
            }
        }
    }
}
```

Appendix C: LDAP Result Codes

An operation result code as defined in RFC 4511 section 4.1.9 is used to indicate the final status of an operation. If a server detects multiple errors for an operation, only one result code is returned.

The server should return the result code that best indicates the nature of the error encountered. Servers may return substituted result codes to prevent unauthorized disclosures.

OpenDJ LDAP Result Codes

Result Code	Name	Description
-1	Undefined	The result code that should only be used if the actual result code has not yet been determined. Despite not being a standard result code, it is an implementation of the null object design pattern for this type.
0	Success	The result code that indicates that the operation completed successfully.
1	Operations Error	The result code that indicates that an internal error prevented the operation from being processed properly.
2	Protocol Error	The result code that indicates that the client sent a malformed or illegal request to the server.
3	Time Limit Exceeded	The result code that indicates that a time limit was exceeded while attempting to process the request.
4	Size Limit Exceeded	The result code that indicates that a size limit was exceeded while attempting to process the request.
5	Compare False	The result code that indicates that the attribute value assertion included in a compare request did not match the targeted entry.
6	Compare True	The result code that indicates that the attribute value assertion included in a compare request did match the targeted entry.
7	Authentication Method Not Supported	The result code that indicates that the requested authentication attempt failed because it referenced an invalid SASL mechanism.
8	Strong Authentication Required	The result code that indicates that the requested operation could not be processed because it requires that the client has completed a strong form of authentication.

Result Code	Name	Description
10	Referral	The result code that indicates that a referral was encountered. Strictly speaking this result code should not be exceptional since it is considered as a "success" response. However, referrals should occur rarely in practice and, when they do occur, should not be ignored since the application may believe that a request has succeeded when, in fact, nothing was done.
11	Administrative Limit Exceeded	The result code that indicates that processing on the requested operation could not continue because an administrative limit was exceeded.
12	Unavailable Critical Extension	The result code that indicates that the requested operation failed because it included a critical extension that is unsupported or inappropriate for that request.
13	Confidentiality Required	The result code that indicates that the requested operation could not be processed because it requires confidentiality for the communication between the client and the server.
14	SASL Bind in Progress	The result code that should be used for intermediate responses in multi-stage SASL bind operations.
16	No Such Attribute	The result code that indicates that the requested operation failed because it targeted an attribute or attribute value that did not exist in the specified entry.
17	Undefined Attribute Type	The result code that indicates that the requested operation failed because it referenced an attribute that is not defined in the server schema.
18	Inappropriate Matching	The result code that indicates that the requested operation failed because it attempted to perform an inappropriate type of matching against an attribute.
19	Constraint Violation	The result code that indicates that the requested operation failed because it would have violated some constraint defined in the server.
20	Attribute or Value Exists	The result code that indicates that the requested operation failed because it would have resulted in a conflict with an existing attribute or attribute value in the target entry.

Result Code	Name	Description
21	Invalid Attribute Syntax	The result code that indicates that the requested operation failed because it violated the syntax for a specified attribute.
32	No Such Entry	The result code that indicates that the requested operation failed because it referenced an entry that does not exist.
33	Alias Problem	The result code that indicates that the requested operation failed because it attempted to perform an illegal operation on an alias.
34	Invalid DN Syntax	The result code that indicates that the requested operation failed because it would have resulted in an entry with an invalid or malformed DN.
36	Alias Dereferencing Problem	The result code that indicates that a problem was encountered while attempting to dereference an alias for a search operation.
48	Inappropriate Authentication	The result code that indicates that an authentication attempt failed because the requested type of authentication was not appropriate for the targeted entry.
49	Invalid Credentials	The result code that indicates that an authentication attempt failed because the user did not provide a valid set of credentials.
50	Insufficient Access Rights	The result code that indicates that the client does not have sufficient permission to perform the requested operation.
51	Busy	The result code that indicates that the server is too busy to process the requested operation.
52	Unavailable	The result code that indicates that either the entire server or one or more required resources were not available for use in processing the request.
53	Unwilling to Perform	The result code that indicates that the server is unwilling to perform the requested operation.
54	Loop Detected	The result code that indicates that a referral or chaining loop was detected while processing the request.
60	Sort Control Missing	The result code that indicates that a search request included a VLV request control without a server-side sort control.

Result Code	Name	Description
61	Offset Range Error	The result code that indicates that a search request included a VLV request control with an invalid offset.
64	Naming Violation	The result code that indicates that the requested operation failed because it would have violated the server's naming configuration.
65	Object Class Violation	The result code that indicates that the requested operation failed because it would have resulted in an entry that violated the server schema.
66	Not Allowed on Non-Leaf	The result code that indicates that the requested operation is not allowed for non-leaf entries.
67	Not Allowed on RDN	The result code that indicates that the requested operation is not allowed on an RDN attribute.
68	Entry Already Exists	The result code that indicates that the requested operation failed because it would have resulted in an entry that conflicts with an entry that already exists.
69	Object Class Modifications Prohibited	The result code that indicates that the operation could not be processed because it would have modified the objectclasses associated with an entry in an illegal manner.
71	Affects Multiple DSAs	The result code that indicates that the operation could not be processed because it would impact multiple DSAs or other repositories.
76	Virtual List View Error	The result code that indicates that the operation could not be processed because there was an error while processing the virtual list view control.
80	Other	The result code that should be used if no other result code is appropriate.
81	Server Connection Closed	The client-side result code that indicates that a previously-established connection to the server was lost. This is for client-side use only and should never be transferred over protocol.
82	Local Error	The client-side result code that indicates that a local error occurred that had nothing to do with interaction with the server. This is for client-side use only and should never be transferred over protocol.

Result Code	Name	Description
83	Encoding Error	The client-side result code that indicates that an error occurred while encoding a request to send to the server. This is for client-side use only and should never be transferred over protocol.
84	Decoding Error	The client-side result code that indicates that an error occurred while decoding a response from the server. This is for client-side use only and should never be transferred over protocol.
85	Client-Side Timeout	The client-side result code that indicates that the client did not receive an expected response in a timely manner. This is for client-side use only and should never be transferred over protocol.
86	Unknown Authentication Mechanism	The client-side result code that indicates that the user requested an unknown or unsupported authentication mechanism. This is for client-side use only and should never be transferred over protocol.
87	Filter Error	The client-side result code that indicates that the filter provided by the user was malformed and could not be parsed. This is for client-side use only and should never be transferred over protocol.
88	Cancelled by User	The client-side result code that indicates that the user cancelled an operation. This is for client-side use only and should never be transferred over protocol.
89	Parameter Error	The client-side result code that indicates that there was a problem with one or more of the parameters provided by the user. This is for client-side use only and should never be transferred over protocol.
90	Out of Memory	The client-side result code that indicates that the client application was not able to allocate enough memory for the requested operation. This is for client-side use only and should never be transferred over protocol.
91	Connect Error	The client-side result code that indicates that the client was not able to establish a connection to the server. This is for client-side use only and should never be transferred over protocol.

Result Code	Name	Description
92	Operation Not Supported	The client-side result code that indicates that the user requested an operation that is not supported. This is for client-side use only and should never be transferred over protocol.
93	Control Not Found	The client-side result code that indicates that the client expected a control to be present in the response from the server but it was not included. This is for client-side use only and should never be transferred over protocol.
94	No Results Returned	The client-side result code that indicates that the requested single entry search operation or read operation failed because the Directory Server did not return any matching entries. This is for client-side use only and should never be transferred over protocol.
95	Unexpected Results Returned	The client-side result code that the requested single entry search operation or read operation failed because the Directory Server returned multiple matching entries (or search references) when only a single matching entry was expected. This is for client-side use only and should never be transferred over protocol.
96	Referral Loop Detected	The client-side result code that indicates that the client detected a referral loop caused by servers referencing each other in a circular manner. This is for client-side use only and should never be transferred over protocol.
97	Referral Hop Limit Exceeded	The client-side result code that indicates that the client reached the maximum number of hops allowed when attempting to follow a referral (i.e., following one referral resulted in another referral which resulted in another referral and so on). This is for client-side use only and should never be transferred over protocol.
118	Canceled	The result code that indicates that a cancel request was successful, or that the specified operation was canceled.
119	No Such Operation	The result code that indicates that a cancel request was unsuccessful because the targeted operation did not exist or had already completed.

Result Code	Name	Description
120	Too Late	The result code that indicates that a cancel request was unsuccessful because processing on the targeted operation had already reached a point at which it could not be canceled.
121	Cannot Cancel	The result code that indicates that a cancel request was unsuccessful because the targeted operation was one that could not be canceled.
122	Assertion Failed	The result code that indicates that the filter contained in an assertion control failed to match the target entry.
123	Authorization Denied	The result code that should be used if the server will not allow the client to use the requested authorization.
16,654	No Operation	The result code that should be used if the server did not actually complete processing on the associated operation because the request included the LDAP No-Op control.

Appendix D: File Layout

OpenDJ software installs and creates the following files and directories. The following list is not meant to be exhaustive:

`legal-notices`

License information

`QuickSetup.app`

Mac OS X GUI for installing OpenDJ

`README`

Brief instructions on installing OpenDJ directory server

`Uninstall.app`

Mac OS X GUI for removing OpenDJ

`bak`

Directory for saving backup files

`bat`

Windows command-line tools and control panel

`bin`

UNIX/Linux/Mac OS X command-line tools and control panel

`changelogDb`

Backend data for the external change log when using replication

`classes`

Directory added to the `CLASSPATH` for OpenDJ, permitting individual classes to be patched

`config`

OpenDJ server configuration and schema, PKI stores, LDIF generation templates, resources for upgrade

`config/MakeLDIF`

Templates for use with the `make-ldif` LDIF generation tool

`config/config.ldif`

LDIF representation of current OpenDJ server config

Use the `dsconfig` command to edit OpenDJ server configuration.

`config/java.properties`

JVM settings for OpenDJ server and tools

`config/schema`

OpenDJ directory server LDAP schema definition files

`config/tasks.ldif`

Data used by task scheduler backend so that scheduled tasks and recurring tasks persist after server restart

`config/tools.properties`

Default settings for command-line tools

Use as a template when creating an `~/.opendj/tools.properties` file.

`config/upgrade`

Resources used by the upgrade command to move to the next version of OpenDJ

`config/wordlist.txt`

List of words used to check password strength

`db`

Backend database files for persistent, indexed backends that hold user data

`example-plugin.zip`

Sample OpenDJ plugin code. Custom plugins are meant to be installed in `lib/extensions`.

`import-tmp`

Used when importing data into OpenDJ

`instance.loc`

Pointer to OpenDJ on the file system, provided for package installations where the program files are separate from the server instance files

`ldif`

Directory for saving LDIF export files

`lib`

Scripts and libraries needed by OpenDJ and added to the `CLASSPATH` for OpenDJ

`lib/extensions`

File system directory to hold your custom plugins

`locks`

Directory to hold lock files used when OpenDJ is running to prevent backends from accidentally being used by more than one server process

`logs`

Access, errors, audit, and replication logs

`logs/server.pid`

Contains the process ID for the server when OpenDJ is running

`setup`

UNIX setup utility

`setup.bat`

Windows setup utility

`template`

Template files for a directory server instance

`uninstall`

UNIX utility for removing OpenDJ

`uninstall.bat`

Windows utility for removing OpenDJ

`upgrade`

UNIX utility for upgrading OpenDJ by pointing to the new .zip

`upgrade.bat`

Windows utility for upgrading OpenDJ by pointing to the new .zip

Appendix E: Ports Used

OpenDJ server software uses the following TCP/IP ports by default:

LDAP: 389 (1389)

OpenDJ directory server listens for LDAP requests from client applications on port 389 by default. OpenDJ directory server uses port 1389 by default for users who cannot use privileged ports. LDAP is enabled by default.

LDAPS: 636 (1636)

OpenDJ directory server listens for LDAPS requests from client applications on port 636 by default. OpenDJ directory server uses port 1636 by default for users who cannot use privileged ports. LDAPS is not enabled by default.

Administrative connections: 4444

OpenDJ directory server listens for administrative traffic on port 4444 by default. The administration connector is enabled by default.

SNMP: 161, 162

OpenDJ directory server listens for SNMP traffic on port 161 by default, and uses port 162 for traps. SNMP is not enabled by default.

JMX: 1689

OpenDJ directory server listens for Java Management eXtension traffic on port 1689 by default. JMX is not enabled by default.

HTTP: 8080

OpenDJ directory server can listen for HTTP client requests to the RESTful API. The default port is 8080, but HTTP access is not enabled by default.

Replication: 8989

OpenDJ directory server listens for replication traffic on port 8989 by default. Replication is not enabled by default.

Appendix F: Standards, RFCs, & Internet-Drafts

OpenDJ 3.5 software implements the following RFCs, Internet-Drafts, and standards:

RFC 1274: The COSINE and Internet X.500 Schema

X.500 Directory Schema, or Naming Architecture, for use in the COSINE and Internet X.500 pilots.

RFC 1321: The MD5 Message-Digest Algorithm

MD5 message-digest algorithm that takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input.

RFC 1777: Lightweight Directory Access Protocol (LDAPv2)

Provide access to the X.500 Directory while not incurring the resource requirements of the Directory Access Protocol.

Classified as an Historic document.

RFC 1778: The String Representation of Standard Attribute Syntaxes

Defines the requirements that must be satisfied by encoding rules used to render X.500 Directory attribute syntaxes into a form suitable for use in the LDAP, then defines the encoding rules for the standard set of attribute syntaxes.

Classified as an Historic document.

RFC 1779: A String Representation of Distinguished Names

Defines a string format for representing names, which is designed to give a clean representation of commonly used names, whilst being able to represent any distinguished name.

Classified as an Historic document.

RFC 2079: Definition of an X.500 Attribute Type and an Object Class to Hold Uniform Resource Identifiers (URIs)

Defines a new attribute type and an auxiliary object class to allow URIs, including URLs, to be stored in directory entries in a standard way.

RFC 2222: Simple Authentication and Security Layer (SASL)

Describes a method for adding authentication support to connection-based protocols.

RFC 2246: The TLS Protocol Version 1.0

Specifies Version 1.0 of the Transport Layer Security protocol.

RFC 2247: Using Domains in LDAP/X.500 Distinguished Names

Defines an algorithm by which a name registered with the Internet Domain Name Service can be represented as an LDAP distinguished name.

RFC 2251: Lightweight Directory Access Protocol (v3)

Describes a directory access protocol designed to provide access to directories supporting the X.500 models, while not incurring the resource requirements of the X.500 Directory Access Protocol.

RFC 2252: Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions

Defines a set of syntaxes for LDAPv3, and the rules by which attribute values of these syntaxes are represented as octet strings for transmission in the LDAP protocol.

RFC 2253: Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names

Defines a common UTF-8 format to represent distinguished names unambiguously.

RFC 2254: The String Representation of LDAP Search Filters

Defines the string format for representing names, which is designed to give a clean representation of commonly used distinguished names, while being able to represent any distinguished name.

RFC 2255: The LDAP URL Format

Describes a format for an LDAP Uniform Resource Locator.

RFC 2256: A Summary of the X.500(96) User Schema for use with LDAPv3

Provides an overview of the attribute types and object classes defined by the ISO and ITU-T committees in the X.500 documents, in particular those intended for use by directory clients.

RFC 2307: An Approach for Using LDAP as a Network Information Service

Describes an experimental mechanism for mapping entities related to TCP/IP and the UNIX system into X.500 entries so that they may be resolved with the Lightweight Directory Access Protocol.

RFC 2377: Naming Plan for Internet Directory-Enabled Applications

Proposes a new directory naming plan that leverages the strengths of the most popular and successful Internet naming schemes for naming objects in a hierarchical directory.

RFC 2696: LDAP Control Extension for Simple Paged Results Manipulation

Allows a client to control the rate at which an LDAP server returns the results of an LDAP search operation.

RFC 2713: Schema for Representing Java(tm) Objects in an LDAP Directory

Defines a common way for applications to store and retrieve Java objects from the directory.

RFC 2714: Schema for Representing CORBA Object References in an LDAP Directory

Define a common way for applications to store and retrieve CORBA object references from the directory.

RFC 2739: Calendar Attributes for vCard and LDAP

Defines a mechanism to locate a user calendar and free/busy time using the LDAP protocol.

RFC 2798: Definition of the inetOrgPerson LDAP Object Class

Define an object class called inetOrgPerson for use in LDAP and X.500 directory services that extends the X.521 standard organizationalPerson class.

RFC 2829: Authentication Methods for LDAP

Specifies particular combinations of security mechanisms which are required and recommended in LDAP implementations.

RFC 2830: Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security

Defines the "Start Transport Layer Security (TLS) Operation" for LDAP.

RFC 2849: The LDAP Data Interchange Format (LDIF) - Technical Specification

Describes a file format suitable for describing directory information or modifications made to directory information.

RFC 2891: LDAP Control Extension for Server Side Sorting of Search Results

Describes two LDAPv3 control extensions for server-side sorting of search results.

RFC 2926: Conversion of LDAP Schemas to and from SLP Templates

Describes a procedure for mapping between Service Location Protocol service advertisements and lightweight directory access protocol descriptions of services.

RFC 3045: Storing Vendor Information in the LDAP root DSE

Specifies two Lightweight Directory Access Protocol attributes, vendorName and vendorVersion that MAY be included in the root DSA-specific Entry (DSE) to advertise vendor-specific information.

RFC 3062: LDAP Password Modify Extended Operation

Describes an LDAP extended operation to allow modification of user passwords which is not dependent upon the form of the authentication identity nor the password storage mechanism used.

RFC 3112: LDAP Authentication Password Schema

Describes schema in support of user/password authentication in a LDAP directory including the authPassword attribute type. This attribute type holds values derived from the user's password(s) (commonly using cryptographic strength one-way hash).

RFC 3296: Named Subordinate References in Lightweight Directory Access Protocol (LDAP) Directories

Details schema and protocol elements for representing and managing named subordinate references in Lightweight Directory Access Protocol (LDAP) Directories.

RFC 3377: Lightweight Directory Access Protocol (v3): Technical Specification

Specifies the set of RFCs comprising the Lightweight Directory Access Protocol Version 3 (LDAPv3), and addresses the "IESG Note" attached to RFCs 2251 through 2256.

RFC 3383: Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)

Provides procedures for registering extensible elements of the Lightweight Directory Access Protocol (LDAP).

RFC 3546: Transport Layer Security (TLS) Extensions

Describes extensions that may be used to add functionality to Transport Layer Security.

RFC 3671: Collective Attributes in the Lightweight Directory Access Protocol (LDAP)

Summarizes the X.500 information model for collective attributes and describes use of collective attributes in LDAP.

RFC 3672: Subentries in the Lightweight Directory Access Protocol (LDAP)

Adapts X.500 subentries mechanisms for use with the Lightweight Directory Access Protocol (LDAP).

RFC 3673: Lightweight Directory Access Protocol version 3 (LDAPv3): All Operational Attributes

Describes an LDAP extension which clients may use to request the return of all operational attributes.

RFC 3674: Feature Discovery in Lightweight Directory Access Protocol (LDAP)

Introduces a general mechanism for discovery of elective features and extensions which cannot be discovered using existing mechanisms.

RFC 3712: Lightweight Directory Access Protocol (LDAP): Schema for Printer Services

Defines a schema, object classes and attributes, for printers and printer services, for use with directories that support Lightweight Directory Access Protocol v3 (LDAP).

RFC 3771: Lightweight Directory Access Protocol (LDAP) Intermediate Response Message

Defines and describes the IntermediateResponse message, a general mechanism for defining single-request/multiple-response operations in Lightweight Directory Access Protocol.

RFC 3829: Lightweight Directory Access Protocol (LDAP) Authorization Identity Request and Response Controls

Extends the Lightweight Directory Access Protocol bind operation with a mechanism for requesting and returning the authorization identity it establishes.

RFC 3876: Returning Matched Values with the Lightweight Directory Access Protocol version 3 (LDAPv3)

Describes a control for the Lightweight Directory Access Protocol version 3 that is used to return a subset of attribute values from an entry.

RFC 3909: Lightweight Directory Access Protocol (LDAP) Cancel Operation

Describes a Lightweight Directory Access Protocol extended operation to cancel (or abandon) an outstanding operation, with a response to indicate the outcome of the operation.

RFC 4346: The Transport Layer Security (TLS) Protocol Version 1.1

Specifies Version 1.1 of the Transport Layer Security protocol.

RFC 4370: Lightweight Directory Access Protocol (LDAP) Proxied Authorization Control

Defines the Proxy Authorization Control, that allows a client to request that an operation be processed under a provided authorization identity instead of under the current authorization identity associated with the connection.

RFC 4403: Lightweight Directory Access Protocol (LDAP) Schema for Universal Description

Defines the Lightweight Directory Access Protocol schema for representing Universal Description, Discovery, and Integration data types in an LDAP directory.

RFC 4422: Simple Authentication and Security Layer (SASL)

Describes a framework for providing authentication and data security services in connection-oriented protocols via replaceable mechanisms.

RFC 4505: Anonymous Simple Authentication and Security Layer (SASL) Mechanism

Describes a new way to provide anonymous login is needed within the context of the Simple Authentication and Security Layer framework.

RFC 4510: Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map

Provides a road map of the LDAP Technical Specification.

RFC 4511: Lightweight Directory Access Protocol (LDAP): The Protocol

Describes the protocol elements, along with their semantics and encodings, of the Lightweight Directory Access Protocol.

RFC 4512: Lightweight Directory Access Protocol (LDAP): Directory Information Models

Describes the X.500 Directory Information Models as used in LDAP.

RFC 4513: Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms

Describes authentication methods and security mechanisms of the Lightweight Directory Access Protocol.

RFC 4514: Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names

Defines the string representation used in the Lightweight Directory Access Protocol to transfer distinguished names.

RFC 4515: Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters

Defines a human-readable string representation of LDAP search filters that is appropriate for use in LDAP URLs and in other applications.

RFC 4516: Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator

Describes a format for a Lightweight Directory Access Protocol Uniform Resource Locator.

RFC 4517: Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules

Defines a base set of syntaxes and matching rules for use in defining attributes for LDAP directories.

RFC 4518: Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation

Defines string preparation algorithms for character-based matching rules defined for use in LDAP.

RFC 4519: Lightweight Directory Access Protocol (LDAP): Schema for User Applications

Provides a technical specification of attribute types and object classes intended for use by LDAP directory clients for many directory services, such as White Pages.

RFC 4523: Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates

Describes schema for representing X.509 certificates, X.521 security information, and related elements in directories accessible using the Lightweight Directory Access Protocol (LDAP).

RFC 4524: COSINE LDAP/X.500 Schema

Provides a collection of schema elements for use with the Lightweight Directory Access Protocol from the COSINE and Internet X.500 pilot projects.

RFC 4525: Lightweight Directory Access Protocol (LDAP) Modify-Increment Extension

Describes an extension to the Lightweight Directory Access Protocol Modify operation to support an increment capability.

RFC 4526: Lightweight Directory Access Protocol (LDAP) Absolute True and False Filters

Extends the Lightweight Directory Access Protocol to support absolute True and False filters

based upon similar capabilities found in X.500 directory systems.

RFC 4527: Lightweight Directory Access Protocol (LDAP) Read Entry Controls

Specifies an extension to the Lightweight Directory Access Protocol to allow the client to read the target entry of an update operation.

RFC 4528: Lightweight Directory Access Protocol (LDAP) Assertion Control

Defines the Lightweight Directory Access Protocol Assertion Control, which allows a client to specify that a directory operation should only be processed if an assertion applied to the target entry of the operation is true.

RFC 4529: Requesting Attributes by Object Class in the Lightweight Directory Access Protocol (LDAP)

Extends LDAP to support a mechanism that LDAP clients may use to request the return of all attributes of an object class.

RFC 4530: Lightweight Directory Access Protocol (LDAP) entryUUID Operational Attribute

Describes the LDAP/X.500 'entryUUID' operational attribute and associated matching rules and syntax.

RFC 4532: Lightweight Directory Access Protocol (LDAP) "Who am I?" Operation

Provides a mechanism for Lightweight Directory Access Protocol clients to obtain the authorization identity the server has associated with the user or application entity.

RFC 4616: The PLAIN Simple Authentication and Security Layer (SASL) Mechanism

Defines a simple cleartext user/password Simple Authentication and Security Layer mechanism called the PLAIN mechanism.

RFC 4634: US Secure Hash Algorithms (SHA and HMAC-SHA)

Specifies Secure Hash Algorithms, SHA-256, SHA-384, and SHA-512, for computing a condensed representation of a message or a data file.

RFC 4752: The Kerberos V5 ("GSSAPI") Simple Authentication and Security Layer (SASL) Mechanism

Describes the method for using the Generic Security Service Application Program Interface (GSS-API) Kerberos V5 in the Simple Authentication and Security Layer, called the GSSAPI mechanism.

RFC 4876: A Configuration Profile Schema for Lightweight Directory Access Protocol (LDAP)-Based Agents

Defines a schema for storing a profile for agents that make use of the Lightweight Directory Access protocol (LDAP).

RFC 5020: The Lightweight Directory Access Protocol (LDAP) entryDN Operational Attribute

Describes the Lightweight Directory Access Protocol (LDAP) / X.500 'entryDN' operational attribute, that provides a copy of the entry's distinguished name for use in attribute value assertions.

FIPS 180-1: Secure Hash Standard (SHA-1)

Specifies a Secure Hash Algorithm, SHA-1, for computing a condensed representation of a message or a data file.

FIPS 180-2: Secure Hash Standard (SHA-1

Specifies four Secure Hash Algorithms for computing a condensed representation of electronic data.

DSMLv2: Directory Service Markup Language

Provides a method for expressing directory queries and updates as XML documents.

JavaScript Object Notation

A data-interchange format that aims to be both "easy for humans to read and write," and also "easy for machines to parse and generate."

Simple Cloud Identity Management: Core Schema 1.0

Platform neutral schema and extension model for representing users and groups in JSON and XML formats. OpenDJ supports the JSON formats.

Appendix G: LDAP Controls

Controls provide a mechanism whereby the semantics and arguments of existing LDAP operations may be extended. One or more controls may be attached to a single LDAP message. A control only affects the semantics of the message it is attached to. Controls sent by clients are termed *request controls*, and those sent by servers are termed *response controls*.

OpenDJ software supports the following LDAP controls:

Account Usability Control

Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.8

Control originally provided by Sun Microsystems, used to determine whether a user account can be used to authenticate to the directory.

Assertion request control

Object Identifier: 1.3.6.1.1.12

RFC: RFC 4528 - Lightweight Directory Access Protocol (LDAP) Assertion Control

Authorization Identity request control

Object Identifier: 2.16.840.1.113730.3.4.16

RFC: RFC 3829 - Lightweight Directory Access Protocol (LDAP) Authorization Identity Request and Response Controls

Authorization Identity response control

Object Identifier: 2.16.840.1.113730.3.4.15

RFC: RFC 3829 - Lightweight Directory Access Protocol (LDAP) Authorization Identity Request

and Response Controls

Entry Change Notification response control

Object Identifier: 2.16.840.1.113730.3.4.7

Internet-Draft: draft-ietf-ldapext-psearch - Persistent Search: A Simple LDAP Change Notification Mechanism

Get Effective Rights request control

Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.2

Internet-Draft: draft-ietf-ldapext-acl-model - Access Control Model for LDAPv3

Manage DSAIT request control

Object Identifier: 2.16.840.1.113730.3.4.2

RFC: RFC 3296 - Named Subordinate References in Lightweight Directory Access Protocol (LDAP) Directories

Matched Values request control

Object Identifier: 1.2.826.0.1.3344810.2.3

RFC: RFC 3876 - Returning Matched Values with the Lightweight Directory Access Protocol version 3 (LDAPv3)

No-Op Control

Object Identifier: 1.3.6.1.4.1.4203.1.10.2

Internet-Draft: draft-zeilenga-ldap-noop - LDAP No-Op Control

Password Expired response control

Object Identifier: 2.16.840.1.113730.3.4.4

Internet-Draft: draft-vchu-ldap-pwd-policy - Password Policy for LDAP Directories

Password Expiring response control

Object Identifier: 2.16.840.1.113730.3.4.5

Internet-Draft: draft-vchu-ldap-pwd-policy - Password Policy for LDAP Directories

Password Policy response control

Object Identifier: 1.3.6.1.4.1.42.2.27.8.5.1

Internet-Draft: draft-behera-ldap-password-policy - Password Policy for LDAP Directories

Permissive Modify request control

Object Identifier: 1.2.840.113556.1.4.1413

Microsoft defined this control that, "Allows an LDAP modify to work under less restrictive conditions. Without it, a delete will fail if an attribute done not exist, and an add will fail if an

attribute already exists. No data is needed in this control." (source of quote)

Persistent Search request control

Object Identifier: 2.16.840.1.113730.3.4.3

Internet-Draft: draft-ietf-ldapext-psearch - Persistent Search: A Simple LDAP Change Notification Mechanism

Post-Read request control

Object Identifier: 1.3.6.1.1.13.2

RFC: RFC 4527 - Lightweight Directory Access Protocol (LDAP) Read Entry Controls

Post-Read response control

Object Identifier: 1.3.6.1.1.13.2

RFC: RFC 4527 - Lightweight Directory Access Protocol (LDAP) Read Entry Controls

Pre-Read request control

Object Identifier: 1.3.6.1.1.13.1

RFC: RFC 4527 - Lightweight Directory Access Protocol (LDAP) Read Entry Controls

Pre-Read response control

Object Identifier: 1.3.6.1.1.13.1

RFC: RFC 4527 - Lightweight Directory Access Protocol (LDAP) Read Entry Controls

Proxied Authorization v1 request control

Object Identifier: 2.16.840.1.113730.3.4.12

Internet-Draft: draft-weltman-ldapv3-proxy-04 - LDAP Proxied Authorization Control

Proxied Authorization v2 request control

Object Identifier: 2.16.840.1.113730.3.4.18

RFC: RFC 4370 - Lightweight Directory Access Protocol (LDAP) Proxied Authorization Control

Public Changelog Exchange Control

Object Identifier: 1.3.6.1.4.1.26027.1.5.4

OpenDJ specific, for using the bookmark cookie when reading the external change log.

Server-Side Sort request control

Object Identifier: 1.2.840.113556.1.4.473

RFC: RFC 2891 - LDAP Control Extension for Server Side Sorting of Search Results

Server-Side Sort response control

Object Identifier: 1.2.840.113556.1.4.474

RFC: RFC 2891 - LDAP Control Extension for Server Side Sorting of Search Results

Simple Paged Results Control

Object Identifier: 1.2.840.113556.1.4.319

RFC: RFC 2696 - LDAP Control Extension for Simple Paged Results Manipulation

Subentries request controls

Object Identifier: 1.3.6.1.4.1.4203.1.10.1

RFC: Subentries in the Lightweight Directory Access Protocol (LDAP)

Object Identifier: 1.3.6.1.4.1.7628.5.101.1

Internet-Draft: draft-ietf-ldup-subentry - LDAP Subentry Schema

Subtree Delete request control

Object Identifier: 1.2.840.113556.1.4.805

Internet-Draft: draft-armijo-ldap-treedelete - Tree Delete Control

Virtual List View request control

Object Identifier: 2.16.840.1.113730.3.4.9

Internet-Draft: draft-ietf-ldapext-ldapv3-vlv - LDAP Extensions for Scrolling View Browsing of Search Results

Virtual List View response control

Object Identifier: 2.16.840.1.113730.3.4.10

Internet-Draft: draft-ietf-ldapext-ldapv3-vlv - LDAP Extensions for Scrolling View Browsing of Search Results

The LDAP Relax Rules Control

Object Identifier: 1.3.6.1.4.1.4203.666.5.12

Internet-Draft: ddraft-zeilenga-ldap-relax-03 - The LDAP Relax Rules Control

Appendix H: LDAP Extended Operations

Extended operations allow additional operations to be defined for services not already available in the protocol

OpenDJ software supports the following LDAP extended operations:

Cancel Extended Request

Object Identifier: 1.3.6.1.1.8

RFC: RFC 3909 - Lightweight Directory Access Protocol (LDAP) Cancel Operation

Get Connection ID Extended Request

Object Identifier: 1.3.6.1.4.1.26027.1.6.2

OpenDJ extended operation to return the connection ID of the associated client connection. This extended operation is intended for OpenDJ internal use.

Password Modify Extended Request

Object Identifier: 1.3.6.1.4.1.4203.1.11.1

RFC: RFC 3062 - LDAP Password Modify Extended Operation

Password Policy State Extended Operation

Object Identifier: 1.3.6.1.4.1.26027.1.6.1

OpenDJ extended operation to query and update password policy state for a given user entry. This extended operation is intended for OpenDJ internal use.

Start Transport Layer Security Extended Request

Object Identifier: 1.3.6.1.4.1.1466.20037

RFC: RFC 4511 - Lightweight Directory Access Protocol (LDAP): The Protocol

Who am I? Extended Request

Object Identifier: 1.3.6.1.4.1.4203.1.11.3

RFC: RFC 4532 - Lightweight Directory Access Protocol (LDAP) "Who am I?" Operation

Appendix I: Localization

OpenDJ software stores data in UTF-8 format. It enables you to store and to search for attribute values according to a variety of language specific locales. OpenDJ software is also itself localized for a smaller variety of languages.

OpenDJ Languages

OpenDJ 3.5 software is localized in the following languages:

- French
- German
- Japanese
- Simplified Chinese
- Spanish

NOTE	Certain messages have also been translated into Catalan, Korean, Polish, and Traditional Chinese. Some error messages including messages labeled ERROR are provided only in English.

Directory Support For Locales and Language Subtypes

OpenDJ software supports the following locales with their associated language and country codes and their collation order object identifiers. Locale support depends on the Java Virtual Machine used at run time. The following list reflects all supported locales.

Supported Locales

Afrikaans

Code tag: af

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.1.1

Albanian

Code tag: sq

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.127.1

Amharic

Code tag: am

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.2.1

Arabic

Code tag: ar

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.3.1

Arabic (Algeria)

Code tag: ar-DZ

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.6.1

Arabic (Bahrain)

Code tag: ar-BH

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.5.1

Arabic (Egypt)

Code tag: ar-EG

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.7.1

Arabic (India)

Code tag: ar-IN

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.8.1

Arabic (Iraq)

Code tag: ar-IQ

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.9.1

Arabic (Jordan)

Code tag: ar-JO

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.10.1

Arabic (Kuwait)

Code tag: ar-KW

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.11.1

Arabic (Lebanon)

Code tag: ar-LB

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.12.1

Arabic (Libya)

Code tag: ar-LY

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.13.1

Arabic (Morocco)

Code tag: ar-MA

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.14.1

Arabic (Oman)

Code tag: ar-OM

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.15.1

Arabic (Qatar)

Code tag: ar-QA

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.16.1

Arabic (Saudi Arabia)

Code tag: ar-SA

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.17.1

Arabic (Sudan)

Code tag: ar-SD

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.18.1

Arabic (Syria)

Code tag: ar-SY

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.19.1

Arabic (Tunisia)

Code tag: ar-TN

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.20.1

Arabic (United Arab Emirates)

Code tag: ar-AE

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.4.1

Arabic (Yemen)

Code tag: ar-YE

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.21.1

Armenian

Code tag: hy

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.89.1

Basque

Code tag: eu

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.70.1

Belarusian

Code tag: be

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.22.1

Bengali

Code tag: bn

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.24.1

Bulgarian

Code tag: bg

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.23.1

Catalan

Code tag: ca

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.25.1

Chinese

Code tag: zh

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.143.1

Chinese (China)

Code tag: zh-CN

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.144.1

Chinese (Hong Kong)

Code tag: zh-HK

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.145.1

Chinese (Macao)

Code tag: zh-MO

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.146.1

Chinese (Singapore)

Code tag: zh-SG

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.147.1

Chinese (Taiwan)

Code tag: zh-TW

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.148.1

Cornish

Code tag: kw

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.99.1

Croatian

Code tag: hr

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.87.1

Czech

Code tag: cs

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.26.1

Danish

Code tag: da

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.27.1

Dutch

Code tag: nl

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.105.1

Dutch (Belgium)

Code tag: nl-BE

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.106.1

Dutch (Netherlands)

Code tag: nl-NL

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.105.1

English

Code tag: en

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.34.1

English (Australia)

Code tag: en-AU

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.35.1

English (Canada)

Code tag: en-CA

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.36.1

English (Hong Kong)

Code tag: en-HK

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.38.1

English (India)

Code tag: en-IN

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.40.1

English (Ireland)

Code tag: en-IE

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.39.1

English (Malta)

Code tag: en-MT

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.41.1

English (New Zealand)

Code tag: en-NZ

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.42.1

English (Philippines)

Code tag: en-PH

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.43.1

English (Singapore)

Code tag: en-SG

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.44.1

English (South Africa)

Code tag: en-ZA

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.46.1

English (U.S. Virgin Islands)

Code tag: en-VI

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.45.1

English (United Kingdom)

Code tag: en-GB

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.37.1

English (United States)

Code tag: en-US

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.34.1

English (Zimbabwe)

Code tag: en-ZW

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.47.1

Esperanto

Code tag: eo

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.48.1

Estonian

Code tag: et

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.69.1

Faroese

Code tag: fo

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.75.1

Finnish

Code tag: fi

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.74.1

French

Code tag: fr

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.76.1

French (Belgium)

Code tag: fr-BE

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.77.1

French (Canada)

Code tag: fr-CA

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.78.1

French (France)

Code tag: fr-FR

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.76.1

French (Luxembourg)

Code tag: fr-LU

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.80.1

French (Switzerland)

Code tag: fr-CH

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.79.1

Gallegan

Code tag: gl

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.82.1

German

Code tag: de

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.28.1

German (Austria)

Code tag: de-AT

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.29.1

German (Belgium)

Code tag: de-BE

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.30.1

German (Germany)

Code tag: de-DE

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.28.1

German (Luxembourg)

Code tag: de-LU

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.32.1

German (Switzerland)

Code tag: de-CH

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.31.1

Greek

Code tag: el

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.33.1

Greenlandic

Code tag: kl

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.95.1

Gujarati

Code tag: gu

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.83.1

Hebrew

Code tag: iw

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.85.1

Hindi

Code tag: hi

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.86.1

Hungarian

Code tag: hu

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.88.1

Icelandic

Code tag: is

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.91.1

Indonesian

Code tag: in

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.90.1

Irish

Code tag: ga

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.81.1

Italian

Code tag: it

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.92.1

Italian (Switzerland)

Code tag: it-CH

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.93.1

Japanese

Code tag: ja

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.94.1

Kannada

Code tag: kn

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.96.1

Konkani

Code tag: kok

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.98.1

Korean

Code tag: ko

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.97.1

Latvian

Code tag: lv

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.101.1

Lithuanian

Code tag: lt

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.100.1

Macedonian

Code tag: mk

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.102.1

Maltese

Code tag: mt

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.104.1

Manx

Code tag: gv

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.84.1

Marathi

Code tag: mr

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.103.1

Norwegian

Code tag: no

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.107.1

Norwegian (Norway)

Code tag: no-NO-B

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.110.1

Norwegian Bokmål

Code tag: nb

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.110.1

Norwegian Nynorsk

Code tag: nn

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.109.1

Oromo

Code tag: om

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.111.1

Oromo (Ethiopia)

Code tag: om-ET

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.112.1

Oromo (Kenya)

Code tag: om-KE

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.113.1

Persian

Code tag: fa

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.71.1

Persian (India)

Code tag: fa-IN

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.72.1

Persian (Iran)

Code tag: fa-IR

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.73.1

Polish

Code tag: pl

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.114.1

Portuguese

Code tag: pt

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.115.1

Portuguese (Brazil)

Code tag: pt-BR

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.116.1

Portuguese (Portugal)

Code tag: pt-PT

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.115.1

Romanian

Code tag: ro

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.117.1

Russian

Code tag: ru

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.118.1

Russian (Russia)

Code tag: ru-RU

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.118.1

Russian (Ukraine)

Code tag: ru-UA

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.119.1

Serbian

Code tag: sr

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.128.1

Serbo-Croatian

Code tag: sh

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.120.1

Slovak

Code tag: sk

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.121.1

Slovenian

Code tag: sl

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.122.1

Somali

Code tag: so

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.123.1

Somali (Djibouti)

Code tag: so-DJ

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.124.1

Somali (Ethiopia)

Code tag: so-ET

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.125.1

Somali (Kenya)

Code tag: so-KE

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.126.1

Somali (Somalia)

Code tag: so-SO

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.123.1

Spanish

Code tag: es

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.49.1

Spanish (Argentina)

Code tag: es-AR

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.50.1

Spanish (Bolivia)

Code tag: es-BO

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.51.1

Spanish (Chile)

Code tag: es-CL

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.52.1

Spanish (Colombia)

Code tag: es-CO

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.53.1

Spanish (Costa Rica)

Code tag: es-CR

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.54.1

Spanish (Dominican Republic)

Code tag: es-DO

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.55.1

Spanish (Ecuador)

Code tag: es-EC

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.56.1

Spanish (El Salvador)

Code tag: es-SV

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.65.1

Spanish (Guatemala)

Code tag: es-GT

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.57.1

Spanish (Honduras)

Code tag: es-HN

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.58.1

Spanish (Mexico)

Code tag: es-MX

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.59.1

Spanish (Nicaragua)

Code tag: es-NI

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.60.1

Spanish (Panama)

Code tag: es-PA

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.61.1

Spanish (Paraguay)

Code tag: es-PY

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.64.1

Spanish (Peru)

Code tag: es-PE

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.62.1

Spanish (Puerto Rico)

Code tag: es-PR

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.63.1

Spanish (Spain)

Code tag: es-ES

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.49.1

Spanish (United States)

Code tag: es-US

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.66.1

Spanish (Uruguay)

Code tag: es-UY

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.67.1

Spanish (Venezuela)

Code tag: es-VE

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.68.1

Swahili

Code tag: sw

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.131.1

Swahili (Kenya)

Code tag: sw-KE

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.132.1

Swahili (Tanzania)

Code tag: sw-TZ

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.133.1

Swedish

Code tag: sv

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.129.1

Swedish (Finland)

Code tag: sv-FI

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.130.1

Swedish (Sweden)

Code tag: sv-SE

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.129.1

Tamil

Code tag: ta

Collation order object identifier: 1 3 1.3.6.1.4.1.42.2.27.9.4.134.1

Telugu

Code tag: te

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.135.1

Thai

Code tag: th

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.136.1

Tigrinya

Code tag: ti

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.137.1

Tigrinya (Eritrea)

Code tag: ti-ER

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.138.1

Tigrinya (Ethiopia)

Code tag: ti-ET

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.139.1

Turkish

Code tag: tr

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.140.1

Ukrainian

Code tag: uk

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.141.1

Vietnamese

Code tag: vi

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.142.1

Supported Language Subtypes

- Afrikaans, af
- Albanian, sq
- Amharic, am
- Arabic, ar
- Armenian, hy

- Basque, eu
- Belarusian, be
- Bengali, bn
- Bulgarian, bg
- Catalan, ca
- Chinese, zh
- Cornish, kw
- Croatian, hr
- Czech, cs
- Danish, da
- Dutch, nl
- English, en
- Esperanto, eo
- Estonian, et
- Faroese, fo
- Finnish, fi
- French, fr
- Gallegan, gl
- German, de
- Greek, el
- Greenlandic, kl
- Gujarati, gu
- Hebrew, iw
- Hindi, hi
- Hungarian, hu
- Icelandic, is
- Indonesian, in
- Irish, ga
- Italian, it
- Japanese, ja
- Kannada, kn
- Konkani, kok
- Korean, ko
- Latvian, lv
- Lithuanian, lt

- Macedonian, mk
- Maltese, mt
- Manx, gv
- Marathi, mr
- Norwegian, no
- Norwegian Bokmål, nb
- Norwegian Nynorsk, nn
- Oromo, om
- Persian, fa
- Polish, pl
- Portuguese, pt
- Romanian, ro
- Russian, ru
- Serbian, sr
- Serbo-Croatian, sh
- Slovak, sk
- Slovenian, sl
- Somali, so
- Spanish, es
- Swahili, sw
- Swedish, sv
- Tamil, ta
- Telugu, te
- Thai, th
- Tigrinya, ti
- Turkish, tr
- Ukrainian, uk
- Vietnamese, vi

Appendix J: Release Levels and Interface Stability

This appendix includes Open Identity Platform definitions for product release levels and interface stability: In addition to the indications concerning interface stability in the documentation, review the following information about OpenDJ user and application programming interfaces.

- Client tools—`ldap*`, `ldif*`, and `*rate` commands—are Evolving.
- The following classes, interfaces, and methods in the OpenDJ APIs are Evolving:

    - `org.forgerock.opendj.ldap.Connections#newInternalConnection`
    - `org.forgerock.opendj.ldap.Connections#newInternalConnectionFactory`
    - `org.forgerock.opendj.ldap.Connections#newServerConnectionFactory`
    - `org.forgerock.opendj.ldap.FutureResult`
    - `org.forgerock.opendj.ldap.LDAPClientContext`
    - `org.forgerock.opendj.ldap.LDAPListener`
    - `org.forgerock.opendj.ldap.LDAPListenerOptions`
    - `org.forgerock.opendj.ldap.MemoryBackend`
    - `org.forgerock.opendj.ldap.RequestContext`
    - `org.forgerock.opendj.ldap.RequestHandler`
    - `org.forgerock.opendj.ldap.RequestHandlerFactory`
    - `org.forgerock.opendj.ldap.ServerConnection`
    - `org.forgerock.opendj.ldap.ServerConnectionFactory`
- The following classes and interfaces in the OpenDJ LDAP SDK APIs are Evolving:
    - `org.forgerock.opendj.ldap.ConnectionSecurityLayer`
    - `org.forgerock.opendj.ldap.LDAPUrl`
    - `org.forgerock.opendj.ldap.requests.BindRequest`, including sub-types and especially SASL sub-types
    - `org.forgerock.opendj.ldap.schema.MatchingRuleImpl`
    - `org.forgerock.opendj.ldap.schema.SchemaValidationPolicy`
    - `org.forgerock.opendj.ldap.schema.SyntaxImpl`
- The following methods are Deprecated:
    - `org.forgerock.opendj.ldap.Connections#newHeartBeatConnectionFactory`
    - `org.forgerock.opendj.ldap.LDAPListenerOptions#getTCPNIOTransport`
    - `org.forgerock.opendj.ldap.LDAPListenerOptions#setTCPNIOTransport`
    - `org.forgerock.opendj.ldap.LDAPOptions#getTCPNIOTransport`
    - `org.forgerock.opendj.ldap.LDAPOptions#setTCPNIOTransport`
- The class `org.forgerock.opendj.ldap.CoreMessages` is Internal.
- For all Java APIs, `com.*` packages are Internal.
- The configuration, user, and application programming interfaces for RESTful access over HTTP to directory data are Evolving. This includes interfaces exposed for the HTTP connection handler, its access log, and also the REST to LDAP gateway.
- Text in log messages should be considered Internal. Log message IDs are Evolving.
- The default content of `cn=schema` (directory server LDAP schema) is Evolving.
- The monitoring interface `cn=monitor` for LDAP and the monitoring interface exposed by the JMX connection handler are Evolving.

- Interfaces that are not described in released product documentation should be considered Internal/Undocumented. For example, the LDIF representation of the server configuration, `config.ldif`, should be considered Internal.

Open Identity Platform Product Release Levels

Open Identity Platform defines Major, Minor, and Maintenance product release levels. The release level is reflected in the version number. The release level tells you what sort of compatibility changes to expect.

Release Level Definitions

Release Label	Version Numbers	Characteristics
Major	Version: x[.0.0] (trailing 0s are optional)	• Bring major new features, minor features, and bug fixes • Can include changes even to Stable interfaces • Can remove previously Deprecated functionality, and in rare cases remove Evolving functionality that has not been explicitly Deprecated • Include changes present in previous Minor and Maintenance releases
Minor	Version: x.y[.0] (trailing 0s are optional)	• Bring minor features, and bug fixes • Can include backwards-compatible changes to Stable interfaces in the same Major release, and incompatible changes to Evolving interfaces • Can remove previously Deprecated functionality • Include changes present in previous Minor and Maintenance releases
Maintenance	Version: x.y.z	• Bring bug fixes • Are intended to be fully compatible with previous versions from the same Minor release

Open Identity Platform Product Interface Stability

Open Identity Platform products support many protocols, APIs, GUIs, and command-line interfaces. Some of these interfaces are standard and very stable. Others offer new functionality that is continuing to evolve.

Open Identity Platform Community acknowledges that you invest in these interfaces, and therefore must know when and how Open Identity Platform Community expects them to change. For that reason, Open Identity Platform Community defines interface stability labels and uses these definitions in Open Identity Platform products.

Interface Stability Definitions

Stability Label	Definition
Stable	This documented interface is expected to undergo backwards-compatible changes only for major releases. Changes may be announced at least one minor release before they take effect.
Evolving	This documented interface is continuing to evolve and so is expected to change, potentially in backwards-incompatible ways even in a minor release. Changes are documented at the time of product release. While new protocols and APIs are still in the process of standardization, they are Evolving. This applies for example to recent Internet-Draft implementations, and also to newly developed functionality.
Deprecated	This interface is deprecated and likely to be removed in a future release. For previously stable interfaces, the change was likely announced in a previous release. Deprecated interfaces will be removed from Open Identity Platform products.
Removed	This interface was deprecated in a previous release and has now been removed from the product.
Internal/Undocumented	Internal and undocumented interfaces can change without notice. If you depend on one of these interfaces, contact Open Identity Platform Approved Vendors to discuss your needs.

Appendix K: Log Message Reference

"Server Logs" in the *Administration Guide* describes logs. Access and audit logs concern client operations rather than OpenDJ directory server and tools, and so are not listed here. Instead, this appendix covers severe and fatal error messages for the directory server and its tools, such as those logged in `/path/to/opendj/logs/errors`, and `/path/to/opendj/logs/replication`.

Log Message Category: ADMIN

ID: 1

Severity: ERROR

Message: An error occurred while trying to retrieve relation configuration entry %s: %s.

ID: 3

Severity: ERROR

Message: An error occurred while trying to retrieve the managed object configuration entry %s: %s.

ID: 4

Severity: ERROR

Message: The managed object configuration entry %s does not appear to exist in the Directory Server configuration. This is a required entry.

ID: 5

Severity: ERROR

Message: An error occurred while trying to decode the managed object configuration entry %s: %s.

ID: 6

Severity: ERROR

Message: The Directory Server was unable to load class %s and use it to create a component instance as defined in configuration entry %s. The error that occurred was: %s. This component will be disabled.

ID: 9

Severity: ERROR

Message: The Directory Server jar file %s in directory %s cannot be loaded because an unexpected error occurred while trying to open the file for reading: %s.

ID: 13

Severity: ERROR

Message: Unable to read the Directory Server extensions because the extensions directory %s exists but is not a directory.

ID: 14

Severity: ERROR

Message: Unable to read the Directory Server extensions from directory %s because an unexpected error occurred while trying to list the files in that directory: %s.

ID: 15

Severity: ERROR

Message: The core administration manifest file %s cannot be located.

ID: 17

Severity: ERROR

Message: The administration manifest file %s associated with the extension %s cannot be loaded because an unexpected error occurred while trying to read it: %s.

ID: 57

Severity: ERROR

Message: Unable to register an add/delete listener against the entry "%s" because it does not exist in the configuration.

ID: 74

Severity: ERROR

Message: Reason unknown.

ID: 75

Severity: ERROR

Message: A configuration exception occurred while evaluating a constraint: %s.

ID: 82

Severity: ERROR

Message: The %s could be found but did not contain any type information (e.g. missing object classes in LDAP).

ID: 83

Severity: ERROR

Message: The %s could be found but did not contain the expected type information (e.g. incorrect object classes in LDAP).

ID: 84

Severity: ERROR

Message: The %s could be found but its type resolved to an abstract managed object definition.

ID: 86

Severity: ERROR

Message: The default values for the "%s" property could not be determined.

ID: 87

Severity: ERROR

Message: The value "%s" is not a valid value for the "%s" property, which must have the following syntax: %s.

ID: 89

Severity: ERROR

Message: The "%s" property must be specified as it is mandatory.

ID: 90

Severity: ERROR

Message: The "%s" property must not be modified as it is read-only.

ID: 91

Severity: ERROR

Message: The "%s" property must not contain more than one value.

ID: 92

Severity: ERROR

Message: An internal error occurred while processing property "%s": unknown property type "%s".

ID: 93

Severity: ERROR

Message: Authentication failure.

ID: 94

Severity: ERROR

Message: The requested authentication mechanism is not supported by the server.

ID: 95

Severity: ERROR

Message: Authorization failure.

ID: 96

Severity: ERROR

Message: A communication problem occurred while contacting the server.

ID: 97

Severity: ERROR

Message: The operation was rejected for the following reason: %s.

ID: 98

Severity: ERROR

Message: The operation was rejected for the following reasons: %s.

ID: 99

Severity: ERROR

Message: The operation could not be performed because a conflicting change has already occurred. There may be another client administration tool in use.

ID: 100

Severity: ERROR

Message: The %s could not be decoded due to the following reason: %s.

ID: 101

Severity: ERROR

Message: The %s could not be decoded due to the following reasons: %s.

ID: 102

Severity: ERROR

Message: Empty managed object names are not permitted.

ID: 103

Severity: ERROR

Message: Blank managed object names are not permitted.

ID: 104

Severity: ERROR

Message: The managed object name "%s" is not a valid value for the naming property "%s", which must have the following syntax: %s.

ID: 105

Severity: ERROR

Message: The managed object name "%s" is not permitted.

ID: 106

Severity: ERROR

Message: The managed object could not be created because there is an existing managed object with the same name.

ID: 107

Severity: ERROR

Message: The requested managed object could not be found.

ID: 108

Severity: ERROR

Message: The "%s" property is mandatory.

ID: 109

Severity: ERROR

Message: The following properties are mandatory: %s.

ID: 110

Severity: ERROR

Message: The property "%s" was not recognized.

ID: 111

Severity: ERROR

Message: A communication problem occurred while contacting the server: %s.

ID: 112

Severity: ERROR

Message: The following constraint violation occurred: %s.

ID: 113

Severity: ERROR

Message: The following constraint violations occurred: %s.

ID: 114

Severity: ERROR

Message: The value "%s" in property "%s" in the %s in entry "%s" refers to a non-existent %s in entry "%s".

ID: 116

Severity: ERROR

Message: The value "%s" in property "%s" in the %s in entry "%s" refers to a disabled %s in entry "%s".

ID: 117

Severity: ERROR

Message: The %s in entry "%s" cannot be deleted because it is referenced by the "%s" property of the %s in entry "%s".

ID: 118

Severity: ERROR

Message: The %s in entry "%s" cannot be disabled because it is referenced by the "%s" property of the %s in entry "%s".

ID: 120

Severity: ERROR

Message: An unexpected error occurred while reading the manifest file: %s.

ID: 121

Severity: ERROR

Message: An error occurred while attempting to load class "%s": %s.

ID: 122

Severity: ERROR

Message: Unable to to find the getInstance() method in the managed object definition class "%s": %s.

ID: 123

Severity: ERROR

Message: Unable to to invoke the getInstance() method in the managed object definition class "%s": %s.

ID: 124

Severity: ERROR

Message: Unable initialize the "%s" managed object definition in class "%s": %s.

ID: 125

Severity: ERROR

Message: The extension "%s" with manifest file %s cannot be loaded because an unexpected error occurred while trying to initialize it: %s.

ID: 126

Severity: ERROR

Message: The core administration classes could not be loaded from manifest file %s because an unexpected error occurred: %s.

ID: 127

Severity: ERROR

Message: The %s "%s" referenced in property "%s" does not exist.

ID: 128

Severity: ERROR

Message: The %s "%s" referenced in property "%s" exists but has an invalid configuration: %s.

ID: 129

Severity: ERROR

Message: The %s "%s" referenced in property "%s" is disabled.

ID: 130

Severity: ERROR

Message: The "%s" property in the %s called "%s" references this %s.

ID: 131

Severity: ERROR

Message: The "%s" property in the %s references this %s.

ID: 132

Severity: ERROR

Message: This %s cannot be disabled because it is referenced by the "%s" property in the %s called "%s".

ID: 133

Severity: ERROR

Message: This %s cannot be disabled because it is referenced by the "%s" property in the %s.

ID: 134

Severity: ERROR

Message: An error occurred while attempting to determine if the %s in entry %s is enabled: %s.

ID: 135

Severity: ERROR

Message: The administration connector self-signed certificate cannot be generated because the following error occurred: %s.

ID: 136

Severity: ERROR

Message: The administration connector self-signed certificate cannot be generated because the following files are missing: %s.

Log Message Category: ADMIN_TOOL

ID: N/A

Severity: ERROR

Message: There is already an existing backend with name: %s.

Log Message Category: BACKEND

ID: 2

Severity: ERROR

Message: An attempt was made to configure the root DSE backend without providing a configuration entry. This is not allowed.

ID: 9

Severity: ERROR

Message: Unwilling to update entry "%s" because modify operations are not supported in the root DSE backend. If you wish to alter the contents of the root DSE itself, then it may be possible to do so by modifying the "%s" entry in the configuration.

ID: 11

Severity: ERROR

Message: Unwilling to perform a search (connection ID %d, operation ID %d) with a base DN of "%s" in the root DSE backend. The base DN for searches in this backend must be the DN of the root DSE itself.

ID: 12

Severity: ERROR

Message: An unexpected failure occurred while trying to process a search operation (connection ID %d, operation ID %d) in the root DSE backend: %s.

ID: 13

Severity: ERROR

Message: Unable to process the search with connection ID %d and operation ID %d because it had an invalid scope of %s.

ID: 14

Severity: ERROR

Message: An unexpected error occurred while trying to open the LDIF writer for the root DSE backend: %s.

ID: 15

Severity: ERROR

Message: An unexpected error occurred while trying to export the root DSE entry to the specified LDIF target: %s.

ID: 17

Severity: ERROR

Message: The root DSE backend does not provide a facility for backup and restore operations. The contents of the root DSE should be backed up as part of the Directory Server configuration.

ID: 21

Severity: ERROR

Message: An attempt was made to configure the monitor backend without providing a configuration entry. This is not allowed, and no monitor information will be available over protocol.

ID: 22

Severity: ERROR

Message: An unexpected error occurred while attempting to decode cn=monitor as the base DN for the Directory Server monitor information: %s. No monitor information will be available over protocol.

ID: 23

Severity: ERROR

Message: Unwilling to add entry "%s" because add operations are not supported in the "%s" backend.

ID: 24

Severity: ERROR

Message: Unwilling to remove entry "%s" because delete operations are not supported in the "%s" backend.

ID: 25

Severity: ERROR

Message: Unwilling to update entry "%s" because modify operations are not supported in the monitor backend. If you wish to alter the contents of the base monitor entry itself, then it may be possible to do so by modifying the "%s" entry in the configuration.

ID: 26

Severity: ERROR

Message: Unwilling to rename entry "%s" because modify DN operations are not supported in the "%s" backend.

ID: 27

Severity: ERROR

Message: An error occurred while attempting to export the base monitor entry: %s.

ID: 28

Severity: ERROR

Message: An error occurred while attempting to export the monitor entry for monitor provider %s: %s.

ID: 29

Severity: ERROR

Message: The "%s" backend does not support LDIF import operations.

ID: 32

Severity: ERROR

Message: Unable to retrieve the requested entry from the "%s" backend because the provided DN was null.

ID: 33

Severity: ERROR

Message: Unable to initialize the "%s" backend because an error occurred while attempting to decode the base DN for this backend: %s.

ID: 34

Severity: ERROR

Message: Unable to retrieve the requested entry %s from the monitor backend because the DN is not below the monitor base of %s.

ID: 38

Severity: ERROR

Message: An attempt was made to configure the schema backend without providing a configuration entry. This is not allowed, and no schema information will be available over protocol.

ID: 40

Severity: ERROR

Message: An error occurred while trying to determine the base DNs to use when publishing the Directory Server schema information, as specified in the ds-cfg-schema-entry-dn attribute of configuration entry %s: %s. The default schema base DN of cn=schema will be used.

ID: 45

Severity: ERROR

Message: An error occurred while attempting to export the base schema entry: %s.

ID: 48

Severity: ERROR

Message: Unable to retrieve the requested entry %s from the schema backend because the DN is equal to one of the schema entry DNs.

ID: 49

Severity: ERROR

Message: An unexpected error occurred while trying to open the LDIF writer for the schema backend: %s.

ID: 51

Severity: ERROR

Message: An error occurred while trying to deregister %s as a schema entry DN: %s.

ID: 53

Severity: ERROR

Message: An error occurred while trying to register %s as a schema entry DN: %s.

ID: 55

Severity: ERROR

Message: The Directory Server was unable to obtain a lock on entry %s after multiple attempts. This could mean that the entry is already locked by a long-running operation or that the entry has previously been locked but was not properly unlocked.

ID: 91

Severity: ERROR

Message: The task defined in entry %s is invalid because it has an invalid state %s.

ID: 92

Severity: ERROR

Message: An error occurred while trying to parse the scheduled start time value %s from task entry %s.

ID: 93

Severity: ERROR

Message: An error occurred while trying to parse the actual start time value %s from task entry %s.

ID: 94

Severity: ERROR

Message: An error occurred while trying to parse the completion time value %s from task entry %s.

ID: 95

Severity: ERROR

Message: Task entry %s is missing required attribute %s.

ID: 96

Severity: ERROR

Message: There are multiple instances of attribute %s in task entry %s.

ID: 97

Severity: ERROR

Message: There are no values for attribute %s in task entry %s.

ID: 98

Severity: ERROR

Message: There are multiple values for attribute %s in task entry %s.

ID: 99

Severity: ERROR

Message: An error occurred while executing the task defined in entry %s: %s.

ID: 100

Severity: ERROR

Message: The provided recurring task entry does not contain attribute %s which is needed to hold the recurring task ID.

ID: 101

Severity: ERROR

Message: The provided recurring task entry contains multiple attributes with type %s, which is used to hold the recurring task ID, but only a single instance is allowed.

ID: 102

Severity: ERROR

Message: The provided recurring task entry does not contain any values for the %s attribute, which is used to specify the recurring task ID.

ID: 103

Severity: ERROR

Message: The provided recurring task entry contains multiple values for the %s attribute, which is used to specify the recurring task ID, but only a single value is allowed.

ID: 104

Severity: ERROR

Message: The provided recurring task entry does not contain attribute %s which is needed to specify recurring task schedule.

ID: 105

Severity: ERROR

Message: The provided recurring task entry contains multiple attributes with type %s, which is used to hold recurring task schedule, but only a single instance is allowed.

ID: 106

Severity: ERROR

Message: The provided recurring task entry does not contain any values for the %s attribute,

which is used to specify recurring task schedule.

ID: 107

Severity: ERROR

Message: The provided recurring task entry contains multiple values for the %s attribute, which is used to specify recurring task schedule, but only a single value is allowed.

ID: 108

Severity: ERROR

Message: An error occurred while attempting to load class %s specified in attribute %s of the provided recurring task entry: %s. Does this class exist in the Directory Server classpath?.

ID: 109

Severity: ERROR

Message: An error occurred while trying to create an instance of class %s as a Directory Server task. Is this class a subclass of %s?.

ID: 110

Severity: ERROR

Message: An error occurred while attempting to perform internal initialization on an instance of class %s with the information contained in the provided entry: %s.

ID: 112

Severity: ERROR

Message: The task backend configuration entry does not contain any base DNs. There must be exactly one base DN for task information in the Directory Server.

ID: 113

Severity: ERROR

Message: The task backend configuration entry contains multiple base DNs. There must be exactly one base DN for task information in the Directory Server.

ID: 114

Severity: ERROR

Message: An error occurred while attempting to decode recurring task base %s as a DN: %s.

ID: 115

Severity: ERROR

Message: An error occurred while attempting to decode scheduled task base %s as a DN: %s.

ID: 121

Severity: ERROR

Message: The specified task data backing file %s already exists and the Directory Server will not attempt to overwrite it. Please delete or rename the existing file before attempting to use that path for the new backing file, or choose a new path.

ID: 122

Severity: ERROR

Message: The specified path %s for the new task data backing file appears to be an invalid path. Please choose a new path for the task data backing file.

ID: 123

Severity: ERROR

Message: The parent directory %s for the new task data backing file %s does not exist. Please create this directory before attempting to use this path for the new backing file or choose a new path.

ID: 124

Severity: ERROR

Message: The parent directory %s for the new task data backing file %s exists but is not a directory. Please choose a new path for the task data backing file.

ID: 125

Severity: ERROR

Message: An error occurred while attempting to determine the new path to the task data backing file: %s.

ID: 130

Severity: ERROR

Message: New entries in the task backend may only be added immediately below %s for scheduled tasks or immediately below %s for recurring tasks.

ID: 133

Severity: ERROR

Message: Unable to add recurring task %s to the task scheduler because another recurring task already exists with the same ID.

ID: 134

Severity: ERROR

Message: Unable to schedule task %s because another task already exists with the same ID.

ID: 136

Severity: ERROR

Message: An error occurred while attempting to schedule the next iteration of recurring task %s:

%s.

ID: 137

Severity: ERROR

Message: An error occurred while attempting to read an entry from the tasks backing file %s on or near line %d: %s. This is not a fatal error, so the task scheduler will attempt to continue parsing the file and schedule any additional tasks that it contains.

ID: 138

Severity: ERROR

Message: An error occurred while attempting to read an entry from the tasks backing file %s on or near line %d: %s. This is an unrecoverable error, and parsing cannot continue.

ID: 139

Severity: ERROR

Message: Entry %s read from the tasks backing file is invalid because it has no parent and does not match the task root DN of %s.

ID: 140

Severity: ERROR

Message: An error occurred while attempting to parse entry %s as a recurring task and add it to the scheduler: %s.

ID: 141

Severity: ERROR

Message: An error occurred while attempting to parse entry %s as a task and add it to the scheduler: %s.

ID: 142

Severity: ERROR

Message: Entry %s read from the tasks backing file %s has a DN which is not valid for a task or recurring task definition and will be ignored.

ID: 143

Severity: ERROR

Message: An error occurred while attempting to read from the tasks data backing file %s: %s.

ID: 144

Severity: ERROR

Message: An error occurred while attempting to create a new tasks backing file %s for use with the task scheduler: %s.

ID: 145

Severity: ERROR

Message: The provided task entry does not contain attribute %s which is needed to specify the fully-qualified name of the class providing the task logic.

ID: 146

Severity: ERROR

Message: The provided task entry contains multiple attributes with type %s, which is used to hold the task class name, but only a single instance is allowed.

ID: 147

Severity: ERROR

Message: The provided task entry does not contain any values for the %s attribute, which is used to specify the fully-qualified name of the class providing the task logic.

ID: 148

Severity: ERROR

Message: The provided task entry contains multiple values for the %s attribute, which is used to specify the task class name, but only a single value is allowed.

ID: 149

Severity: ERROR

Message: An error occurred while attempting to load class %s specified in attribute %s of the provided task entry: %s. Does this class exist in the Directory Server classpath?.

ID: 150

Severity: ERROR

Message: An error occurred while trying to create an instance of class %s as a Directory Server task. Is this class a subclass of %s?.

ID: 151

Severity: ERROR

Message: An error occurred while attempting to perform internal initialization on an instance of class %s with the information contained in the provided entry: %s.

ID: 153

Severity: ERROR

Message: An error occurred while attempting to rename the new tasks backing file from %s to %s: %s. If the Directory Server is restarted, then the task scheduler may not work as expected.

ID: 154

Severity: ERROR

Message: An error occurred while attempting to write the new tasks data backing file %s: %s. Configuration information reflecting the latest update may be lost.

ID: 161

Severity: ERROR

Message: Unable to remove pending task %s because no such task exists.

ID: 162

Severity: ERROR

Message: Unable to remove pending task %s because the task is no longer pending.

ID: 163

Severity: ERROR

Message: Unable to remove completed task %s because no such task exists in the list of completed tasks.

ID: 164

Severity: ERROR

Message: Unable to remove entry %s from the task backend because its DN is either not appropriate for that backend or it is not below the scheduled or recurring tasks base entry.

ID: 165

Severity: ERROR

Message: Unable to remove entry %s from the task backend because there is no scheduled task associated with that entry DN.

ID: 166

Severity: ERROR

Message: Unable to delete entry %s from the task backend because the associated task is currently running.

ID: 167

Severity: ERROR

Message: Unable to remove entry %s from the task backend because there is no recurring task associated with that entry DN.

ID: 168

Severity: ERROR

Message: Unable to process the search operation in the task backend because the provided base DN %s is not valid for entries in the task backend.

ID: 169

Severity: ERROR

Message: Unable to process the search operation in the task backend because there is no scheduled task associated with the provided search base entry %s.

ID: 170

Severity: ERROR

Message: Unable to process the search operation in the task backend because there is no recurring task associated with the provided search base entry %s.

ID: 171

Severity: ERROR

Message: Unable to initialize the "%s" backend because the provided configuration entry is null.

ID: 176

Severity: ERROR

Message: Requested entry %s does not exist in the backup backend.

ID: 177

Severity: ERROR

Message: Unable to retrieve entry %s from the backup backend because the requested DN is one level below the base DN but does not specify a backup directory.

ID: 178

Severity: ERROR

Message: Unable to retrieve entry %s from the backup backend because the requested backup directory is invalid: %s.

ID: 179

Severity: ERROR

Message: An error occurred while attempting to examine the requested backup directory: %s.

ID: 180

Severity: ERROR

Message: Unable to retrieve entry %s from the backup backend because the requested DN is two levels below the base DN but does not specify a backup ID.

ID: 181

Severity: ERROR

Message: Unable to retrieve entry %s from the backup backend because it does not have a parent.

ID: 182

Severity: ERROR

Message: Unable to retrieve entry %s from the backup backend because the DN does not contain the backup directory in which the requested backup should reside.

ID: 183

Severity: ERROR

Message: Backup %s does not exist in backup directory %s.

ID: 186

Severity: ERROR

Message: Unwilling to update entry "%s" because modify operations are not supported in the "%s" backend.

ID: 188

Severity: ERROR

Message: The requested entry %s does not exist in the backup backend.

ID: 192

Severity: ERROR

Message: Exactly one base DN must be provided for use with the memory-based backend.

ID: 193

Severity: ERROR

Message: Entry %s already exists in the memory-based backend.

ID: 194

Severity: ERROR

Message: Entry %s does not belong in the memory-based backend.

ID: 195

Severity: ERROR

Message: Unable to add entry %s because its parent entry %s does not exist in the memory-based backend.

ID: 196

Severity: ERROR

Message: Entry %s does not exist in the "%s" backend.

ID: 197

Severity: ERROR

Message: Cannot delete entry %s because it has one or more subordinate entries.

ID: 199

Severity: ERROR

Message: Unable to create an LDIF writer: %s.

ID: 200

Severity: ERROR

Message: Cannot write entry %s to LDIF: %s.

ID: 201

Severity: ERROR

Message: Unable to create an LDIF reader: %s.

ID: 202

Severity: ERROR

Message: An unrecoverable error occurred while reading from LDIF: %s.

ID: 203

Severity: ERROR

Message: An unexpected error occurred while processing the import: %s.

ID: 204

Severity: ERROR

Message: The memory-based backend does not support backup or restore operations.

ID: 205

Severity: ERROR

Message: Cannot rename entry %s because it has one or more subordinate entries.

ID: 206

Severity: ERROR

Message: Cannot rename entry %s because the target entry is in a different backend.

ID: 207

Severity: ERROR

Message: Cannot rename entry %s because the new parent entry %s doesn’t exist.

ID: 210

Severity: ERROR

Message: An error occurred while attempting to register base DN %s in the Directory Server: %s.

ID: 212

Severity: ERROR

Message: The schema backend does not support the %s modification type.

ID: 213

Severity: ERROR

Message: The schema backend does not support the modification of the %s attribute type. Only attribute types, object classes, ldap syntaxes, name forms, DIT content rules, DIT structure rules, and matching rule uses may be modified.

ID: 216

Severity: ERROR

Message: An error occurred while attempting to decode the object class "%s": %s.

ID: 217

Severity: ERROR

Message: Unable to add objectclass %s because its superior class of %s is not defined in the server schema.

ID: 218

Severity: ERROR

Message: Unable to add objectclass %s because it requires attribute %s which is not defined in the server schema.

ID: 219

Severity: ERROR

Message: Unable to add objectclass %s because it allows attribute %s which is not defined in the server schema.

ID: 222

Severity: ERROR

Message: An error occurred while attempting to write the updated schema: %s.

ID: 223

Severity: ERROR

Message: An error occurred while attempting to decode the name form "%s": %s.

ID: 224

Severity: ERROR

Message: An error occurred while attempting to decode the DIT content rule "%s": %s.

ID: 225

Severity: ERROR

Message: An error occurred while attempting to decode the DIT structure rule "%s": %s.

ID: 226

Severity: ERROR

Message: An error occurred while attempting to decode the matching rule use "%s": %s.

ID: 227

Severity: ERROR

Message: The server will not allow removing all values for the %s attribute type in the server schema.

ID: 228

Severity: ERROR

Message: Unable to add attribute type %s because it conflicts with multiple existing attribute types (%s and %s).

ID: 230

Severity: ERROR

Message: Unable to add objectclass %s because it conflicts with multiple existing objectclasses (%s and %s).

ID: 231

Severity: ERROR

Message: Unable to add name form %s because it conflicts with multiple existing name forms (%s and %s).

ID: 232

Severity: ERROR

Message: Unable to add name form %s because it references structural objectclass %s which is not defined in the server schema.

ID: 233

Severity: ERROR

Message: Unable to add name form %s because it references required attribute type %s which is not defined in the server schema.

ID: 234

Severity: ERROR

Message: Unable to add name form %s because it references optional attribute type %s which is not defined in the server schema.

ID: 235

Severity: ERROR

Message: Unable to add DIT content rule %s because it conflicts with multiple existing DIT content rules (%s and %s).

ID: 236

Severity: ERROR

Message: Unable to add DIT content rule %s because it references structural objectclass %s which is already associated with another DIT content rule %s.

ID: 237

Severity: ERROR

Message: Unable to add DIT content rule %s because it references structural objectclass %s which is not defined in the server schema.

ID: 238

Severity: ERROR

Message: Unable to add DIT content rule %s because it references auxiliary objectclass %s which is not defined in the server schema.

ID: 239

Severity: ERROR

Message: Unable to add DIT content rule %s because it references required attribute type %s which is not defined in the server schema.

ID: 240

Severity: ERROR

Message: Unable to add DIT content rule %s because it references optional attribute type %s which is not defined in the server schema.

ID: 241

Severity: ERROR

Message: Unable to add DIT content rule %s because it references prohibited attribute type %s which is not defined in the server schema.

ID: 242

Severity: ERROR

Message: Unable to add DIT structure rule %s because it conflicts with multiple existing DIT structure rules (%s and %s).

ID: 243

Severity: ERROR

Message: Unable to add DIT structure rule %s because it references name form %s which is already associated with another DIT structure rule %s.

ID: 244

Severity: ERROR

Message: Unable to add DIT structure rule %s because it references name form %s which is not defined in the server schema.

ID: 245

Severity: ERROR

Message: Unable to add matching rule use %s because it conflicts with multiple existing matching rule uses (%s and %s).

ID: 246

Severity: ERROR

Message: Unable to add matching rule use %s because it references matching rule %s which is already associated with another matching rule use %s.

ID: 247

Severity: ERROR

Message: Unable to add matching rule use %s because it references attribute type %s which is not defined in the server schema.

ID: 248

Severity: ERROR

Message: Circular reference detected for attribute type %s in which the superior type chain references the attribute type itself.

ID: 249

Severity: ERROR

Message: Circular reference detected for objectclass %s in which the superior class chain references the objectclass itself.

ID: 250

Severity: ERROR

Message: Circular reference detected for DIT structure rule %s in which the superior rule chain references the DIT structure rule itself.

ID: 251

Severity: ERROR

Message: An error occurred while attempting to create copies of the existing schema files before applying the updates: %s. The server was able to restore the original schema configuration, so no additional cleanup should be required.

ID: 252

Severity: ERROR

Message: An error occurred while attempting to create copies of the existing schema files before applying the updates: %s. A problem also occurred when attempting to restore the original schema configuration, so the server may be left in an inconsistent state and could require manual cleanup.

ID: 253

Severity: ERROR

Message: An error occurred while attempting to write new versions of the server schema files: %s. The server was able to restore the original schema configuration, so no additional cleanup should be required.

ID: 254

Severity: ERROR

Message: An error occurred while attempting to write new versions of the server schema files: %s. A problem also occurred when attempting to restore the original schema configuration, so the server may be left in an inconsistent state and could require manual cleanup.

ID: 255

Severity: ERROR

Message: Unable to remove attribute type %s from the server schema because no such attribute type is defined.

ID: 256

Severity: ERROR

Message: Unable to remove attribute type %s from the server schema because it is referenced as the superior type for attribute type %s.

ID: 257

Severity: ERROR

Message: Unable to remove attribute type %s from the server schema because it is referenced as a required or optional attribute type in objectclass %s.

ID: 258

Severity: ERROR

Message: Unable to remove attribute type %s from the server schema because it is referenced as a required or optional attribute type in name form %s.

ID: 259

Severity: ERROR

Message: Unable to remove attribute type %s from the server schema because it is referenced as a required, optional, or prohibited attribute type in DIT content rule %s.

ID: 260

Severity: ERROR

Message: Unable to remove attribute type %s from the server schema because it is referenced by matching rule use %s.

ID: 261

Severity: ERROR

Message: Unable to remove objectclass %s from the server schema because no such objectclass is defined.

ID: 262

Severity: ERROR

Message: Unable to remove objectclass %s from the server schema because it is referenced as the superior class for objectclass %s.

ID: 263

Severity: ERROR

Message: Unable to remove objectclass %s from the server schema because it is referenced as the structural class for name form %s.

ID: 264

Severity: ERROR

Message: Unable to remove objectclass %s from the server schema because it is referenced as a structural or auxiliary class for DIT content rule %s.

ID: 265

Severity: ERROR

Message: Unable to remove name form %s from the server schema because no such name form is defined.

ID: 266

Severity: ERROR

Message: Unable to remove name form %s from the server schema because it is referenced by DIT structure rule %s.

ID: 267

Severity: ERROR

Message: Unable to remove DIT content rule %s from the server schema because no such DIT content rule is defined.

ID: 268

Severity: ERROR

Message: Unable to remove DIT structure rule %s from the server schema because no such DIT structure rule is defined.

ID: 269

Severity: ERROR

Message: Unable to remove DIT structure rule %s from the server schema because it is referenced as a superior rule for DIT structure rule %s.

ID: 270

Severity: ERROR

Message: Unable to remove matching rule use %s from the server schema because no such matching rule use is defined.

ID: 271

Severity: ERROR

Message: Unable to add name form %s because it references objectclass %s which is defined in the server schema but is not a structural objectclass.

ID: 272

Severity: ERROR

Message: Unable to add DIT content rule %s because it references structural objectclass %s which is defined in the server schema but is not structural.

ID: 274

Severity: ERROR

Message: Unable to add attribute type %s because the superior type %s is marked as OBSOLETE in the server schema.

ID: 275

Severity: ERROR

Message: Unable to add attribute type %s because the associated matching rule %s is marked as OBSOLETE in the server schema.

ID: 276

Severity: ERROR

Message: Unable to add object class %s because the superior class %s is marked as OBSOLETE in the server schema.

ID: 277

Severity: ERROR

Message: Unable to add object class %s because required attribute %s is marked as OBSOLETE in the server schema.

ID: 278

Severity: ERROR

Message: Unable to add object class %s because optional attribute %s is marked as OBSOLETE in the server schema.

ID: 279

Severity: ERROR

Message: Unable to add name form %s because its structural object class %s is marked as OBSOLETE in the server schema.

ID: 280

Severity: ERROR

Message: Unable to add name form %s because it requires attribute type %s which is marked as OBSOLETE in the server schema.

ID: 281

Severity: ERROR

Message: Unable to add name form %s because it allows attribute type %s which is marked as OBSOLETE in the server schema.

ID: 282

Severity: ERROR

Message: Unable to add DIT content rule %s because its structural object class %s is marked as OBSOLETE in the server schema.

ID: 283

Severity: ERROR

Message: Unable to add DIT content rule %s because it references auxiliary object class %s which is defined in the server schema but is not an auxiliary class.

ID: 285

Severity: ERROR

Message: Unable to add DIT content rule %s because it requires attribute type %s which is marked as OBSOLETE in the server schema.

ID: 286

Severity: ERROR

Message: Unable to add DIT content rule %s because it allows attribute type %s which is marked as OBSOLETE in the server schema.

ID: 287

Severity: ERROR

Message: Unable to add DIT content rule %s because it prohibits attribute type %s which is marked as OBSOLETE in the server schema.

ID: 288

Severity: ERROR

Message: Unable to add DIT structure rule %s because its name form %s is marked OBSOLETE in the server schema.

ID: 289

Severity: ERROR

Message: Unable to add DIT structure rule %s because it references superior rule %s which is marked as OBSOLETE in the server schema.

ID: 290

Severity: ERROR

Message: Unable to add matching rule use %s because its matching rule %s is marked OBSOLETE in the server schema.

ID: 291

Severity: ERROR

Message: Unable to add matching rule use %s because it references attribute type %s which is marked as OBSOLETE in the server schema.

ID: 292

Severity: ERROR

Message: Unable to add DIT content rule %s because it references auxiliary object class %s which is marked as OBSOLETE in the server schema.

ID: 293

Severity: ERROR

Message: You do not have sufficient privileges to modify the Directory Server schema.

ID: 294

Severity: ERROR

Message: Unable to find a file containing concatenated schema element definitions in order to determine if any schema changes were made with the server offline. The file was expected in the %s directory and should have been named either %s or %s.

ID: 295

Severity: ERROR

Message: An error occurred while attempting to determine whether any schema changes had been made by directly editing the schema files with the server offline: %s.

ID: 296

Severity: ERROR

Message: An error occurred while attempting to write file %s containing a concatenated list of all server schema elements: %s. The server may not be able to accurately identify any schema changes made with the server offline.

ID: 298

Severity: ERROR

Message: The Directory Server is not configured to allow task %s to be invoked.

ID: 301

Severity: ERROR

Message: Requested entry %s does not exist in the trust store backend.

ID: 302

Severity: ERROR

Message: Unable to process entry %s in the trust store backend because the requested DN is one level below the base DN but does not specify a certificate name.

ID: 303

Severity: ERROR

Message: Error while trying to retrieve certificate %s from the trust store file %s: %s.

ID: 305

Severity: ERROR

Message: Indexes are not supported in the "%s" backend.

ID: 306

Severity: ERROR

Message: Unable to initialize the trust store backend from configuration entry %s because it does not contain exactly one base DN.

ID: 307

Severity: ERROR

Message: LDIF import and export operations are not supported in the "%s" backend.

ID: 308

Severity: ERROR

Message: Backup and restore operations are not supported in the "%s" backend.

ID: 309

Severity: ERROR

Message: The trust store file %s specified in attribute ds-cfg-trust-store-file of configuration entry %s does not exist.

ID: 310

Severity: ERROR

Message: The trust store type %s specified in attribute ds-cfg-trust-store-type of configuration entry %s is not valid: %s.

ID: 311

Severity: ERROR

Message: An error occurred while trying to create the PIN file %s specified in attribute ds-cfg-trust-store-pin-file of configuration entry %s.

ID: 312

Severity: ERROR

Message: An error occurred while trying to read the trust store PIN from file %s specified in configuration attribute ds-cfg-trust-store-pin-file of configuration entry %s: %s.

ID: 313

Severity: ERROR

Message: File %s specified in attribute ds-cfg-trust-store-pin-file of configuration entry %s should contain the PIN needed to access the trust store, but this file is empty.

ID: 314

Severity: ERROR

Message: Environment variable %s which is specified in attribute ds-cfg-trust-store-pin-environment-variable of configuration entry %s should contain the PIN needed to access the trust store, but this property is not set.

ID: 315

Severity: ERROR

Message: Java property %s which is specified in attribute ds-cfg-trust-store-pin-property of configuration entry %s should contain the PIN needed to access the file-based trust manager, but this property is not set.

ID: 316

Severity: ERROR

Message: An unexpected error occurred while trying to determine the value of configuration attribute ds-cfg-trust-store-file in configuration entry %s: %s.

ID: 317

Severity: ERROR

Message: An error occurred while trying to load the trust store contents from file %s: %s.

ID: 318

Severity: ERROR

Message: An error occurred while trying to create a trust manager factory to access the contents of trust store file %s: %s.

ID: 319

Severity: ERROR

Message: The certificate entry %s already exists.

ID: 320

Severity: ERROR

Message: Error while attempting to generate a self-signed certificate %s in the trust store file %s: %s.

ID: 321

Severity: ERROR

Message: Error while trying to add certificate %s to the trust store file %s: %s.

ID: 323

Severity: ERROR

Message: The entry %s could not be added because it does not contain a certificate attribute %s.

ID: 324

Severity: ERROR

Message: The entry %s could not be added because it contains multiple certificate attributes %s.

ID: 325

Severity: ERROR

Message: The entry %s could not be added because it does not contain a value of certificate attribute %s.

ID: 326

Severity: ERROR

Message: The entry %s could not be added because it contains multiple values of certificate attribute %s.

ID: 327

Severity: ERROR

Message: Error while writing certificate %s to a file: %s.

ID: 329

Severity: ERROR

Message: The root container for backend %s has not been initialized preventing this backend from processing the requested operation.

ID: 330

Severity: ERROR

Message: Unable to obtain a write lock on entry %s.

ID: 331

Severity: ERROR

Message: Entry %s cannot be modified because it does not represent a task entry. Only task entries may be modified in the task backend.

ID: 332

Severity: ERROR

Message: Entry %s cannot be modified because it does not represent a valid task in the server.

ID: 333

Severity: ERROR

Message: Entry %s cannot be modified because the assoicated task has completed running. Completed tasks cannot be modified.

ID: 334

Severity: ERROR

Message: Entry %s cannot be modified because the server does not currently support modifying recurring task entries.

ID: 335

Severity: ERROR

Message: The task associated with entry %s is currently running. The only modification allowed for running tasks is to replace the value of the ds-task-state attribute with "cancel".

ID: 337

Severity: ERROR

Message: Error while trying to delete certificate %s from the trust store file %s: %s.

ID: 338

Severity: ERROR

Message: Unable to retrieve entry %s from the trust store backend because the certificate %s does not exist.

ID: 339

Severity: ERROR

Message: The LDIF backend defined in configuration entry %s only supports a single base DN, but was configured for use with multiple base DNs.

ID: 342

Severity: ERROR

Message: LDIF file %s configured for use with the LDIF backend defined in configuration entry %s has multiple entries with a DN of %s.

ID: 343

Severity: ERROR

Message: LDIF file %s configured for use with the LDIF backend defined in configuration entry %s includes entry %s which is not below the base DN defined for that backend.

ID: 344

Severity: ERROR

Message: LDIF file %s configured for use with the LDIF backend defined in configuration entry %s contains entry %s but its parent entry has not yet been read.

ID: 345

Severity: ERROR

Message: An error occurred while trying to create file %s to write an updated version of the data for the LDIF backend defined in configuration entry %s: %s.

ID: 346

Severity: ERROR

Message: An error occurred while trying to write updated data to file %s for the LDIF backend defined in configuration entry %s: %s.

ID: 347

Severity: ERROR

Message: An error occurred while attempting to rename file %s to %s while writing updated data for the LDIF backend defined in configuration entry %s: %s.

ID: 348

Severity: ERROR

Message: Entry %s already exists in the LDIF backend.

ID: 349

Severity: ERROR

Message: The parent for entry %s does not exist.

ID: 350

Severity: ERROR

Message: Entry %s does not exist.

ID: 351

Severity: ERROR

Message: Entry %s has one or more subordinate entries and cannot be deleted until all of its subordinate entries are removed first.

ID: 352

Severity: ERROR

Message: Entry %s does not exist.

ID: 353

Severity: ERROR

Message: Source entry %s does not exist.

ID: 354

Severity: ERROR

Message: Target entry %s already exists.

ID: 355

Severity: ERROR

Message: The new parent DN %s does not exist.

ID: 356

Severity: ERROR

Message: Entry %s specified as the search base DN does not exist.

ID: 357

Severity: ERROR

Message: An error occurred while trying to create the writer for the LDIF export operation: %s.

ID: 358

Severity: ERROR

Message: An error occurred while trying to write entry %s during the LDIF export: %s.

ID: 359

Severity: ERROR

Message: An error occurred while trying to create the reader for the LDIF import operation: %s.

ID: 360

Severity: ERROR

Message: An unrecoverable error occurred while attempting to read data from the import file: %s. The LDIF import cannot continue.

ID: 361

Severity: ERROR

Message: The LDIF backend currently does not provide a backup or restore mechanism. Use LDIF import and export operations instead.

ID: 365

Severity: ERROR

Message: The target entry %s does not exist.

ID: 366

Severity: ERROR

Message: The target entry %s does not exist.

ID: 367

Severity: ERROR

Message: Error reading key %s from key store %s: %s.

ID: 368

Severity: ERROR

Message: This backend does not provide support for the hasSubordinates operational attribute.

ID: 369

Severity: ERROR

Message: This backend does not provide support for the numSubordinates operational attribute.

ID: 371

Severity: ERROR

Message: The provided recurring task entry attribute %s holding the recurring task schedule has invalid number of tokens.

ID: 372

Severity: ERROR

Message: The provided recurring task entry attribute %s holding the recurring task schedule has invalid minute token.

ID: 373

Severity: ERROR

Message: The provided recurring task entry attribute %s holding the recurring task schedule has invalid hour token.

ID: 374

Severity: ERROR

Message: The provided recurring task entry attribute %s holding the recurring task schedule has invalid day of the month token.

ID: 375

Severity: ERROR

Message: The provided recurring task entry attribute %s holding the recurring task schedule has invalid month of the year token.

ID: 376

Severity: ERROR

Message: The provided recurring task entry attribute %s holding the recurring task schedule has invalid day of the week token.

ID: 377

Severity: ERROR

Message: The provided recurring task entry attribute %s holding the recurring task schedule has invalid tokens combination yielding a nonexistent calendar date.

ID: 378

Severity: ERROR

Message: An error occurred while attempting to export task backend data: %s.

ID: 407

Severity: ERROR

Message: The information for backup %s could not be found in the backup directory %s.

ID: 409

Severity: ERROR

Message: Unable to add DIT structure rule %s because its rule identifier conflicts with existing DIT structure rule (%s).

ID: 412

Severity: ERROR

Message: Unable to schedule task %s because its dependency task %s is missing.

ID: 415

Severity: ERROR

Message: Unable to add ldap syntax description with OID %s because it conflicts with an existing ldap syntax description.

ID: 416

Severity: ERROR

Message: Unable to remove ldap syntax description %s from the server schema because no such ldap syntax description is defined.

ID: 417

Severity: ERROR

Message: The provided value "%s" could not be parsed as an ldap syntax because its OID %s corresponds to an attribute syntax that is already implemented.

ID: 418

Severity: ERROR

Message: An error occurred while attempting to decode the ldapsyntax description "%s": %s.

ID: 419

Severity: ERROR

Message: The provided recurring task schedule value has an invalid number of tokens.

ID: 420

Severity: ERROR

Message: The provided recurring task schedule value has an invalid minute token.

ID: 421

Severity: ERROR

Message: The provided recurring task schedule value has an invalid hour token.

ID: 422

Severity: ERROR

Message: The provided recurring task schedule value has an invalid day of the month token.

ID: 423

Severity: ERROR

Message: The provided recurring task schedule value has an invalid month of the year token.

ID: 424

Severity: ERROR

Message: The provided recurring task schedule value has an invalid day of the week token.

ID: 425

Severity: ERROR

Message: The schema backend does not support the Replace modification type for the %s attribute type.

ID: 426

Severity: ERROR

Message: An error occurred while trying to close file %s for the LDIF backend defined in configuration entry %s: %s.

ID: 427

Severity: ERROR

Message: The file %s written for the LDIF backend defined in configuration entry %s is 0 bytes long and unusable.

ID: 428

Severity: ERROR

Message: Configuration attribute ds-cfg-db-cache-size has a value of %d but the JVM has only %d available. Consider using ds-cfg-db-cache-percent.

ID: 429

Severity: ERROR

Message: Configuration attribute ds-cfg-db-cache-percent has a value of %d%% but the JVM has only %d%% available.

ID: 430

Severity: ERROR

Message: Unable to process the virtual list view request because the target assertion could not be decoded as a valid value for the '%s' attribute type.

ID: 433

Severity: ERROR

Message: An error occurred while trying to list the files to backup for backend '%s': %s.

ID: 434

Severity: ERROR

Message: An error occurred while trying to switch to append mode for backend '%s': %s.

ID: 435

Severity: ERROR

Message: An error occurred while trying to end append mode for backend '%s': %s.

ID: 438

Severity: ERROR

Message: Insufficient free memory (%d bytes) to perform import. At least %d bytes of free memory is required.

ID: 440

Severity: ERROR

Message: The attribute '%s' cannot have indexing of type '%s' because it does not have a corresponding matching rule.

ID: 441

Severity: ERROR

Message: Unable to process the virtual list view request because the target start position was before the beginning of the result set.

ID: 443

Severity: ERROR

Message: The entry database does not contain a record for ID %s.

ID: 444

Severity: ERROR

Message: Unable to examine the entry with ID %s for sorting purposes: %s.

ID: 445

Severity: ERROR

Message: Execution error during backend operation: %s.

ID: 446

Severity: ERROR

Message: Interrupted error during backend operation: %s.

ID: 447

Severity: ERROR

Message: The backend database directory could not be created: %s.

ID: 451

Severity: ERROR

Message: The backend database directory '%s' is not a valid directory.

ID: 453

Severity: ERROR

Message: The entry '%s' cannot be added because an entry with that name already exists.

ID: 454

Severity: ERROR

Message: The entry '%s' cannot be added because its parent entry does not exist.

ID: 455

Severity: ERROR

Message: There is no index configured for attribute type '%s'.

ID: 456

Severity: ERROR

Message: An error occurred while preloading the database cache for backend %s: %s.

ID: 457

Severity: ERROR

Message: An error occurred while attempting to decode an attribute description token from the compressed schema definitions: %s.

ID: 458

Severity: ERROR

Message: An error occurred while attempting to decode an object class set token from the

compressed schema definitions: %s.

ID: 459

Severity: ERROR

Message: An error occurred while attempting to store compressed schema information in the database: %s.

ID: 460

Severity: ERROR

Message: An error occurred while parsing the search filter %s defined for VLV index %s: %s.

ID: 461

Severity: ERROR

Message: Sort attribute %s for VLV index %s is not defined in the server schema.

ID: 462

Severity: ERROR

Message: Database exception: %s.

ID: 463

Severity: ERROR

Message: A plugin caused the delete operation to be aborted while deleting a subordinate entry %s.

ID: 464

Severity: ERROR

Message: The entry '%s' cannot be removed because it has subordinate entries.

ID: 465

Severity: ERROR

Message: The entry '%s' cannot be removed because it does not exist.

ID: 466

Severity: ERROR

Message: An entry container named '%s' is already registered for base DN '%s'.

ID: 467

Severity: ERROR

Message: The entry database does not contain a valid record for ID %s.

ID: 468

Severity: ERROR

Message: I/O error occurred while exporting entry: %s.

ID: 469

Severity: ERROR

Message: The backend must be disabled before the import process can start.

ID: 471

Severity: ERROR

Message: Unable to create the temporary directory %s.

ID: 481

Severity: ERROR

Message: The parent entry '%s' does not exist.

ID: 482

Severity: ERROR

Message: Entry record is not compatible with this version of the backend database. Entry version: %x.

ID: 483

Severity: ERROR

Message: An error occurred while reading from index %s. The index seems to be corrupt and is now operating in a degraded state. The index must be rebuilt before it can return to normal operation.

ID: 484

Severity: ERROR

Message: The following paged results control cookie value was not recognized: %s.

ID: 487

Severity: ERROR

Message: A plugin caused the modify DN operation to be aborted while moving and/or renaming an entry from %s to %s.

ID: 488

Severity: ERROR

Message: A plugin caused the modify DN operation to be aborted while moving and/or renaming an entry from %s to %s because the change to that entry violated the server schema configuration: %s.

ID: 489

Severity: ERROR

Message: The entry cannot be renamed to '%s' because an entry with that name already exists.

ID: 490

Severity: ERROR

Message: The entry '%s' cannot be renamed because it does not exist.

ID: 491

Severity: ERROR

Message: The entry '%s' cannot be modified because it does not exist.

ID: 492

Severity: ERROR

Message: The entry cannot be moved because the new parent entry '%s' does not exist.

ID: 493

Severity: ERROR

Message: The database environment could not be opened: %s.

ID: 494

Severity: ERROR

Message: Rebuilding system index(es) must be done with the backend containing the base DN disabled.

ID: 495

Severity: ERROR

Message: The backend database files could not be removed: %s.

ID: 496

Severity: ERROR

Message: The requested search operation included both the simple paged results control and the virtual list view control. These controls are mutually exclusive and cannot be used together.

ID: 497

Severity: ERROR

Message: The search results cannot be sorted because the given search request is not indexed.

ID: 498

Severity: ERROR

Message: The search base entry '%s' does not exist.

ID: 499

Severity: ERROR

Message: You do not have sufficient privileges to perform an unindexed search.

ID: 500

Severity: ERROR

Message: Unchecked exception during database transaction: %s.

ID: 501

Severity: ERROR

Message: There is no VLV index configured with name '%s'.

ID: 561

Severity: ERROR

Message: The database logging level string '%s' provided for configuration entry '%s' is invalid. The value must be one of OFF, SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST, or ALL. Note that these values are case sensitive.

ID: 569

Severity: ERROR

Message: Configuration attribute ds-cfg-db-cache-size has a value of %d which is less than the minimum: %d.

ID: 570

Severity: ERROR

Message: Configuration attributes ds-cfg-db-txn-no-sync and ds-cfg-db-txn-write-no-sync are mutually exclusive and cannot be both set at the same time.

ID: 579

Severity: ERROR

Message: The backend must be disabled before verification process can start.

ID: 583

Severity: ERROR

Message: Missing ID %d%n%s.

ID: 584

Severity: ERROR

Message: Missing entry %s in VLV index %s.

ID: 585

Severity: ERROR

Message: Reference to unknown entry ID %s%n%s.

ID: 586

Severity: ERROR

Message: Reference to entry ID %s has a key which does not match the expected key%n%s.

ID: 587

Severity: ERROR

Message: Empty ID set: %n%s.

ID: 588

Severity: ERROR

Message: Duplicate reference to ID %d%n%s.

ID: 589

Severity: ERROR

Message: Reference to unknown ID %d%n%s.

ID: 590

Severity: ERROR

Message: Reference to entry <%s> which does not match the value%n%s.

ID: 591

Severity: ERROR

Message: File dn2id is missing key %s.

ID: 592

Severity: ERROR

Message: File dn2id has ID %d instead of %d for key %s.

ID: 593

Severity: ERROR

Message: File dn2id has DN <%s> referencing unknown ID %d.

ID: 594

Severity: ERROR

Message: File dn2id has DN <%s> referencing entry with wrong DN <%s>.

ID: 595

Severity: ERROR

Message: The stored entry count in id2entry (%d) does not agree with the actual number of entry records found (%d).

ID: 596

Severity: ERROR

Message: File id2childrenCount has wrong number of children for DN <%s> (got %d, expecting %d).

ID: 597

Severity: ERROR

Message: File id2ChildrenCount references non-existing EntryID <%d>.

ID: 600

Severity: ERROR

Message: Ignoring schema definition '%s' because the following error occurred while it was being parsed: %s.

ID: 601

Severity: ERROR

Message: Schema definition could not be parsed as valid attribute value.

ID: 602

Severity: ERROR

Message: Attribute %s is set as confidential on a backend whose entries are still cleartext. Enable confidentiality on the backend first.

ID: 603

Severity: ERROR

Message: The attribute '%s' cannot enable confidentiality for keys and values at the same time.

ID: 604

Severity: ERROR

Message: Cannot encode entry for writing on storage: %s.

ID: 605

Severity: ERROR

Message: Input stream ended unexpectedly while decoding entry.

ID: 606

Severity: ERROR

Message: Confidentiality cannot be disabled on suffix '%s' because the following indexes have confidentiality still enabled: %s.

ID: 608

Severity: ERROR

Message: Error while enabling confidentiality with cipher %s, %d bits: %s.

ID: 644

Severity: ERROR

Message: There are insufficient resources to perform the operation.

Log Message Category: CONFIG

ID: 1

Severity: ERROR

Message: Configuration attribute %s is required to have at least one value but the resulted operation would have removed all values.

ID: 2

Severity: ERROR

Message: Provided value %s for configuration attribute %s was rejected. The reason provided was: %s.

ID: 3

Severity: ERROR

Message: Configuration attribute %s is single-valued, but multiple values were provided.

ID: 4

Severity: ERROR

Message: Configuration attribute %s is single-valued, but adding the provided value(s) would have given it multiple values.

ID: 5

Severity: ERROR

Message: Configuration attribute %s already contains a value %s.

ID: 6

Severity: ERROR

Message: Cannot remove value %s from configuration attribute %s because the specified value

does not exist.

ID: 7

Severity: ERROR

Message: Unable to set the value for Boolean configuration attribute %s because the provided value %s was not either 'true' or 'false'.

ID: 8

Severity: ERROR

Message: Unable to retrieve the value for configuration attribute %s as an integer because that attribute does not have any values.

ID: 9

Severity: ERROR

Message: Unable to retrieve the value for configuration attribute %s as an integer because that attribute has multiple values.

ID: 10

Severity: ERROR

Message: Unable to retrieve the value for configuration attribute %s as a Java int because the value is outside the allowable range for an int.

ID: 11

Severity: ERROR

Message: Unable to set the value for integer configuration attribute %s because the provided value %s cannot be interpreted as an integer value: %s.

ID: 12

Severity: ERROR

Message: Unable to set the value for configuration attribute %s because the provided value %d is less than the lowest allowed value of %d.

ID: 13

Severity: ERROR

Message: Unable to set the value for configuration attribute %s because the provided value %d is greater than the largest allowed value of %d.

ID: 14

Severity: ERROR

Message: Unable to parse value %s for configuration attribute %s as an integer value: %s.

ID: 15

Severity: ERROR

Message: Unable to retrieve the value for configuration attribute %s as a string because that attribute does not have any values.

ID: 16

Severity: ERROR

Message: Unable to retrieve the value for configuration attribute %s as a string because that attribute has multiple values.

ID: 17

Severity: ERROR

Message: An empty value string was provided for configuration attribute %s.

ID: 18

Severity: ERROR

Message: The value %s is not included in the list of acceptable values for configuration attribute %s.

ID: 19

Severity: ERROR

Message: '%s' is not a valid unit for configuration attribute %s.

ID: 20

Severity: ERROR

Message: Cannot decode %s as an integer value and a unit for configuration attribute %s because no value/unit delimiter could be found.

ID: 21

Severity: ERROR

Message: Could not decode the integer portion of value %s for configuration attribute %s: %s.

ID: 22

Severity: ERROR

Message: The provided value %s for integer with unit attribute %s is not allowed: %s.

ID: 23

Severity: ERROR

Message: Unable to add configuration entry %s as a child of configuration entry %s because a child entry was already found with that DN.

ID: 24

Severity: ERROR

Message: Unable to remove entry %s as a child of configuration entry %s because that entry did not have a child with the specified DN.

ID: 25

Severity: ERROR

Message: Unable to remove entry %s as a child of configuration entry %s because that entry had children of its own and non-leaf entries may not be removed.

ID: 26

Severity: ERROR

Message: The specified configuration file %s does not exist or is not readable.

ID: 27

Severity: ERROR

Message: An unexpected error occurred while attempting to determine whether configuration file %s exists: %s.

ID: 28

Severity: ERROR

Message: An error occurred while attempting to open the configuration file %s for reading: %s.

ID: 29

Severity: ERROR

Message: An error occurred while attempting to read the contents of configuration file %s: %s.

ID: 30

Severity: ERROR

Message: Invalid configuration attribute %s detected: the only attribute option allowed in the Directory Server configuration is "pending" to indicate the set of pending values.

ID: 31

Severity: ERROR

Message: An error occurred at or near line %d while trying to parse the configuration from LDIF file %s: %s.

ID: 32

Severity: ERROR

Message: The specified configuration file %s does not appear to contain any configuration entries.

ID: 33

Severity: ERROR

Message: The first entry read from LDIF configuration file %s had a DN of "%s" rather than the expected "%s" which should be used as the Directory Server configuration root.

ID: 34

Severity: ERROR

Message: An unexpected error occurred while attempting to process the Directory Server configuration file %s: %s.

ID: 35

Severity: ERROR

Message: Configuration entry %s starting at or near line %s in the LDIF configuration file %s has the same DN as another entry already read from that file.

ID: 36

Severity: ERROR

Message: Configuration entry %s starting at or near line %d in the configuration LDIF file %s does not appear to have a parent entry (expected parent DN was %s).

ID: 37

Severity: ERROR

Message: The Directory Server was unable to determine the parent DN for configuration entry %s starting at or near line %d in the configuration LDIF file %s.

ID: 38

Severity: ERROR

Message: Unable to determine the Directory Server instance root from either an environment variable or based on the location of the configuration file. Please set an environment variable named %s with a value containing the absolute path to the server installation root.

ID: 39

Severity: ERROR

Message: An unexpected error occurred while trying to write configuration entry %s to LDIF: %s.

ID: 40

Severity: ERROR

Message: An unexpected error occurred while trying to close the LDIF writer: %s.

ID: 41

Severity: ERROR

Message: The Directory Server configuration may not be altered by importing a new configuration from LDIF.

ID: 49

Severity: ERROR

Message: An error occurred while attempting to create a Directory Server logger from the information in configuration entry %s: %s.

ID: 50

Severity: ERROR

Message: Configuration entry %s does not contain a valid objectclass for a Directory Server access, error, or debug logger definition.

ID: 54

Severity: ERROR

Message: Class %s specified in attribute ds-cfg-java-class of configuration entry %s cannot be instantiated as a Directory Server access logger: %s.

ID: 55

Severity: ERROR

Message: Class %s specified in attribute ds-cfg-java-class of configuration entry %s cannot be instantiated as a Directory Server error logger: %s.

ID: 56

Severity: ERROR

Message: Class %s specified in attribute ds-cfg-java-class of configuration entry %s cannot be instantiated as a Directory Server debug logger: %s.

ID: 64

Severity: ERROR

Message: Configuration attribute %s appears to contain multiple pending value sets.

ID: 65

Severity: ERROR

Message: Configuration attribute %s appears to contain multiple active value sets.

ID: 66

Severity: ERROR

Message: Configuration attribute %s does not contain an active value set.

ID: 67

Severity: ERROR

Message: Unable to parse value %s for configuration attribute %s as an integer value because the element was of an invalid type (%s).

ID: 68

Severity: ERROR

Message: Unable to parse value for configuration attribute %s as a set of integer values because the array contained elements of an invalid type (%s).

ID: 69

Severity: ERROR

Message: Unable to parse value %s for configuration attribute %s as a string value: %s.

ID: 70

Severity: ERROR

Message: Unable to parse value %s for configuration attribute %s as a string value because the element was of an invalid type (%s).

ID: 71

Severity: ERROR

Message: Unable to parse value for configuration attribute %s as a set of string values because the array contained elements of an invalid type (%s).

ID: 72

Severity: ERROR

Message: Unable to parse value %s for configuration attribute %s as an integer with unit value because the element was of an invalid type (%s).

ID: 74

Severity: ERROR

Message: Configuration entry %s does not contain attribute %s (or that attribute exists but is not accessible using JMX).

ID: 78

Severity: ERROR

Message: There is no method %s for any invokable component registered with configuration entry %s.

ID: 83

Severity: ERROR

Message: The Directory Server could not register a JMX MBean for the component associated with configuration entry %s: %s.

ID: 84

Severity: ERROR

Message: An unexpected error occurred while trying to export the Directory Server configuration to LDIF: %s.

ID: 94

Severity: ERROR

Message: Worker thread "%s" has experienced too many repeated failures while attempting to retrieve the next operation from the work queue (%d failures experienced, maximum of %d failures allowed). This worker thread will be destroyed.

ID: 95

Severity: ERROR

Message: A problem occurred while trying to create and start an instance of class %s to use as a monitor provider for the Directory Server work queue: %s. No monitor information will be available for the work queue.

ID: 98

Severity: ERROR

Message: A null value was provided for DN configuration attribute %s.

ID: 99

Severity: ERROR

Message: An error occurred while trying to parse value "%s" of attribute %s as a DN: %s.

ID: 100

Severity: ERROR

Message: Unable to parse value %s for configuration attribute %s as a DN: %s.

ID: 101

Severity: ERROR

Message: Unable to parse value %s for configuration attribute %s as a DN because the element was of an invalid type (%s).

ID: 102

Severity: ERROR

Message: Unable to parse value for configuration attribute %s as a set of DN values because the array contained elements of an invalid type (%s).

ID: 103

Severity: ERROR

Message: An unexpected error occurred while trying to register the configuration handler base DN "%s" as a private suffix with the Directory Server: %s.

ID: 104

Severity: ERROR

Message: An error occurred while trying to retrieve configuration entry cn=Backends,cn=config in order to initialize the Directory Server backends: %s.

ID: 105

Severity: ERROR

Message: The entry cn=Backends,cn=config does not appear to exist in the Directory Server configuration. This is a required entry.

ID: 107

Severity: ERROR

Message: An unexpected error occurred while interacting with backend configuration entry %s: %s.

ID: 112

Severity: ERROR

Message: An unexpected error occurred while attempting to determine whether the backend associated with configuration entry %s should be enabled or disabled: %s. It will be disabled.

ID: 115

Severity: ERROR

Message: The Directory Server was unable to load class %s and use it to create a backend instance as defined in configuration entry %s. The error that occurred was: %s. This backend will be disabled.

ID: 116

Severity: ERROR

Message: An error occurred while trying to initialize a backend loaded from class %s with the information in configuration entry %s: %s. This backend will be disabled.

ID: 117

Severity: ERROR

Message: The class %s specified in configuration entry %s does not contain a valid Directory Server backend implementation.

ID: 140

Severity: ERROR

Message: An error occurred while trying to initialize an instance of class %s as a monitor

provider as defined in configuration entry %s: %s.

ID: 154

Severity: ERROR

Message: An error occurred while trying to initialize a connection handler loaded from class %s with the information in configuration entry %s: %s. This connection handler will be disabled.

ID: 172

Severity: ERROR

Message: An error occurred while trying to initialize a matching rule loaded from class %s with the information in configuration entry %s: %s. This matching rule will be disabled.

ID: 186

Severity: ERROR

Message: An error occurred while trying to initialize an attribute syntax loaded from class %s with the information in configuration entry %s: %s. This syntax will be disabled.

ID: 188

Severity: ERROR

Message: Unable to read the Directory Server schema definitions because the schema directory %s does not exist.

ID: 189

Severity: ERROR

Message: Unable to read the Directory Server schema definitions because the schema directory %s exists but is not a directory.

ID: 190

Severity: ERROR

Message: Unable to read the Directory Server schema definitions from directory %s because an unexpected error occurred while trying to list the files in that directory: %s.

ID: 200

Severity: ERROR

Message: An unexpected error occurred that prevented the server from installing its default entry cache framework: %s.

ID: 202

Severity: ERROR

Message: An error occurred while attempting to initialize an instance of class %s for use as the Directory Server entry cache: %s. As a result, the entry cache will be disabled.

ID: 203

Severity: ERROR

Message: The configuration for the entry cache defined in configuration entry %s was not acceptable: %s.

ID: 204

Severity: ERROR

Message: The configuration for the entry cache defined in configuration entry %s was not acceptable: the entry cache level %d is already in use.

ID: 215

Severity: ERROR

Message: An unexpected error occurred while attempting to remove entry %s as a child of configuration entry %s: %s.

ID: 228

Severity: ERROR

Message: Configuration attribute %s is read-only and its values may not be altered.

ID: 245

Severity: ERROR

Message: An error occurred while attempting to initialize an instance of class %s as a Directory Server plugin using the information in configuration entry %s: %s. This plugin will be disabled.

ID: 256

Severity: ERROR

Message: Class %s specified in configuration entry %s does not contain a valid extended operation handler implementation: %s.

ID: 261

Severity: ERROR

Message: An error occurred while trying to initialize an instance of class %s as an extended operation handler as defined in configuration entry %s: %s.

ID: 277

Severity: ERROR

Message: An error occurred while trying to initialize an instance of class %s as a SASL mechanism handler as defined in configuration entry %s: %s.

ID: 278

Severity: ERROR

Message: Entry %s cannot be removed from the Directory Server configuration because that DN does not have a parent.

ID: 280

Severity: ERROR

Message: Entry %s cannot be added to the Directory Server configuration because another configuration entry already exists with that DN.

ID: 281

Severity: ERROR

Message: Entry %s cannot be added to the Directory Server configuration because that DN does not have a parent.

ID: 282

Severity: ERROR

Message: Entry %s cannot be added to the Directory Server configuration because its parent entry %s does not exist.

ID: 283

Severity: ERROR

Message: The Directory Server is unwilling to add configuration entry %s because one of the add listeners registered with the parent entry %s rejected this change with the message: %s.

ID: 284

Severity: ERROR

Message: An unexpected error occurred while attempting to add configuration entry %s as a child of entry %s: %s.

ID: 285

Severity: ERROR

Message: Entry %s cannot be removed from the Directory Server configuration because the specified entry does not exist.

ID: 286

Severity: ERROR

Message: Entry %s cannot be removed from the Directory Server configuration because the specified entry has one or more subordinate entries.

ID: 287

Severity: ERROR

Message: Entry %s cannot be removed from the Directory Server configuration because the entry does not have a parent and removing the configuration root entry is not allowed.

ID: 288

Severity: ERROR

Message: Entry %s cannot be removed from the Directory Server configuration because one of the delete listeners registered with the parent entry %s rejected this change with the message: %s.

ID: 289

Severity: ERROR

Message: An unexpected error occurred while attempting to remove configuration entry %s as a child of entry %s: %s.

ID: 290

Severity: ERROR

Message: Entry %s cannot be modified because the specified entry does not exist.

ID: 291

Severity: ERROR

Message: Entry %s cannot be modified because one of the configuration change listeners registered for that entry rejected the change: %s.

ID: 292

Severity: ERROR

Message: An unexpected error occurred while attempting to modify configuration entry %s as a child of entry %s: %s.

ID: 293

Severity: ERROR

Message: The search operation cannot be processed because base entry %s does not exist.

ID: 294

Severity: ERROR

Message: The search operation cannot be processed because the specified search scope %s is invalid.

ID: 300

Severity: ERROR

Message: An error occurred while attempting to export the new Directory Server configuration to file %s: %s.

ID: 301

Severity: ERROR

Message: An error occurred while attempting to rename the new Directory Server configuration from file %s to %s: %s.

ID: 302

Severity: ERROR

Message: Modify DN operations are not allowed in the Directory Server configuration.

ID: 328

Severity: ERROR

Message: Indicates whether the Directory Server trust manager provider should be enabled. A trust manager provider is required for operations that require access to a trust manager (e.g., communication over SSL). Changes to this configuration attribute will take effect immediately, but will only impact future attempts to access the trust manager.

ID: 376

Severity: ERROR

Message: An error occurred while trying to initialize an instance of class %s as a password storage scheme as defined in configuration entry %s: %s.

ID: 377

Severity: ERROR

Message: Unable to add a new password storage scheme entry with DN %s because there is already a storage scheme registered with that DN.

ID: 422

Severity: ERROR

Message: The Directory Server was unable to acquire a shared lock for backend %s: %s. This generally means that the backend is in use by a process that requires an exclusive lock (e.g., importing from LDIF or restoring a backup). This backend will be disabled.

ID: 442

Severity: ERROR

Message: An error occurred while trying to initialize an instance of class %s as an identity mapper as defined in configuration entry %s: %s.

ID: 448

Severity: ERROR

Message: The Directory Server does not have any identity mapper configured for use in conjunction with proxied authorization V2 operations. The Directory Server will not be able to process requests containing the proxied authorization control with a username-based authorization ID.

ID: 449

Severity: ERROR

Message: The configured proxied authorization identity mapper DN %s does not refer to an active identity mapper. The Directory Server will not be able to process requests containing the proxied authorization control with a username-based authorization ID.

ID: 463

Severity: ERROR

Message: An error occurred while attempting to load class %s referenced in synchronization provider configuration entry %s: %s.

ID: 464

Severity: ERROR

Message: An error occurred while attempting to instantiate class %s referenced in synchronization provider configuration entry %s: %s.

ID: 465

Severity: ERROR

Message: An error occurred while attempting to initialize the Directory Server synchronization provider referenced in configuration entry %s: %s.

ID: 489

Severity: ERROR

Message: An error occurred while trying to initialize an instance of class %s as a password validator as defined in configuration entry %s: %s.

ID: 505

Severity: ERROR

Message: An error occurred while trying to initialize an instance of class %s as a password generator as defined in configuration entry %s: %s.

ID: 514

Severity: ERROR

Message: No password policies have been defined below the cn=Password Policies,cn=config entry in the Directory Server configuration. At least one password policy configuration must be defined.

ID: 515

Severity: ERROR

Message: The password policy defined in configuration entry %s is invalid: %s.

ID: 516

Severity: ERROR

Message: The Directory Server default password policy is defined as %s, but that entry does not exist or is not below the password policy configuration base cn=Password Policies,cn=config.

ID: 533

Severity: ERROR

Message: An error occurred while attempting to instantiate class %s referenced in the access control configuration entry %s: %s.

ID: 541

Severity: ERROR

Message: Unable to register "%s" as an alternate bind DN for user "%s" because it is already registered as an alternate bind DN for root user "%s".

ID: 558

Severity: ERROR

Message: An error occurred while trying to initialize an instance of class %s as an account status notification handler as defined in configuration entry %s: %s.

ID: 559

Severity: ERROR

Message: Unable to add a new account status notification handler entry with DN %s because there is already a notification handler registered with that DN.

ID: 563

Severity: ERROR

Message: An error occurred while attempting to apply the changes contained in file %s to the server configuration at startup: %s.

ID: 564

Severity: ERROR

Message: Unable to apply a change at server startup: %s.

ID: 565

Severity: ERROR

Message: One or more errors occurred while applying changes on server startup: %s.

ID: 567

Severity: ERROR

Message: Configuration entry %s does not contain a valid value for configuration attribute ds-

cfg-db-directory-permissions (It should be an UNIX permission mode in three-digit octal notation.).

ID: 568

Severity: ERROR

Message: Invalid UNIX file permissions %s does not allow read and write access to the backend database directory by the backend.

ID: 571

Severity: ERROR

Message: No default password policy is configured for the Directory Server. The default password policy must be specified by the ds-cfg-default-password-policy attribute in the cn=config entry.

ID: 573

Severity: ERROR

Message: An error occurred while trying to create the configuration archive directory %s.

ID: 574

Severity: ERROR

Message: An error occurred while trying to create the configuration archive directory %s: %s.

ID: 575

Severity: ERROR

Message: An error occurred while trying to write the current configuration to the configuration archive: %s.

ID: 591

Severity: ERROR

Message: An error occurred while trying to initialize an instance of class %s as a group implementation as in configuration entry %s: %s.

ID: 598

Severity: ERROR

Message: You do not have sufficient privileges to perform add operations in the Directory Server configuration.

ID: 599

Severity: ERROR

Message: You do not have sufficient privileges to perform delete operations in the Directory Server configuration.

ID: 600

Severity: ERROR

Message: You do not have sufficient privileges to perform modify operations in the Directory Server configuration.

ID: 601

Severity: ERROR

Message: You do not have sufficient privileges to perform modify DN operations in the Directory Server configuration.

ID: 602

Severity: ERROR

Message: You do not have sufficient privileges to perform search operations in the Directory Server configuration.

ID: 603

Severity: ERROR

Message: You do not have sufficient privileges to change the set of default root privileges.

ID: 614

Severity: ERROR

Message: An error occurred while trying to initialize an instance of class %s as a certificate mapper as defined in configuration entry %s: %s.

ID: 617

Severity: ERROR

Message: An error occurred while attempting to retrieve the key manager provider base entry cn=Key Manager Providers,cn=config from the Directory Server configuration: %s.

ID: 627

Severity: ERROR

Message: An error occurred while trying to initialize an instance of class %s as a key manager provider as defined in configuration entry %s: %s.

ID: 630

Severity: ERROR

Message: An error occurred while attempting to retrieve the trust manager provider base entry cn=Trust Manager Providers,cn=config from the Directory Server configuration: %s.

ID: 640

Severity: ERROR

Message: An error occurred while trying to initialize an instance of class %s as a trust manager provider as defined in configuration entry %s: %s.

ID: 643

Severity: ERROR

Message: Unable to retrieve JMX attribute %s associated with configuration entry %s: %s.

ID: 645

Severity: ERROR

Message: %s.%s returned a result of null for entry %s.

ID: 646

Severity: ERROR

Message: %s.%s failed for entry %s: result code=%s, admin action required=%b, messages="%s".

ID: 649

Severity: ERROR

Message: Unable to parse value "%s" from config entry "%s" as a valid search filter: %s.

ID: 650

Severity: ERROR

Message: An error occurred while trying to load an instance of class %s referenced in configuration entry %s as a virtual attribute provider: %s.

ID: 651

Severity: ERROR

Message: The virtual attribute configuration in entry "%s" is not valid because attribute type %s is single-valued but provider %s may generate multiple values.

ID: 652

Severity: ERROR

Message: The virtual attribute configuration in entry "%s" is not valid because attribute type %s is single-valued but the conflict behavior is configured to merge real and virtual values.

ID: 653

Severity: ERROR

Message: Configuration entry %s cannot be modified because the change would alter its structural object class.

ID: 654

Severity: ERROR

Message: An error occurred while attempting to calculate a SHA-1 digest of file %s: %s.

ID: 656

Severity: ERROR

Message: The Directory Server encountered an error while attempting to determine whether the configuration file %s has been externally edited with the server online, and/or trying to preserve such changes: %s. Any manual changes made to that file may have been lost.

ID: 657

Severity: ERROR

Message: Class %s specified in attribute ds-cfg-java-class of configuration entry %s cannot be instantiated as a Directory Server log rotation policy: %s.

ID: 658

Severity: ERROR

Message: Class %s specified in attribute ds-cfg-java-class of configuration entry %s cannot be instantiated as a Directory Server log retention policy: %s.

ID: 659

Severity: ERROR

Message: An error occurred while attempting to create a Directory Server log rotation policy from the information in configuration entry %s: %s.

ID: 660

Severity: ERROR

Message: An error occurred while attempting to create a Directory Server log retention policy from the information in configuration entry %s: %s.

ID: 661

Severity: ERROR

Message: An error occurred while attempting to create a text writer for a Directory Server logger from the information in configuration entry %s: %s.

ID: 674

Severity: ERROR

Message: Unable to initialize an instance of class %s as a work queue as specified in configuration entry %s: %s.

ID: 676

Severity: ERROR

Message: The attempt to apply the configuration add failed. The preliminary checks were all successful and the entry was added to the server configuration, but at least one of the

configuration add listeners reported an error when attempting to apply the change: %s.

ID: 677

Severity: ERROR

Message: The attempt to apply the configuration delete failed. The preliminary checks were all successful and the entry was removed from the server configuration, but at least one of the configuration delete listeners reported an error when attempting to apply the change: %s.

ID: 678

Severity: ERROR

Message: The attempt to apply the configuration modification failed. The preliminary checks were all successful and the modified entry was written to the server configuration, but at least one of the configuration change listeners reported an error when attempting to apply the change: %s.

ID: 679

Severity: ERROR

Message: The configuration for the key manager provider defined in configuration entry %s was not acceptable: %s.

ID: 680

Severity: ERROR

Message: The configuration for the trust manager provider defined in configuration entry %s was not acceptable: %s.

ID: 681

Severity: ERROR

Message: The configuration for the trust manager provider defined in configuration entry %s was not acceptable: %s.

ID: 682

Severity: ERROR

Message: The configuration for the account status notification handler defined in configuration entry %s was not acceptable: %s.

ID: 683

Severity: ERROR

Message: The configuration for the attribute syntax defined in configuration entry %s was not acceptable: %s.

ID: 684

Severity: ERROR

Message: The configuration for the certificate mapper defined in configuration entry %s was not acceptable: %s.

ID: 686

Severity: ERROR

Message: The configuration for the group implementation defined in configuration entry %s was not acceptable: %s.

ID: 687

Severity: ERROR

Message: The configuration for the identity mapper defined in configuration entry %s was not acceptable: %s.

ID: 688

Severity: ERROR

Message: The configuration for the matching rule defined in configuration entry %s was not acceptable: %s.

ID: 689

Severity: ERROR

Message: The configuration for the password generator defined in configuration entry %s was not acceptable: %s.

ID: 690

Severity: ERROR

Message: The configuration for the password storage scheme defined in configuration entry %s was not acceptable: %s.

ID: 691

Severity: ERROR

Message: The configuration for the password validator defined in configuration entry %s was not acceptable: %s.

ID: 692

Severity: ERROR

Message: The configuration for the plugin defined in configuration entry %s was not acceptable: %s.

ID: 693

Severity: ERROR

Message: The configuration for the SASL mechanism handler defined in configuration entry %s was not acceptable: %s.

ID: 694

Severity: ERROR

Message: The configuration for the virtual attribute provider defined in configuration entry %s was not acceptable: %s.

ID: 695

Severity: ERROR

Message: The configuration for the alert handler defined in configuration entry %s was not acceptable: %s.

ID: 696

Severity: ERROR

Message: An error occurred while trying to initialize an instance of class %s as an alert handler as defined in configuration entry %s: %s.

ID: 697

Severity: ERROR

Message: The provided SMTP server value '%s' is invalid. An SMTP server value must have an IP address or a resolvable name, and it may optionally be followed by a colon and an integer value between 1 and 65535 to specify the server port number.

ID: 698

Severity: ERROR

Message: An error occurred while attempting to open the current configuration file %s for reading in order to copy it to the ".startok" file: %s.

ID: 699

Severity: ERROR

Message: An error occurred while attempting to open file %s in order to write the ".startok" configuration file: %s.

ID: 700

Severity: ERROR

Message: An error occurred while attempting to copy the current configuration from file %s into temporary file %s for use as the ".startok" configuration file: %s.

ID: 701

Severity: ERROR

Message: An error occurred while attempting to rename file %s to %s for use as the ".startok" configuration file: %s.

ID: 704

Severity: ERROR

Message: An error occurred while trying to parse and validate Berkeley DB JE property %s: %s.

ID: 705

Severity: ERROR

Message: An error occurred while trying to parse and validate Berkeley DB JE property %s: the property does not follow a singular property=value form.

ID: 706

Severity: ERROR

Message: An error occurred while trying to parse and validate Berkeley DB JE property %s: the property shadows configuration attribute %s.

ID: 707

Severity: ERROR

Message: An error occurred while trying to parse and validate Berkeley DB JE property %s: the property is already defined for this component.

ID: 709

Severity: ERROR

Message: An error occurred while attempting to open the configured log file %s for logger %s: %s.

ID: 715

Severity: ERROR

Message: Invalid UNIX file permissions %s does not allow write access to the log file by the log publisher.

ID: 716

Severity: ERROR

Message: Invalid UNIX file permissions %s: %s.

ID: 726

Severity: ERROR

Message: The configuration entry '%s' is currently defined to be the default password policy, however it is not a password policy.

ID: 727

Severity: ERROR

Message: The default password policy value '%s' is invalid because it refers to an authentication

policy which is not a password policy.

ID: 728

Severity: ERROR

Message: The timestamp format string "%s" is not a valid format string. The format string should conform to the syntax described in the documentation for the "java.text.SimpleDateFormat" class.

ID: 729

Severity: ERROR

Message: The access log filtering criteria defined in "%s" could not be parsed because it contains an invalid user DN pattern "%s".

ID: 730

Severity: ERROR

Message: The access log filtering criteria defined in "%s" could not be parsed because it contains an invalid target DN pattern "%s".

ID: 732

Severity: ERROR

Message: Class %s specified in attribute ds-cfg-java-class of configuration entry %s cannot be instantiated as a Directory Server HTTP access logger: %s.

ID: 733

Severity: ERROR

Message: The log format for configuration entry %s is empty. No information will be logged even if logging is activated.

ID: 735

Severity: ERROR

Message: An error occurred while attempting to update a Directory Server logger from the information in configuration entry %s: %s.

ID: 736

Severity: ERROR

Message: An error occurred while attempting to delete a Directory Server logger from the information in configuration entry %s: %s.

ID: 737

Severity: ERROR

Message: Cannot configure java.util.logging root logger level: %s. java.util.logging support is now disabled.

ID: 738

Severity: ERROR

Message: An error occurred while trying to initialize an instance of class %s as an HTTP endpoint as defined in configuration entry %s: %s.

ID: 739

Severity: ERROR

Message: An error occurred while starting the HTTP endpoint as defined in configuration entry %s: %s.

ID: 741

Severity: ERROR

Message: The HTTP endpoint configuration defined in %s is invalid: %s.

ID: 742

Severity: ERROR

Message: Invalid configuration URL in the REST2LDAP endpoint configuration entry %s: %s.

ID: 743

Severity: ERROR

Message: Cannot initialize the configuration framework: %s.

ID: 744

Severity: ERROR

Message: Unable to retrieve children of configuration entry with dn: %s.

ID: 745

Severity: ERROR

Message: Unable to load the configuration-enabled schema: %s.

ID: 746

Severity: ERROR

Message: Backend config error when trying to delete an entry: %s.

ID: 747

Severity: ERROR

Message: The HTTP endpoint configuration defined in %s is referencing a non existing authorization DN %s.

ID: 748

Severity: ERROR

Message: The HTTP endpoint configuration defined in %s is referencing mutually exclusive authorization DNs %s and %s.

ID: 749

Severity: ERROR

Message: Unable to read the configuration from %s in the REST2LDAP endpoint configuration entry %s: %s.

ID: 750

Severity: ERROR

Message: Invalid JSON element %s from %s in the REST2LDAP endpoint configuration entry %s: %s.

ID: 751

Severity: ERROR

Message: Invalid configuration element from %s in the REST2LDAP endpoint configuration entry %s: %s.

ID: 752

Severity: ERROR

Message: The OAuth2 authorization mechanism defined in %s contains an invalid JSON Pointer %s: %s.

ID: 753

Severity: ERROR

Message: The authorization mechanism defined in %s is referencing a non-existing or non-readable directory: %s.

ID: 754

Severity: ERROR

Message: The authorization mechanism defined in %s is referencing a non existing DN: %s.

ID: 755

Severity: ERROR

Message: The authorization mechanism defined in %s is referencing an invalid URL %s: %s.

ID: 756

Severity: ERROR

Message: Unable to configure the authorization mechanism defined in %s: %s.

ID: 757

Severity: ERROR

Message: The requested admin API version '%s' is unsupported. This endpoint only supports the following admin API version(s): %s.

ID: 763

Severity: ERROR

Message: Unable to configure the backend '%s' because one of its base DNs is the empty DN.

Log Message Category: CORE

ID: 1

Severity: ERROR

Message: Abandon requests cannot be canceled.

ID: 2

Severity: ERROR

Message: Bind requests cannot be canceled.

ID: 3

Severity: ERROR

Message: Unbind requests cannot be canceled.

ID: 108

Severity: ERROR

Message: %s encountered an uncaught exception while processing operation %s: %s.

ID: 118

Severity: ERROR

Message: The Directory Server is currently running. The configuration may not be bootstrapped while the server is online.

ID: 120

Severity: ERROR

Message: Unable to create an instance of class %s to serve as the Directory Server configuration handler: %s.

ID: 121

Severity: ERROR

Message: An error occurred while trying to initialize the configuration handler %s using configuration file %s: %s.

ID: 122

Severity: ERROR

Message: The Directory Server may not be started before the configuration has been bootstrapped.

ID: 123

Severity: ERROR

Message: The Directory Server may not be started while it is already running. Please stop the running instance before attempting to start it again.

ID: 126

Severity: ERROR

Message: Entry %s violates the Directory Server schema configuration because it is missing attribute %s which is required by objectclass %s.

ID: 127

Severity: ERROR

Message: Entry %s violates the Directory Server schema configuration because it includes attribute %s which is not allowed by any of the objectclasses defined in that entry.

ID: 130

Severity: ERROR

Message: An error occurred while attempting to bootstrap the attribute syntax defined in class %s: %s.

ID: 138

Severity: ERROR

Message: An error occurred while attempting to create the JMX MBean server that will be used for monitoring, notification, and configuration interaction within the Directory Server: %s.

ID: 140

Severity: ERROR

Message: An uncaught exception during processing for thread %s has caused it to terminate abnormally. The stack trace for that exception is: %s.

ID: 142

Severity: ERROR

Message: The Directory Server shutdown hook detected that the JVM is shutting down. This generally indicates that JVM received an external request to stop (e.g., through a kill signal).

ID: 143

Severity: ERROR

Message: Unable to decode the provided filter string as a search filter because the provided string was empty or null.

ID: 144

Severity: ERROR

Message: An unexpected error occurred while attempting to decode the string "%s" as a search filter: %s.

ID: 145

Severity: ERROR

Message: The provided search filter "%s" had mismatched parentheses around the portion between positions %d and %d.

ID: 146

Severity: ERROR

Message: The provided search filter "%s" was missing an equal sign in the suspected simple filter component between positions %d and %d.

ID: 147

Severity: ERROR

Message: The provided search filter "%s" had an invalid escaped byte value at position %d. A backslash in a value must be followed by two hexadecimal characters that define the byte that has been encoded.

ID: 148

Severity: ERROR

Message: The provided search filter "%s" could not be decoded because the compound filter between positions %d and %d did not start with an open parenthesis and end with a close parenthesis (they may be parentheses for different filter components).

ID: 149

Severity: ERROR

Message: The provided search filter "%s" could not be decoded because the closing parenthesis at position %d did not have a corresponding open parenthesis.

ID: 150

Severity: ERROR

Message: The provided search filter "%s" could not be decoded because the opening parenthesis at position %d did not have a corresponding close parenthesis.

ID: 151

Severity: ERROR

Message: The provided search filter "%s" could not be decoded because the assumed substring filter value between positions %d and %d did not have any asterisk wildcard characters.

ID: 152

Severity: ERROR

Message: The provided search filter "%s" could not be decoded because the extensible match component starting at position %d did not have a colon to denote the end of the attribute type name.

ID: 153

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because it contained an unknown filter type %s.

ID: 154

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because the internal check returned an unknown result type "%s".

ID: 155

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because the set of filter components for an %s component was NULL.

ID: 156

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because the filter was nested beyond the maximum allowed depth of 100 levels.

ID: 157

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because the NOT filter component did not include a subcomponent.

ID: 158

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because an equality component had a NULL attribute type.

ID: 159

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because an equality component for attribute %s had a NULL assertion value.

ID: 160

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because a substring component had a NULL attribute type.

ID: 161

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because a substring component for attribute %s did not have any subInitial, subAny, or subFinal elements.

ID: 162

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because a greater-or-equal component had a NULL attribute type.

ID: 163

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because a greater-or-equal component for attribute %s had a NULL assertion value.

ID: 164

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because a less-or-equal component had a NULL attribute type.

ID: 165

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because a less-or-equal component for attribute %s had a NULL assertion value.

ID: 166

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because a presence component had a NULL attribute type.

ID: 167

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because an approximate component had a NULL attribute type.

ID: 168

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because an approximate component for attribute %s had a NULL assertion value.

ID: 169

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because a contained extensible match filter did not have an assertion value.

ID: 170

Severity: ERROR

Message: Unable to determine whether entry "%s" matches filter "%s" because a contained extensible match filter did not have either an attribute type or a matching rule ID.

ID: 171

Severity: ERROR

Message: Unable to decode the provided string as a relative distinguished name because the provided string was empty or null.

ID: 172

Severity: ERROR

Message: Unable to decode the provided string "%s" as a relative distinguished name because the string ended with an attribute type name (%s).

ID: 173

Severity: ERROR

Message: Unable to decode the provided string "%s" as a relative distinguished name because the first non-blank character after the attribute type %s was not an equal sign (character read was %c).

ID: 174

Severity: ERROR

Message: Unable to decode the provided string "%s" as a relative distinguished name because it contained an unexpected plus, comma, or semicolon at position %d, which is not allowed in an RDN.

ID: 175

Severity: ERROR

Message: Unable to decode the provided string "%s" as a relative distinguished name because an illegal character %c was found at position %d, where either the end of the string or a '+' sign were expected.

ID: 183

Severity: ERROR

Message: An error occurred while trying to retrieve the root DSE configuration entry (cn=Root DSE,cn=config) from the Directory Server configuration: %s.

ID: 186

Severity: ERROR

Message: Unable to register objectclass %s with the server schema because its OID %s conflicts with the OID of an existing objectclass %s.

ID: 187

Severity: ERROR

Message: Unable to register objectclass %s with the server schema because its name %s conflicts with the name of an existing objectclass %s.

ID: 190

Severity: ERROR

Message: Unable to register matching rule %s with the server schema because its name %s conflicts with the name of an existing matching rule %s.

ID: 191

Severity: ERROR

Message: Unable to register matching rule use %s with the server schema because its matching rule %s conflicts with the matching rule for an existing matching rule use %s.

ID: 192

Severity: ERROR

Message: Unable to register DIT content rule %s with the server schema because its structural objectclass %s conflicts with the structural objectclass for an existing DIT content rule %s.

ID: 193

Severity: ERROR

Message: Unable to register DIT structure rule %s with the server schema because its name form %s conflicts with the name form for an existing DIT structure rule %s.

ID: 194

Severity: ERROR

Message: Unable to register DIT structure rule %s with the server schema because its rule ID %d conflicts with the rule ID for an existing DIT structure rule %s.

ID: 195

Severity: ERROR

Message: Unable to register name form %s with the server schema because its structural objectclass %s conflicts with the structural objectclass for an existing name form %s.

ID: 196

Severity: ERROR

Message: Unable to register name form %s with the server schema because its OID %s conflicts with the OID for an existing name form %s.

ID: 197

Severity: ERROR

Message: Unable to register name form %s with the server schema because its name %s conflicts with the name for an existing name form %s.

ID: 198

Severity: ERROR

Message: Entry %s violates the Directory Server schema configuration because it includes multiple conflicting structural objectclasses %s and %s. Only a single structural objectclass is allowed in an entry.

ID: 199

Severity: ERROR

Message: Entry %s violates the Directory Server schema configuration because it does not include a structural objectclass. All entries must contain a structural objectclass.

ID: 205

Severity: ERROR

Message: Entry %s violates the Directory Server schema configuration because it includes multiple values for attribute %s, which is defined as a single-valued attribute.

ID: 206

Severity: ERROR

Message: Entry %s violates the Directory Server schema configuration because its RDN does not contain attribute %s that is required by name form %s.

ID: 207

Severity: ERROR

Message: Entry %s violates the Directory Server schema configuration because its RDN contains attribute %s that is not allowed by name form %s.

ID: 208

Severity: ERROR

Message: Entry %s violates the Directory Server schema configuration because it is missing attribute %s which is required by DIT content rule %s.

ID: 209

Severity: ERROR

Message: Entry %s violates the Directory Server schema configuration because it contains attribute %s which is prohibited by DIT content rule %s.

ID: 211

Severity: ERROR

Message: Entry %s violates the Directory Server schema configuration because it includes auxiliary objectClass %s that is not allowed by DIT content rule %s.

ID: 213

Severity: ERROR

Message: The Directory Server was unable to evaluate entry %s to determine whether it was compliant with the DIT structure rule configuration because parent entry %s either does not exist or could not be retrieved.

ID: 214

Severity: ERROR

Message: The Directory Server was unable to evaluate entry %s to determine whether it was compliant with the DIT rule configuration because the parent entry %s does not appear to contain a valid structural objectclass.

ID: 215

Severity: ERROR

Message: Entry %s violates the Directory Server schema configuration because DIT structure rule %s does not allow entries of type %s to be placed immediately below entries of type %s.

ID: 216

Severity: ERROR

Message: An unexpected error occurred while attempting to check entry %s against DIT structure rule %s: %s.

ID: 218

Severity: ERROR

Message: Unable to bind to the Directory Server because no such user exists in the server.

ID: 220

Severity: ERROR

Message: A fatal error occurred when executing one of the Directory Server startup plugins: %s (error ID %d). The Directory Server startup process has been aborted.

ID: 221

Severity: ERROR

Message: Unable to bind to the Directory Server using simple authentication because that user does not have a password.

ID: 222

Severity: ERROR

Message: Unable to process the bind request because it attempted to use an unknown SASL mechanism %s that is not available in the Directory Server.

ID: 228

Severity: ERROR

Message: The specified entry %s does not exist in the Directory Server.

ID: 230

Severity: ERROR

Message: The provided entry cannot be added because it contains a null DN. This DN is reserved for the root DSE, and that entry may not be added over protocol.

ID: 231

Severity: ERROR

Message: The provided entry %s cannot be added because it does not have a parent and is not defined as one of the suffixes within the Directory Server.

ID: 233

Severity: ERROR

Message: Entry %s cannot be added because its parent entry %s does not exist in the server.

ID: 234

Severity: ERROR

Message: Entry %s cannot be added because the server failed to obtain a write lock for this entry after multiple attempts.

ID: 235

Severity: ERROR

Message: Entry %s cannot be removed because the server failed to obtain a write lock for this entry after multiple attempts.

ID: 238

Severity: ERROR

Message: The maximum time limit of %d seconds for processing this search operation has

expired.

ID: 239

Severity: ERROR

Message: This search operation has sent the maximum of %d entries to the client.

ID: 240

Severity: ERROR

Message: The entry %s specified as the search base does not exist in the Directory Server.

ID: 241

Severity: ERROR

Message: Entry %s does not exist in the Directory Server.

ID: 242

Severity: ERROR

Message: Entry %s cannot be removed because the backend that should contain that entry has a subordinate backend with a base DN of %s that is below the target DN.

ID: 243

Severity: ERROR

Message: A modify DN operation cannot be performed on entry %s because the new RDN would not have a parent DN.

ID: 244

Severity: ERROR

Message: The modify DN operation for entry %s cannot be performed because no backend is registered to handle that DN.

ID: 245

Severity: ERROR

Message: The modify DN operation for entry %s cannot be performed because no backend is registered to handle the new DN %s.

ID: 246

Severity: ERROR

Message: The modify DN operation for entry %s cannot be performed because the backend holding the current entry is different from the backend used to handle the new DN %s. Modify DN operations may not span multiple backends.

ID: 247

Severity: ERROR

Message: The modify DN operation for entry %s cannot be performed because the server was unable to obtain a write lock for that DN.

ID: 249

Severity: ERROR

Message: The modify DN operation for entry %s cannot be performed because the server was unable to obtain a write lock for the new DN %s.

ID: 250

Severity: ERROR

Message: The modify DN operation for entry %s cannot be performed because that entry does not exist in the server.

ID: 251

Severity: ERROR

Message: Entry %s cannot be modified because the server failed to obtain a write lock for this entry after multiple attempts.

ID: 252

Severity: ERROR

Message: Entry %s cannot be modified because no such entry exists in the server.

ID: 253

Severity: ERROR

Message: Entry %s cannot be modified because the modification contained an add component for attribute %s but no values were provided.

ID: 254

Severity: ERROR

Message: When attempting to modify entry %s to add one or more values for attribute %s, value "%s" was found to be invalid according to the associated syntax: %s.

ID: 255

Severity: ERROR

Message: Entry %s cannot be modified because it would have resulted in one or more duplicate values for attribute %s: %s.

ID: 256

Severity: ERROR

Message: Entry %s cannot be modified because the change to attribute %s would have removed a value used in the RDN.

ID: 257

Severity: ERROR

Message: Entry %s cannot be modified because the attempt to update attribute %s would have removed one or more values from the attribute that were not present: %s.

ID: 258

Severity: ERROR

Message: Entry %s cannot be modified because an attempt was made to remove one or more values from attribute %s but this attribute is not present in the entry.

ID: 259

Severity: ERROR

Message: When attempting to modify entry %s to replace the set of values for attribute %s, value "%s" was found to be invalid according to the associated syntax: %s.

ID: 260

Severity: ERROR

Message: Entry %s cannot be modified because an attempt was made to increment the value of attribute %s which is used as an RDN attribute for the entry.

ID: 261

Severity: ERROR

Message: Entry %s cannot be modified because an attempt was made to increment the value of attribute %s but the request did not include a value for that attribute specifying the amount by which to increment the value.

ID: 262

Severity: ERROR

Message: Entry %s cannot be modified because an attempt was made to increment the value of attribute %s but the request contained multiple values, where only a single integer value is allowed.

ID: 263

Severity: ERROR

Message: Entry %s cannot be modified because an attempt was made to increment the value of attribute %s but the value "%s" contained in the request could not be parsed as an integer.

ID: 264

Severity: ERROR

Message: Entry %s cannot be modified because an attempt was made to increment the value of attribute %s but that attribute did not have any values in the target entry.

ID: 265

Severity: ERROR

Message: Entry %s cannot be modified because an attempt was made to increment the value of attribute %s but the value "%s" could not be parsed as an integer.

ID: 266

Severity: ERROR

Message: Entry %s cannot be modified because the resulting entry would have violated the server schema: %s.

ID: 267

Severity: ERROR

Message: Entry %s cannot be modified because there is no backend registered to handle operations for that entry.

ID: 268

Severity: ERROR

Message: There is no extended operation handler registered with the Directory Server for handling extended operations with a request OID of %s.

ID: 269

Severity: ERROR

Message: Entry %s violates the Directory Server schema configuration because it contains an unknown objectclass %s.

ID: 270

Severity: ERROR

Message: An unexpected error was encountered while processing a search in one of the Directory Server backends: %s.

ID: 271

Severity: ERROR

Message: The modify DN operation for entry %s cannot be performed because the change would have violated the server schema: %s.

ID: 276

Severity: ERROR

Message: Object class %s cannot be added to entry %s because that class is not defined in the Directory Server schema.

ID: 277

Severity: ERROR

Message: Object class %s is already present in entry %s and cannot be added a second time.

ID: 279

Severity: ERROR

Message: The password provided by the user did not match any password(s) stored in the user's entry.

ID: 288

Severity: ERROR

Message: An error occurred while attempting to initialize the command-line arguments: %s.

ID: 289

Severity: ERROR

Message: An error occurred while attempting to parse the provided set of command line arguments: %s.

ID: 290

Severity: ERROR

Message: An error occurred while attempting to bootstrap the Directory Server: %s.

ID: 291

Severity: ERROR

Message: An error occurred while trying to start the Directory Server: %s.

ID: 292

Severity: ERROR

Message: The line "%s" associated with the backup information in directory %s could not be parsed because it did not contain an equal sign to delimit the property name from the value.

ID: 293

Severity: ERROR

Message: The line "%s" associated with the backup information in directory %s could not be parsed because it did not include a property name.

ID: 294

Severity: ERROR

Message: The backup information structure in directory %s could not be parsed because it contained multiple backup IDs (%s and %s).

ID: 295

Severity: ERROR

Message: The backup information structure in directory %s could not be parsed because it contained an unknown property %s with value %s.

ID: 296

Severity: ERROR

Message: An unexpected error occurred while trying to decode a backup information structure in directory %s: %s.

ID: 297

Severity: ERROR

Message: Unable to decode a backup information structure in directory %s because the structure did not include a backup ID.

ID: 298

Severity: ERROR

Message: The backup information structure with backup ID %s in directory %s was not valid because it did not contain the backup date.

ID: 299

Severity: ERROR

Message: Cannot add a backup with ID %s to backup directory %s because another backup already exists with that ID.

ID: 300

Severity: ERROR

Message: Cannot remove backup %s from backup directory %s because no backup with that ID exists in that directory.

ID: 301

Severity: ERROR

Message: Cannot remove backup %s from backup directory %s because it is listed as a dependency for backup %s.

ID: 302

Severity: ERROR

Message: Backup directory %s does not exist and an error occurred while attempting to create it: %s.

ID: 303

Severity: ERROR

Message: The backup directory path %s exists but does not reference a directory.

ID: 304

Severity: ERROR

Message: An error occurred while trying to remove saved backup descriptor file %s: %s. The new backup descriptor has been written to %s but will not be used until it is manually renamed to %s.

ID: 305

Severity: ERROR

Message: An error occurred while trying to rename the current backup descriptor file %s to %s: %s. The new backup descriptor has been written to %s but will not be used until it is manually renamed to %s.

ID: 306

Severity: ERROR

Message: An error occurred while trying to rename the new backup descriptor file %s to %s: %s. The new backup descriptor will not be used until it is manually renamed.

ID: 307

Severity: ERROR

Message: No backup directory descriptor file was found at %s.

ID: 308

Severity: ERROR

Message: The backup descriptor file %s is invalid because the first line should have contained the DN of the backend configuration entry but was blank.

ID: 309

Severity: ERROR

Message: The backup descriptor file %s is invalid because the first line of the file was "%s", but the DN of the backend configuration entry was expected.

ID: 310

Severity: ERROR

Message: An error occurred while trying to decode the value "%s" read from the first line of %s as the DN of the backend configuration entry: %s.

ID: 311

Severity: ERROR

Message: The attempt to obtain a shared lock on file %s was rejected because an exclusive lock was already held on that file.

ID: 312

Severity: ERROR

Message: The attempt to obtain a shared lock on file %s was rejected because the attempt to create the lock file failed: %s.

ID: 313

Severity: ERROR

Message: The attempt to obtain a shared lock on file %s was rejected because the attempt to open the lock file failed: %s.

ID: 314

Severity: ERROR

Message: The attempt to obtain a shared lock on file %s was rejected because an error occurred while attempting to acquire the lock: %s.

ID: 315

Severity: ERROR

Message: The shared lock requested for file %s was not granted, which indicates that another process already holds an exclusive lock on that file.

ID: 316

Severity: ERROR

Message: The attempt to obtain an exclusive lock on file %s was rejected because an exclusive lock was already held on that file.

ID: 317

Severity: ERROR

Message: The attempt to obtain an exclusive lock on file %s was rejected because a shared lock was already held on that file.

ID: 318

Severity: ERROR

Message: The attempt to obtain an exclusive lock on file %s was rejected because the attempt to create the lock file failed: %s.

ID: 319

Severity: ERROR

Message: The attempt to obtain an exclusive lock on file %s was rejected because the attempt to open the lock file failed: %s.

ID: 320

Severity: ERROR

Message: The attempt to obtain an exclusive lock on file %s was rejected because an error occurred while attempting to acquire the lock: %s.

ID: 321

Severity: ERROR

Message: The exclusive lock requested for file %s was not granted, which indicates that another process already holds a shared or exclusive lock on that file.

ID: 322

Severity: ERROR

Message: The attempt to release the exclusive lock held on %s failed: %s.

ID: 323

Severity: ERROR

Message: The attempt to release the shared lock held on %s failed: %s.

ID: 324

Severity: ERROR

Message: The attempt to release the lock held on %s failed because no record of a lock on that file was found.

ID: 343

Severity: ERROR

Message: The Directory Server could not acquire an exclusive lock on file %s: %s. This generally means that another instance of this server is already running.

ID: 346

Severity: ERROR

Message: Entry %s cannot be modified because the modification attempted to update attribute %s which is defined as NO-USER-MODIFICATION in the server schema.

ID: 347

Severity: ERROR

Message: Entry %s cannot be added because it includes attribute %s which is defined as NO-USER-MODIFICATION in the server schema.

ID: 348

Severity: ERROR

Message: Entry %s cannot be renamed because the current DN includes attribute %s which is defined as NO-USER-MODIFICATION in the server schema and the deleteOldRDN flag was set in the modify DN request.

ID: 349

Severity: ERROR

Message: Entry %s cannot be renamed because the new RDN includes attribute %s which is defined as NO-USER-MODIFICATION in the server schema, and the target value for that attribute is not already included in the entry.

ID: 356

Severity: ERROR

Message: The modify DN operation for entry %s cannot be performed because a pre-operation plugin modified the entry in a way that caused it to violate the server schema: %s.

ID: 357

Severity: ERROR

Message: Entry %s cannot be modified because the request contained an LDAP assertion control and the associated filter did not match the contents of the entry.

ID: 358

Severity: ERROR

Message: Entry %s cannot be modified because the request contained an LDAP assertion control, but an error occurred while attempting to compare the target entry against the filter contained in the control: %s.

ID: 359

Severity: ERROR

Message: Entry %s cannot be modified because the request contained a critical control with OID %s that is not supported by the Directory Server for this type of operation.

ID: 362

Severity: ERROR

Message: Entry %s cannot be removed because the request contained an LDAP assertion control and the associated filter did not match the contents of the entry.

ID: 363

Severity: ERROR

Message: Entry %s cannot be removed because the request contained an LDAP assertion control, but an error occurred while attempting to compare the target entry against the filter contained in the control: %s.

ID: 364

Severity: ERROR

Message: Entry %s cannot be removed because the request contained a critical control with OID %s that is not supported by the Directory Server for this type of operation.

ID: 365

Severity: ERROR

Message: Entry %s cannot be renamed because the request contained an LDAP assertion control and the associated filter did not match the contents of the entry.

ID: 366

Severity: ERROR

Message: Entry %s cannot be renamed because the request contained an LDAP assertion control, but an error occurred while attempting to compare the target entry against the filter contained in the control: %s.

ID: 367

Severity: ERROR

Message: Entry %s cannot be renamed because the request contained a critical control with OID %s that is not supported by the Directory Server for this type of operation.

ID: 368

Severity: ERROR

Message: Entry %s cannot be added because the request contained an LDAP assertion control and the associated filter did not match the contents of the provided entry.

ID: 369

Severity: ERROR

Message: Entry %s cannot be added because the request contained an LDAP assertion control, but an error occurred while attempting to compare the provided entry against the filter contained in the control: %s.

ID: 370

Severity: ERROR

Message: Entry %s cannot be added because the request contained a critical control with OID %s that is not supported by the Directory Server for this type of operation.

ID: 371

Severity: ERROR

Message: The search request cannot be processed because it contains an LDAP assertion control and an error occurred while trying to retrieve the base entry to compare it against the assertion filter: %s.

ID: 372

Severity: ERROR

Message: The search request cannot be processed because it contains an LDAP assertion control but the search base entry does not exist.

ID: 373

Severity: ERROR

Message: The search request cannot be processed because it contains an LDAP assertion control and the assertion filter did not match the contents of the base entry.

ID: 374

Severity: ERROR

Message: The search request cannot be processed because it contains an LDAP assertion control, but an error occurred while attempting to compare the base entry against the assertion filter: %s.

ID: 375

Severity: ERROR

Message: The search request cannot be processed because it contains a critical control with OID %s that is not supported by the Directory Server for this type of operation.

ID: 376

Severity: ERROR

Message: Cannot perform the compare operation on entry %s because the request contained an LDAP assertion control and the associated filter did not match the contents of the entry.

ID: 377

Severity: ERROR

Message: Cannot perform the compare operation on entry %s because the request contained an LDAP assertion control, but an error occurred while attempting to compare the target entry against the filter contained in that control: %s.

ID: 378

Severity: ERROR

Message: Cannot perform the compare operation on entry %s because the request contained a critical control with OID %s that is not supported by the Directory Server for this type of operation.

ID: 385

Severity: ERROR

Message: Entry %s cannot be added because it is missing attribute %s that is contained in the entry's RDN. All attributes used in the RDN must also be provided in the attribute list for the entry.

ID: 394

Severity: ERROR

Message: Unable to process the bind request because it contained a control with OID %s that was

marked critical but this control is not supported for the bind operation.

ID: 400

Severity: ERROR

Message: The entry %s cannot be added because an entry with that name already exists.

ID: 401

Severity: ERROR

Message: An error occurred during preoperation synchronization processing for the add operation with connection ID %d and operation ID %d: %s.

ID: 402

Severity: ERROR

Message: An error occurred during postoperation synchronization processing for the add operation with connection ID %d and operation ID %d: %s.

ID: 403

Severity: ERROR

Message: An error occurred during preoperation synchronization processing for the delete operation with connection ID %d and operation ID %d: %s.

ID: 404

Severity: ERROR

Message: An error occurred during postoperation synchronization processing for the delete operation with connection ID %d and operation ID %d: %s.

ID: 405

Severity: ERROR

Message: An error occurred during preoperation synchronization processing for the modify operation with connection ID %d and operation ID %d: %s.

ID: 406

Severity: ERROR

Message: An error occurred during postoperation synchronization processing for the modify operation with connection ID %d and operation ID %d: %s.

ID: 407

Severity: ERROR

Message: An error occurred during preoperation synchronization processing for the modify DN operation with connection ID %d and operation ID %d: %s.

ID: 408

Severity: ERROR

Message: An error occurred during postoperation synchronization processing for the modify DN operation with connection ID %d and operation ID %d: %s.

ID: 409

Severity: ERROR

Message: An error occurred during conflict resolution synchronization processing for the add operation with connection ID %d and operation ID %d: %s.

ID: 410

Severity: ERROR

Message: An error occurred during conflict resolution synchronization processing for the delete operation with connection ID %d and operation ID %d: %s.

ID: 411

Severity: ERROR

Message: An error occurred during conflict resolution synchronization processing for the modify operation with connection ID %d and operation ID %d: %s.

ID: 412

Severity: ERROR

Message: An error occurred during conflict resolution synchronization processing for the modify DN operation with connection ID %d and operation ID %d: %s.

ID: 413

Severity: ERROR

Message: Unable to add entry %s because the Directory Server is configured in read-only mode.

ID: 414

Severity: ERROR

Message: Unable to add entry %s because the backend that should hold that entry is configured in read-only mode.

ID: 415

Severity: ERROR

Message: Unable to delete entry %s because the Directory Server is configured in read-only mode.

ID: 416

Severity: ERROR

Message: Unable to delete entry %s because the backend that holds that entry is configured in read-only mode.

ID: 417

Severity: ERROR

Message: Unable to modify entry %s because the Directory Server is configured in read-only mode.

ID: 418

Severity: ERROR

Message: Unable to modify entry %s because the backend that holds that entry is configured in read-only mode.

ID: 419

Severity: ERROR

Message: Unable to rename entry %s because the Directory Server is configured in read-only mode.

ID: 420

Severity: ERROR

Message: Unable to rename entry %s because the backend that holds that entry is configured in read-only mode.

ID: 421

Severity: ERROR

Message: Unable to process the simple bind request because it contained a bind DN but no password, which is forbidden by the server configuration.

ID: 425

Severity: ERROR

Message: The password policy definition contained in configuration entry "%s" is invalid because the specified password attribute "%s" is not defined in the server schema.

ID: 426

Severity: ERROR

Message: The password policy definition contained in configuration entry "%s" is invalid because the specified password attribute "%s" has a syntax OID of %s. The password attribute must have a syntax OID of either 1.3.6.1.4.1.26027.1.3.1 (for the user password syntax) or 1.3.6.1.4.1.4203.1.1.2 (for the authentication password syntax).

ID: 477

Severity: ERROR

Message: An error occurred while attempting to determine the value for attribute ds-cfg-require-change-by-time in configuration entry %s: %s.

ID: 482

Severity: ERROR

Message: The password policy definition contained in configuration entry "%s" is invalid because the specified last login time format "%s" is not a valid format string The last login time format string should conform to the syntax described in the API documentation for the <CODE>java.text.SimpleDateFormat</CODE> class.

ID: 485

Severity: ERROR

Message: The password policy definition contained in configuration entry "%s" is invalid because the specified previous last login time format "%s" is not a valid format string The previous last login time format strings should conform to the syntax described in the API documentation for the <CODE>java.text.SimpleDateFormat</CODE> class.

ID: 496

Severity: ERROR

Message: Attribute options are not allowed for the password attribute %s.

ID: 497

Severity: ERROR

Message: Only a single value may be provided for the password attribute %s.

ID: 498

Severity: ERROR

Message: Pre-encoded passwords are not allowed for the password attribute %s.

ID: 499

Severity: ERROR

Message: The password value for attribute %s was found to be unacceptable: %s.

ID: 500

Severity: ERROR

Message: The password policy defined in configuration entry %s is configured to always send at least one warning notification before the password is expired, but no warning interval has been set. If configuration attribute ds-cfg-expire-passwords-without-warning is set to "false", then configuration attribute ds-cfg-password-expiration-warning-interval must have a positive value.

ID: 501

Severity: ERROR

Message: A bind operation is currently in progress on the associated client connection. No other requests may be made on this client connection until the bind processing has completed.

ID: 502

Severity: ERROR

Message: %s must change their password before it will be allowed to request any other operations.

ID: 504

Severity: ERROR

Message: An error occurred while attempting to decode the ds-pwp-password-policy-dn value "%s" in user entry "%s" as a DN: %s.

ID: 505

Severity: ERROR

Message: User entry %s is configured to use a password policy subentry of %s but no such password policy has been defined in the server configuration.

ID: 506

Severity: ERROR

Message: An error occurred while attempting to decode value "%s" for attribute %s in user entry %s in accordance with the generalized time format: %s.

ID: 507

Severity: ERROR

Message: Unable to decode value "%s" for attribute %s in user entry %s as a Boolean value.

ID: 508

Severity: ERROR

Message: The entry %s cannot be added due to insufficient access rights.

ID: 509

Severity: ERROR

Message: The user cannot bind due to insufficient access rights.

ID: 510

Severity: ERROR

Message: The entry %s cannot be compared due to insufficient access rights.

ID: 511

Severity: ERROR

Message: The entry %s cannot be deleted due to insufficient access rights.

ID: 512

Severity: ERROR

Message: The extended operation %s cannot be performed due to insufficient access rights.

ID: 513

Severity: ERROR

Message: The entry %s cannot be renamed due to insufficient access rights.

ID: 514

Severity: ERROR

Message: The entry %s cannot be modified due to insufficient access rights.

ID: 515

Severity: ERROR

Message: The entry %s cannot be searched due to insufficient access rights.

ID: 516

Severity: ERROR

Message: Rejecting a simple bind request because the password policy requires secure authentication.

ID: 517

Severity: ERROR

Message: Rejecting a bind request because the account has been administratively disabled.

ID: 518

Severity: ERROR

Message: Rejecting a bind request because the account has been locked due to too many failed authentication attempts.

ID: 519

Severity: ERROR

Message: Rejecting a bind request because the account has been locked after the user’s password was not changed in a timely manner after an administrative reset.

ID: 520

Severity: ERROR

Message: Rejecting a bind request because the account has been locked after remaining idle for too long.

ID: 521

Severity: ERROR

Message: Rejecting a bind request because that user’s password is expired.

ID: 522

Severity: ERROR

Message: An error occurred while attempting to update password policy state information for user %s: %s.

ID: 523

Severity: ERROR

Message: Rejecting a SASL %s bind request for user %s because the password policy requires secure authentication.

ID: 530

Severity: ERROR

Message: The alternate root bind DN "%s" is already registered with the Directory Server for actual root entry DN "%s".

ID: 531

Severity: ERROR

Message: Rejecting a bind request because the account has expired.

ID: 532

Severity: ERROR

Message: Attributes used to hold user passwords are not allowed to have any attribute options.

ID: 533

Severity: ERROR

Message: Users are not allowed to change their own passwords.

ID: 534

Severity: ERROR

Message: Password changes must be performed over a secure authentication channel.

ID: 535

Severity: ERROR

Message: The password cannot be changed because it has not been long enough since the last password change.

ID: 536

Severity: ERROR

Message: Multiple password values are not allowed in user entries.

ID: 537

Severity: ERROR

Message: User passwords may not be provided in pre-encoded form.

ID: 538

Severity: ERROR

Message: Invalid modification type %s attempted on password attribute %s.

ID: 539

Severity: ERROR

Message: The user entry does not have any existing passwords to remove.

ID: 541

Severity: ERROR

Message: The provided user password does not match any password in the user's entry.

ID: 542

Severity: ERROR

Message: The password policy requires that user password changes include the current password in the request.

ID: 543

Severity: ERROR

Message: The password change would result in multiple password values in the user entry, which is not allowed.

ID: 544

Severity: ERROR

Message: The provided password value was rejected by a password validator: %s.

ID: 545

Severity: ERROR

Message: %s must change their password before it will be allowed to perform any other operations.

ID: 548

Severity: ERROR

Message: The account has been locked as a result of too many failed authentication attempts (time to unlock: %s).

ID: 549

Severity: ERROR

Message: The account has been locked as a result of too many failed authentication attempts. It may only be unlocked by an administrator.

ID: 556

Severity: ERROR

Message: The specified password value already exists in the user entry.

ID: 559

Severity: ERROR

Message: Unable to add one or more values to attribute %s because at least one of the values already exists.

ID: 560

Severity: ERROR

Message: Unable to remove one or more values from attribute %s because at least one of the attributes does not exist in the entry.

ID: 561

Severity: ERROR

Message: The increment operation is not supported for the objectClass attribute.

ID: 562

Severity: ERROR

Message: Unknown modification type %s requested.

ID: 564

Severity: ERROR

Message: Unable to increment the value of attribute %s because the provided modification did not have exactly one value to use as the increment.

ID: 565

Severity: ERROR

Message: Unable to increment the value of attribute %s because either the current value or the increment could not be parsed as an integer.

ID: 566

Severity: ERROR

Message: Entry %s cannot be updated because the request did not contain any modifications.

ID: 568

Severity: ERROR

Message: Unable to increment the value of attribute %s because that attribute does not exist in the entry.

ID: 570

Severity: ERROR

Message: Unable to process the request for extended operation %s because it contained an unsupported critical control with OID %s.

ID: 571

Severity: ERROR

Message: Unable to register backend %s with the Directory Server because another backend with the same backend ID is already registered.

ID: 572

Severity: ERROR

Message: Unable to register base DN %s with the Directory Server for backend %s because that base DN is already registered for backend %s.

ID: 573

Severity: ERROR

Message: Unable to register base DN %s with the Directory Server for backend %s because that backend already contains another base DN %s that is within the same hierarchical path.

ID: 574

Severity: ERROR

Message: Unable to register base DN %s with the Directory Server for backend %s because that backend already contains another base DN %s that is not subordinate to the same base DN in the parent backend.

ID: 575

Severity: ERROR

Message: Unable to register base DN %s with the Directory Server for backend %s because that backend already contains one or more other base DNs that are subordinate to backend %s but the new base DN is not.

ID: 577

Severity: ERROR

Message: Unable to de-register base DN %s with the Directory Server because that base DN is not

registered for any active backend.

ID: 579

Severity: ERROR

Message: Unable to update the schema element with definition "%s" because a circular reference was identified when attempting to rebuild other schema elements dependent upon it.

ID: 580

Severity: ERROR

Message: Rejecting the requested operation because the connection has not been authenticated.

ID: 583

Severity: ERROR

Message: Entry %s cannot be modified because the modification attempted to set one or more new values for attribute %s which is marked OBSOLETE in the server schema.

ID: 584

Severity: ERROR

Message: Object class %s added to entry %s is marked OBSOLETE in the server schema.

ID: 585

Severity: ERROR

Message: The modify DN operation for entry %s cannot be performed because the new RDN includes attribute type %s which is declared OBSOLETE in the server schema.

ID: 586

Severity: ERROR

Message: Entry %s is invalid according to the server schema because there is no DIT structure rule that applies to that entry, but there is a DIT structure rule for the parent entry %s.

ID: 587

Severity: ERROR

Message: An unexpected error occurred while attempting to perform DIT structure rule processing for the parent of entry %s: %s.

ID: 589

Severity: ERROR

Message: You do not have sufficient privileges to reset user passwords.

ID: 590

Severity: ERROR

Message: You do not have sufficient privileges to access the server configuration.

ID: 591

Severity: ERROR

Message: You do not have sufficient privileges to add entries that include privileges.

ID: 592

Severity: ERROR

Message: You do not have sufficient privileges to modify the set of privileges contained in an entry.

ID: 595

Severity: ERROR

Message: You do not have sufficient privileges to use the proxied authorization control.

ID: 597

Severity: ERROR

Message: Entry %s violates the Directory Server schema configuration because it includes attribute %s without any values.

ID: 598

Severity: ERROR

Message: OpenDJ is configured to run as a Windows service and it cannot run in no-detach mode.

ID: 600

Severity: ERROR

Message: Unable to decode an entry because it had an unsupported entry version byte value of %s.

ID: 601

Severity: ERROR

Message: Unable to decode an entry because an unexpected exception was caught during processing: %s.

ID: 602

Severity: ERROR

Message: The provided search filter "%s" could not be decoded because the NOT filter between positions %d and %d did not contain exactly one filter component.

ID: 611

Severity: ERROR

Message: The request control with Object Identifier (OID) "%s" cannot be used due to insufficient access rights.

ID: 612

Severity: ERROR

Message: The connection handler %s is trying to use the listener %s which is already in use by another connection handler.

ID: 614

Severity: ERROR

Message: No enabled connection handler available.

ID: 615

Severity: ERROR

Message: Could not start connection handlers.

ID: 616

Severity: ERROR

Message: Unable to process the non-root bind because the server is in lockdown mode.

ID: 620

Severity: ERROR

Message: Unable to decode the provided attribute because it used an undefined attribute description token %s.

ID: 621

Severity: ERROR

Message: Unable to decode the provided object class set because it used an undefined token %s.

ID: 622

Severity: ERROR

Message: Unable to write the updated compressed schema token data: %s.

ID: 623

Severity: ERROR

Message: Unable to decode the provided entry encode configuration element because it has an invalid length.

ID: 625

Severity: ERROR

Message: Unable to create an extensible match search filter using the provided information

because it did not contain either an attribute type or a matching rule ID. At least one of these must be provided.

ID: 626

Severity: ERROR

Message: The provided search filter "%s" could not be decoded because the extensible match component starting at position %d did not contain either an attribute description or a matching rule ID. At least one of these must be provided.

ID: 627

Severity: ERROR

Message: The provided search filter "%s" could not be decoded because the extensible match component starting at position %d referenced an unknown matching rule %s.

ID: 628

Severity: ERROR

Message: Rejecting a bind request for user %s because either the entire server or the user's backend has a writability mode of 'disabled' and password policy state updates would not be allowed.

ID: 629

Severity: ERROR

Message: The provided new password was found in the password history for the user.

ID: 633

Severity: ERROR

Message: The password policy configuration entry "%s" is invalid because if a maximum password age is configured, then the password expiration warning interval must be shorter than the maximum password age.

ID: 634

Severity: ERROR

Message: The password policy configuration entry "%s" is invalid because if both a minimum password age and a maximum password age are configured, then the sum of the minimum password age and the password expiration warning interval must be shorter than the maximum password age.

ID: 638

Severity: ERROR

Message: An error occurred while attempting to disconnect client connection %d: %s.

ID: 639

Severity: ERROR

Message: An unexpected error occurred in the idle time limit thread: %s.

ID: 640

Severity: ERROR

Message: The Directory Server is currently running. Environment configuration changes are not allowed with the server running.

ID: 641

Severity: ERROR

Message: The specified server root directory '%s' is invalid. The specified path must exist and must be a directory.

ID: 642

Severity: ERROR

Message: The specified config file path '%s' is invalid. The specified path must exist and must be a file.

ID: 643

Severity: ERROR

Message: The specified config handler class '%s' is invalid. The specified class must be a subclass of the org.opends.server.api.ConfigHandler superclass.

ID: 644

Severity: ERROR

Message: The specified schema configuration directory '%s' is invalid. The specified path must exist and must be a directory.

ID: 645

Severity: ERROR

Message: The specified lock directory '%s' is invalid. The specified path must exist and must be a directory.

ID: 648

Severity: ERROR

Message: The Directory Server is currently running. The environment configuration can not be altered while the server is online.

ID: 649

Severity: ERROR

Message: An error occurred while attempting to initialize a SSL context for server to server communication: %s.

ID: 650

Severity: ERROR

Message: The ADS trust store backend %s is not enabled.

ID: 651

Severity: ERROR

Message: The backend %s is not a trust store backend.

ID: 654

Severity: ERROR

Message: An error occurred in the trust store synchronization thread: %s.

ID: 657

Severity: ERROR

Message: The password storage scheme defined in configuration entry %s does not support the auth password syntax, which is used by password attribute %s.

ID: 659

Severity: ERROR

Message: Password policy configuration entry %s references deprecated password storage scheme DN %s which does not support the auth password syntax.

ID: 661

Severity: ERROR

Message: CryptoManager cannot get the requested digest %s: %s.

ID: 662

Severity: ERROR

Message: CryptoManager cannot get the requested MAC engine %s: %s.

ID: 663

Severity: ERROR

Message: CryptoManager cannot get the requested encryption cipher %s: %s.

ID: 664

Severity: ERROR

Message: CryptoManager cannot get the preferred key wrapping cipher: %s.

ID: 665

Severity: ERROR

Message: CryptoManager failed to add entry "%s" to initiate instance key generation.

ID: 666

Severity: ERROR

Message: CryptoManager failed to retrieve entry "%s" (the instance-key-pair public-key-certificate): %s.

ID: 667

Severity: ERROR

Message: CryptoManager failed to compute an instance key identifier: %s.

ID: 668

Severity: ERROR

Message: Failed to add entry "%s".

ID: 669

Severity: ERROR

Message: CryptoManager failed to publish the instance-key-pair public-key-certificate entry in ADS: %s.

ID: 670

Severity: ERROR

Message: CryptoManager failed to retrieve the collection of instance-key-pair public-key-certificates from ADS container "%s": %s.

ID: 671

Severity: ERROR

Message: CryptoManager failed to encode symmetric key attribute value: %s.

ID: 672

Severity: ERROR

Message: CryptoManager symmetric key attribute value "%s" syntax is invalid: incorrect number of fields.

ID: 673

Severity: ERROR

Message: CryptoManager symmetric key attribute value "%s" syntax is invalid. Parsing failed in field "%s" at offset %d.

ID: 674

Severity: ERROR

Message: CryptoManager failed to retrieve the instance-key-pair private-key: %s.

ID: 675

Severity: ERROR

Message: CryptoManager failed to decipher the wrapped secret-key value: %s.

ID: 676

Severity: ERROR

Message: CryptoManager cannot find the public-key-certificate (identifier "%s") requested for symmetric key re-encoding.

ID: 677

Severity: ERROR

Message: CryptoManager failed to decode the key entry identifier "%s": %s.

ID: 678

Severity: ERROR

Message: CrytpoManager passed invalid MAC algorithm "%s": %s.

ID: 679

Severity: ERROR

Message: CryptoManager failed to initialize MAC engine: %s.

ID: 680

Severity: ERROR

Message: CryptoManager passed invalid Cipher transformation "%s": %s.

ID: 681

Severity: ERROR

Message: CryptoManager cannot initialize Cipher: %s.

ID: 682

Severity: ERROR

Message: CryptoManager failed to write the stream prologue: %s.

ID: 683

Severity: ERROR

Message: CryptoManager failed to decrypt the supplied data because it could not read the symmetric key identifier in the data prologue: %s.

ID: 684

Severity: ERROR

Message: CryptoManager failed to decrypt the supplied data because the symmetric key identifier in the data prologue does not match any known key entries.

ID: 685

Severity: ERROR

Message: CryptoManager failed to decrypt the supplied data because it could not read the cipher initialization vector in the data prologue.

ID: 686

Severity: ERROR

Message: CryptoManager failed to decrypt the supplied data because there was an error reading from the input stream: %s.

ID: 687

Severity: ERROR

Message: CryptoManager failed to import the symmetric key entry "%s" because it could not obtain a symmetric key attribute value that can be decoded by this instance.

ID: 688

Severity: ERROR

Message: CryptoManager detected a field mismatch between the key entry to be imported and an entry in the key cache that share the key identifier "%s".

ID: 689

Severity: ERROR

Message: CryptoManager failed to import the symmetric key entry "%s": %s.

ID: 690

Severity: ERROR

Message: CryptoManager failed to import the symmetric key entry "%s" because it could not add a symmetric key attribute value that can be decoded by this instance.

ID: 691

Severity: ERROR

Message: CryptoManager failed to instantiate a KeyGenerator for algorithm "%s": %s.

ID: 692

Severity: ERROR

Message: CryptoManager failed to add locally produced symmetric key entry "%s": %s.

ID: 693

Severity: ERROR

Message: CryptoManager cipher transformation specification "%s" is invalid: it must be of the form "algorithm/mode/padding".

ID: 694

Severity: ERROR

Message: CryptoManager cipher transformation specification "%s" is invalid: it must be of the form "algorithm/mode/padding".

ID: 695

Severity: ERROR

Message: CryptoManager failed to decrypt the supplied data because it could not read the version number in the data prologue: %s.

ID: 696

Severity: ERROR

Message: CryptoManager failed to decrypt the supplied data because the version "%d" in the data prologue is unknown.

ID: 697

Severity: ERROR

Message: The provided entry %s cannot be added because its suffix is not defined as one of the suffixes within the Directory Server.

ID: 700

Severity: ERROR

Message: Start TLS extended operations cannot be canceled.

ID: 701

Severity: ERROR

Message: Cancel extended operations can not be canceled.

ID: 702

Severity: ERROR

Message: The modify DN operation for entry %s cannot be performed because the new superior entry %s is equal to or a subordinate of the entry to be moved.

ID: 703

Severity: ERROR

Message: Unable to register workflow element %s with the Directory Server because another

workflow element with the same ID is already registered.

ID: 715

Severity: ERROR

Message: Entry %s can not be added because BER encoding of %s attribute is not supported.

ID: 721

Severity: ERROR

Message: The CryptoManager entry "%s" (the instance-key-pair public-key-certificate) does not contain a public-key certificate.

ID: 723

Severity: ERROR

Message: In no-detach mode, the 'timeout' option cannot be used.

ID: 726

Severity: ERROR

Message: The entry %s does not contain the pwdPolicy objectclass, which is required for Directory Server password policy.

ID: 727

Severity: ERROR

Message: Unable to decode the provided string "%s" as a relative distinguished name because it does not contain a value for attribute type %s.

ID: 728

Severity: ERROR

Message: CryptoManager failed to initialize because the specified cipher key length "%d" is beyond the allowed cryptography strength "%d" in jurisdiction policy files.

ID: 729

Severity: ERROR

Message: Failed to update free disk space for directory %s: %s.

ID: 730

Severity: ERROR

Message: The directory server is not accepting a new persistent search request because the server has already reached its limit.

ID: 739

Severity: ERROR

Message: This operation involves LDAP subentries which you do not have sufficient privileges to administer.

ID: 743

Severity: ERROR

Message: When attempting to modify entry %s, one value for attribute %s was found to be invalid according to the associated syntax: %s.

ID: 744

Severity: ERROR

Message: When attempting to modify entry %s to replace the set of values for attribute %s, one value was found to be invalid according to the associated syntax: %s.

ID: 745

Severity: ERROR

Message: The password policy definition contained in configuration entry "%s" is invalid because the password validator "%s" specified in attribute "%s" cannot be found.

ID: 746

Severity: ERROR

Message: The password could not be validated because of misconfiguration. Please contact the administrator.

ID: 747

Severity: ERROR

Message: The password for user %s could not be validated because the password policy subentry %s is referring to an unknown password validator (%s). Please make sure the password policy subentry only refers to validators that exist on all replicas.

ID: 748

Severity: ERROR

Message: Could not get filesystem for directory %s: %s.

ID: 749

Severity: ERROR

Message: The disk containing directory %s used by %s is low on free space (%d bytes free). Write operations are only permitted by a user with the BYPASS_LOCKDOWN privilege until the free space rises above the threshold. Replication updates are still allowed.

ID: 750

Severity: ERROR

Message: The disk containing directory %s used by %s is full (%d bytes free). Write operations to

the backend, replication updates included, will fail until the free space rises above the threshold.

ID: 752

Severity: ERROR

Message: A StartTLS operation is currently in progress on the associated client connection. No other requests may be made on this client connection until the StartTLS processing has completed.

ID: 753

Severity: ERROR

Message: A SASL bind operation is currently in progress on the associated client connection. No other requests may be made on this client connection until the SASL bind processing has completed.

ID: 754

Severity: ERROR

Message: Cannot properly use SHA-1 using the java provider. Verify java.security is properly configured.

ID: 755

Severity: ERROR

Message: Cannot complete initialization of server's backends because the root and administrative backends have not been initialized yet.

Log Message Category: EXTENSION

ID: 1

Severity: ERROR

Message: An error occurred while attempting to initialize the message digest generator for the %s algorithm: %s.

ID: 2

Severity: ERROR

Message: An error occurred while attempting to base64-decode the password value %s: %s.

ID: 3

Severity: ERROR

Message: The %s password storage scheme is not reversible, so it is impossible to recover the plaintext version of an encoded password.

ID: 4

Severity: ERROR

Message: An error occurred while trying to register the JMX alert handler with the MBean server: %s.

ID: 5

Severity: ERROR

Message: An unexpected error occurred while attempting to encode a password using the storage scheme defined in class %s: %s.

ID: 6

Severity: ERROR

Message: The ds-cfg-include-filter attribute of configuration entry %s, which specifies a set of search filters that may be used to control which entries are included in the cache, has an invalid value of "%s": %s.

ID: 7

Severity: ERROR

Message: The ds-cfg-exclude-filter attribute of configuration entry %s, which specifies a set of search filters that may be used to control which entries are excluded from the cache, has an invalid value of "%s": %s.

ID: 8

Severity: ERROR

Message: A fatal error occurred while trying to initialize fifo entry cache: %s.

ID: 9

Severity: ERROR

Message: A fatal error occurred while trying to initialize soft reference entry cache: %s.

ID: 33

Severity: ERROR

Message: An unexpected error occurred while attempting to decode the password modify extended request sequence: %s.

ID: 34

Severity: ERROR

Message: The password modify extended request cannot be processed because it does not contain an authorization ID and the underlying connection is not authenticated.

ID: 35

Severity: ERROR

Message: The password modify extended request cannot be processed because the server was unable to obtain a write lock on user entry %s after multiple attempts.

ID: 36

Severity: ERROR

Message: The password modify extended request cannot be processed because the server cannot decode "%s" as a valid DN for use in the authorization ID for the operation.

ID: 37

Severity: ERROR

Message: The password modify extended request cannot be processed because it contained an invalid userIdentity field. The provided userIdentity string was "%s".

ID: 38

Severity: ERROR

Message: The password modify extended request cannot be processed because it was not possible to identify the user entry to update based on the authorization DN of "%s".

ID: 41

Severity: ERROR

Message: The password modify extended operation cannot be processed because the current password provided for the user is invalid.

ID: 45

Severity: ERROR

Message: The keystore file %s specified in attribute ds-cfg-key-store-file of configuration entry %s does not exist.

ID: 46

Severity: ERROR

Message: An unexpected error occurred while trying to determine the value of configuration attribute ds-cfg-key-store-file in configuration entry %s: %s.

ID: 50

Severity: ERROR

Message: Java property %s which is specified in attribute ds-cfg-key-store-pin-property of configuration entry %s should contain the PIN needed to access the file-based key manager, but this property is not set.

ID: 53

Severity: ERROR

Message: Environment variable %s which is specified in attribute ds-cfg-key-store-pin-environment-variable of configuration entry %s should contain the PIN needed to access the file-based key manager, but this property is not set.

ID: 56

Severity: ERROR

Message: File %s specified in attribute ds-cfg-key-store-pin-file of configuration entry %s should contain the PIN needed to access the file-based key manager, but this file does not exist.

ID: 57

Severity: ERROR

Message: An error occurred while trying to read the keystore PIN from file %s specified in configuration attribute ds-cfg-key-store-pin-file of configuration entry %s: %s.

ID: 58

Severity: ERROR

Message: File %s specified in attribute ds-cfg-key-store-pin-file of configuration entry %s should contain the PIN needed to access the file-based key manager, but this file is empty.

ID: 62

Severity: ERROR

Message: An error occurred while trying to load the keystore contents from file %s: %s.

ID: 63

Severity: ERROR

Message: The keystore type %s specified in attribute ds-cfg-key-store-type of configuration entry %s is not valid: %s.

ID: 68

Severity: ERROR

Message: Java property %s which is specified in attribute ds-cfg-key-store-pin-property of configuration entry %s should contain the PIN needed to access the PKCS#11 key manager, but this property is not set.

ID: 71

Severity: ERROR

Message: Environment variable %s which is specified in attribute ds-cfg-key-store-pin-environment-variable of configuration entry %s should contain the PIN needed to access the PKCS#11 key manager, but this property is not set.

ID: 74

Severity: ERROR

Message: File %s specified in attribute ds-cfg-key-store-pin-file of configuration entry %s should contain the PIN needed to access the PKCS#11 key manager, but this file does not exist.

ID: 75

Severity: ERROR

Message: An error occurred while trying to read the keystore PIN from file %s specified in configuration attribute ds-cfg-key-store-pin-file of configuration entry %s: %s.

ID: 76

Severity: ERROR

Message: File %s specified in attribute ds-cfg-key-store-pin-file of configuration entry %s should contain the PIN needed to access the PKCS#11 key manager, but this file is empty.

ID: 79

Severity: ERROR

Message: An unexpected error occurred while trying to determine the value of configuration attribute ds-cfg-key-store-pin in configuration entry %s: %s.

ID: 81

Severity: ERROR

Message: An error occurred while trying to access the PKCS#11 key manager: %s.

ID: 83

Severity: ERROR

Message: An error occurred while trying to create a key manager factory to access the contents of keystore file %s: %s.

ID: 84

Severity: ERROR

Message: An error occurred while trying to create a key manager factory to access the contents of the PKCS#11 keystore: %s.

ID: 87

Severity: ERROR

Message: The trust store file %s specified in attribute ds-cfg-trust-store-file of configuration entry %s does not exist.

ID: 88

Severity: ERROR

Message: An unexpected error occurred while trying to determine the value of configuration attribute ds-cfg-trust-store-file in configuration entry %s: %s.

ID: 92

Severity: ERROR

Message: Java property %s which is specified in attribute ds-cfg-trust-store-pin-property of configuration entry %s should contain the PIN needed to access the file-based trust manager, but this property is not set.

ID: 95

Severity: ERROR

Message: Environment variable %s which is specified in attribute ds-cfg-trust-store-pin-environment-variable of configuration entry %s should contain the PIN needed to access the file-based trust manager, but this property is not set.

ID: 98

Severity: ERROR

Message: File %s specified in attribute ds-cfg-trust-store-pin-file of configuration entry %s should contain the PIN needed to access the file-based trust manager, but this file does not exist.

ID: 99

Severity: ERROR

Message: An error occurred while trying to read the trust store PIN from file %s specified in configuration attribute ds-cfg-trust-store-pin-file of configuration entry %s: %s.

ID: 100

Severity: ERROR

Message: File %s specified in attribute ds-cfg-trust-store-pin-file of configuration entry %s should contain the PIN needed to access the file-based trust manager, but this file is empty.

ID: 104

Severity: ERROR

Message: An error occurred while trying to load the trust store contents from file %s: %s.

ID: 105

Severity: ERROR

Message: An error occurred while trying to create a trust manager factory to access the contents of trust store file %s: %s.

ID: 106

Severity: ERROR

Message: The trust store type %s specified in attribute ds-cfg-trust-store-type of configuration entry %s is not valid: %s.

ID: 118

Severity: ERROR

Message: Could not map the provided certificate chain to a user entry because no peer certificate

was available.

ID: 119

Severity: ERROR

Message: Could not map the provided certificate chain to a user because the peer certificate was not an X.509 certificate (peer certificate format was %s).

ID: 120

Severity: ERROR

Message: Could not map the provided certificate chain to a user because the peer certificate subject "%s" could not be decoded as an LDAP DN: %s.

ID: 121

Severity: ERROR

Message: Could not map the provided certificate chain to a user because an error occurred while attempting to retrieve the user entry with DN "%s": %s.

ID: 122

Severity: ERROR

Message: Could not map the provided certificate chain to a user because no user entry exists with a DN of %s.

ID: 123

Severity: ERROR

Message: The SASL EXTERNAL bind request could not be processed because the associated bind request does not have a reference to the client connection.

ID: 124

Severity: ERROR

Message: The SASL EXTERNAL bind request could not be processed because the associated client connection instance is not an instance of LDAPClientConnection.

ID: 126

Severity: ERROR

Message: The SASL EXTERNAL bind request could not be processed because the client did not present a certificate chain during SSL/TLS negotiation.

ID: 127

Severity: ERROR

Message: The SASL EXTERNAL bind request failed because the certificate chain presented by the client during SSL/TLS negotiation could not be mapped to a user entry in the Directory Server.

ID: 128

Severity: ERROR

Message: StartTLS cannot be used on this connection because the underlying client connection is not available.

ID: 129

Severity: ERROR

Message: StartTLS cannot be used on this client connection because this connection type is not capable of using StartTLS to protect its communication.

ID: 137

Severity: ERROR

Message: Unable to authenticate via SASL EXTERNAL because the mapped user entry %s does not have any certificates with which to verify the presented peer certificate.

ID: 138

Severity: ERROR

Message: Unable to authenticate via SASL EXTERNAL because the mapped user entry %s did not contain the peer certificate presented by the client.

ID: 139

Severity: ERROR

Message: An error occurred while attempting to validate the peer certificate presented by the client with a certificate from the user's entry %s: %s.

ID: 147

Severity: ERROR

Message: SASL PLAIN authentication requires that SASL credentials be provided but none were included in the bind request.

ID: 148

Severity: ERROR

Message: The SASL PLAIN bind request did not include any NULL characters. NULL characters are required as delimiters between the authorization ID and authentication ID, and also between the authentication ID and the password.

ID: 149

Severity: ERROR

Message: The SASL PLAIN bind request did not include a second NULL character in the credentials, which is required as a delimiter between the authentication ID and the password.

ID: 150

Severity: ERROR

Message: The authentication ID contained in the SASL PLAIN bind request had a length of zero characters, which is not allowed. SASL PLAIN authentication does not allow an empty string for use as the authentication ID.

ID: 151

Severity: ERROR

Message: The password contained in the SASL PLAIN bind request had a length of zero characters, which is not allowed. SASL PLAIN authentication does not allow an empty string for use as the password.

ID: 152

Severity: ERROR

Message: An error occurred while attempting to decode the SASL PLAIN authentication ID "%s" because it appeared to contain a DN but DN decoding failed: %s.

ID: 153

Severity: ERROR

Message: The authentication ID in the SASL PLAIN bind request appears to be an empty DN. This is not allowed.

ID: 154

Severity: ERROR

Message: An error occurred while attempting to retrieve user entry %s as specified in the DN-based authentication ID of a SASL PLAIN bind request: %s.

ID: 157

Severity: ERROR

Message: The server was not able to find any user entries for the provided authentication ID of %s.

ID: 160

Severity: ERROR

Message: The provided password is invalid.

ID: 166

Severity: ERROR

Message: An unexpected error occurred while attempting to obtain an MD5 digest engine for use by the CRAM-MD5 SASL handler: %s.

ID: 172

Severity: ERROR

Message: The SASL CRAM-MD5 bind request contained SASL credentials but there is no stored challenge for this client connection. The first CRAM-MD5 bind request in the two-stage process must not contain client SASL credentials.

ID: 173

Severity: ERROR

Message: The SASL CRAM-MD5 bind request contained SASL credentials, but the stored SASL state information for this client connection is not in an appropriate form for the challenge.

ID: 174

Severity: ERROR

Message: The SASL CRAM-MD5 bind request from the client included SASL credentials but there was no space to separate the username from the authentication digest.

ID: 175

Severity: ERROR

Message: The SASL CRAM-MD5 bind request included SASL credentials, but the decoded digest string had an invalid length of %d bytes rather than the %d bytes expected for a hex representation of an MD5 digest.

ID: 176

Severity: ERROR

Message: The SASL CRAM-MD5 bind request included SASL credentials, but the decoded digest was not comprised of only hexadecimal digits: %s.

ID: 177

Severity: ERROR

Message: An error occurred while attempting to decode the SASL CRAM-MD5 username "%s" because it appeared to contain a DN but DN decoding failed: %s.

ID: 178

Severity: ERROR

Message: The username in the SASL CRAM-MD5 bind request appears to be an empty DN. This is not allowed.

ID: 180

Severity: ERROR

Message: An error occurred while attempting to retrieve user entry %s as specified in the DN-based username of a SASL CRAM-MD5 bind request: %s.

ID: 184

Severity: ERROR

Message: The server was not able to find any user entries for the provided username of %s.

ID: 188

Severity: ERROR

Message: The provided password is invalid.

ID: 189

Severity: ERROR

Message: SASL CRAM-MD5 authentication is not possible for user %s because none of the passwords in the user entry are stored in a reversible form.

ID: 193

Severity: ERROR

Message: The client connection included %s state information, indicating that the client was in the process of performing a %s bind, but the bind request did not include any credentials.

ID: 194

Severity: ERROR

Message: An unexpected error occurred while attempting to determine the value of the ds-cfg-server-fqdn attribute in configuration entry %s: %s.

ID: 195

Severity: ERROR

Message: An unexpected error occurred while trying to create an %s context: %s.

ID: 196

Severity: ERROR

Message: An error occurred while attempting to decode the SASL %s username "%s" because it appeared to contain a DN but DN decoding failed: %s.

ID: 197

Severity: ERROR

Message: The username in the SASL %s bind request appears to be an empty DN. This is not allowed.

ID: 199

Severity: ERROR

Message: An error occurred while attempting to retrieve user entry %s as specified in the DN-based username of a SASL %s bind request: %s.

ID: 200

Severity: ERROR

Message: The username contained in the SASL %s bind request had a length of zero characters, which is not allowed. %s authentication does not allow an empty string for use as the username.

ID: 201

Severity: ERROR

Message: The server was not able to find any user entries for the provided username of %s.

ID: 202

Severity: ERROR

Message: The provided authorization ID %s contained an invalid DN: %s.

ID: 203

Severity: ERROR

Message: The entry %s specified as the authorization identity does not exist.

ID: 204

Severity: ERROR

Message: The entry %s specified as the authorization identity could not be retrieved: %s.

ID: 205

Severity: ERROR

Message: The server was unable to find any entry corresponding to authorization ID %s.

ID: 207

Severity: ERROR

Message: An error occurred while attempting to retrieve the clear-text password(s) for user %s in order to perform SASL %s authentication: %s.

ID: 208

Severity: ERROR

Message: SASL %s authentication is not possible for user %s because none of the passwords in the user entry are stored in a reversible form.

ID: 209

Severity: ERROR

Message: SASL %s protocol error: %s.

ID: 210

Severity: ERROR

Message: The authenticating user %s does not have sufficient privileges to assume a different authorization identity.

ID: 211

Severity: ERROR

Message: The authenticating user %s does not have sufficient access to assume a different authorization identity.

ID: 212

Severity: ERROR

Message: The server was unable to find any entry corresponding to authentication ID %s.

ID: 213

Severity: ERROR

Message: The server was unable to because both the ds-cfg-kdc-address and ds-cfg-realm attributes must be defined or neither defined.

ID: 214

Severity: ERROR

Message: An error occurred while attempting to map authorization ID %s to a user entry: %s.

ID: 215

Severity: ERROR

Message: An error occurred while attempting to write a temporary JAAS configuration file for use during GSSAPI processing: %s.

ID: 216

Severity: ERROR

Message: An error occurred while attempting to create the JAAS login context for GSSAPI authentication: %s.

ID: 217

Severity: ERROR

Message: No client connection was available for use in processing the GSSAPI bind request.

ID: 277

Severity: ERROR

Message: You do not have sufficient privileges to use the proxied authorization control.

ID: 306

Severity: ERROR

Message: ID string %s mapped to multiple users.

ID: 307

Severity: ERROR

Message: The internal search based on ID string %s could not be processed efficiently: %s. Check the server configuration to ensure that all associated backends are properly configured for these types of searches.

ID: 308

Severity: ERROR

Message: An internal failure occurred while attempting to resolve ID string %s to a user entry: %s.

ID: 313

Severity: ERROR

Message: An error occurred while attempting to map username %s to a Directory Server entry: %s.

ID: 319

Severity: ERROR

Message: An error occurred while attempting to map username %s to a Directory Server entry: %s.

ID: 325

Severity: ERROR

Message: An error occurred while attempting to map username %s to a Directory Server entry: %s.

ID: 327

Severity: ERROR

Message: Unable to process the cancel request because the extended operation did not include a request value.

ID: 328

Severity: ERROR

Message: An error occurred while attempting to decode the value of the cancel extended request: %s.

ID: 330

Severity: ERROR

Message: Password storage scheme %s does not support use with the authentication password attribute syntax.

ID: 335

Severity: ERROR

Message: The configured minimum password length of %d characters is greater than the configured maximum password length of %d.

ID: 336

Severity: ERROR

Message: The provided password is shorter than the minimum required length of %d characters.

ID: 337

Severity: ERROR

Message: The provided password is longer than the maximum allowed length of %d characters.

ID: 341

Severity: ERROR

Message: Configuration entry "%s" does not contain attribute ds-cfg-password-character-set which specifies the sets of characters that should be used when generating the password. This is a required attribute.

ID: 342

Severity: ERROR

Message: Configuration entry "%s" contains multiple definitions for the %s character set.

ID: 343

Severity: ERROR

Message: An error occurred while attempting to decode the value(s) of the configuration attribute ds-cfg-password-character-set, which is used to hold the character set(s) for use in generating the password: %s.

ID: 346

Severity: ERROR

Message: The password format string "%s" references an undefined character set "%s".

ID: 347

Severity: ERROR

Message: The password format string "%s" contains an invalid syntax. This value should be a comma-delimited sequence of elements, where each element is the name of a character set followed by a colon and the number of characters to choose at random from that character set.

ID: 348

Severity: ERROR

Message: An error occurred while attempting to decode the value for configuration attribute ds-cfg-password-format, which is used to specify the format for the generated passwords: %s.

ID: 354

Severity: ERROR

Message: An error occurred while attempting to get the password policy for user %s: %s.

ID: 355

Severity: ERROR

Message: The current password must be provided for self password changes.

ID: 356

Severity: ERROR

Message: Password modify operations that supply the user's current password must be performed over a secure communication channel.

ID: 357

Severity: ERROR

Message: End users are not allowed to change their passwords.

ID: 358

Severity: ERROR

Message: Password changes must be performed over a secure communication channel.

ID: 359

Severity: ERROR

Message: The password cannot be changed because the previous password change was too recent.

ID: 360

Severity: ERROR

Message: The password cannot be changed because it is expired.

ID: 361

Severity: ERROR

Message: No new password was provided, and no password generator has been defined that may be used to automatically create a new password.

ID: 362

Severity: ERROR

Message: An error occurred while attempting to create a new password using the password

generator: %s.

ID: 363

Severity: ERROR

Message: The password policy does not allow users to supply pre-encoded passwords.

ID: 364

Severity: ERROR

Message: The provided new password failed the validation checks defined in the server: %s.

ID: 365

Severity: ERROR

Message: Unable to encode the provided password using the default scheme(s): %s.

ID: 368

Severity: ERROR

Message: The identity mapper with configuration entry DN %s as specified for use with the password modify extended operation defined in entry %s either does not exist or is not enabled. The identity mapper is a required component, and the password modify extended operation will not be enabled.

ID: 369

Severity: ERROR

Message: An error occurred while attempting to determine the identity mapper to use in conjunction with the password modify extended operation defined in configuration entry %s: %s. The password modify extended operation will not be enabled for use in the server.

ID: 370

Severity: ERROR

Message: The provided authorization ID string "%s" could not be mapped to any user in the directory.

ID: 371

Severity: ERROR

Message: An error occurred while attempting to map authorization ID string "%s" to a user entry: %s.

ID: 377

Severity: ERROR

Message: An error occurred while attempting to retrieve the clear-text password(s) for user %s in order to perform SASL CRAM-MD5 authentication: %s.

ID: 378

Severity: ERROR

Message: An error occurred while attempting to verify the password for user %s during SASL PLAIN authentication: %s.

ID: 381

Severity: ERROR

Message: The user account has been administratively disabled.

ID: 382

Severity: ERROR

Message: The user account is locked.

ID: 383

Severity: ERROR

Message: Unable to examine entry %s as a potential member of static group %s because that entry does not exist in the Directory Server.

ID: 384

Severity: ERROR

Message: An error occurred while attempting to retrieve entry %s as a potential member of static group %s: %s.

ID: 385

Severity: ERROR

Message: Entry %s cannot be parsed as a valid static group because static groups are not allowed to have both the %s and %s object classes.

ID: 386

Severity: ERROR

Message: Entry %s cannot be parsed as a valid static group because it does not contain exactly one of the %s or the %s object classes.

ID: 387

Severity: ERROR

Message: Value %s for attribute %s in entry %s cannot be parsed as a valid DN: %s. It will be excluded from the set of group members.

ID: 388

Severity: ERROR

Message: Cannot add user %s as a new member of static group %s because that user is already in

the member list for the group.

ID: 389

Severity: ERROR

Message: Cannot remove user %s as a member of static group %s because that user is not included in the member list for the group.

ID: 390

Severity: ERROR

Message: Cannot add user %s as a new member of static group %s because an error occurred while attempting to perform an internal modification to update the group: %s.

ID: 391

Severity: ERROR

Message: Cannot remove user %s as a member of static group %s because an error occurred while attempting to perform an internal modification to update the group: %s.

ID: 392

Severity: ERROR

Message: You do not have sufficient privileges to perform password reset operations.

ID: 393

Severity: ERROR

Message: The provided authorization ID was empty, which is not allowed for DIGEST-MD5 authentication.

ID: 400

Severity: ERROR

Message: The provided authorization ID %s contained an invalid DN: %s.

ID: 401

Severity: ERROR

Message: The authenticating user %s does not have sufficient privileges to specify an alternate authorization ID.

ID: 402

Severity: ERROR

Message: The entry corresponding to authorization DN %s does not exist in the Directory Server.

ID: 403

Severity: ERROR

Message: An error occurred while attempting to retrieve entry %s specified as the authorization ID: %s.

ID: 404

Severity: ERROR

Message: No entry corresponding to authorization ID %s was found in the server.

ID: 405

Severity: ERROR

Message: An error occurred while attempting to map authorization ID %s to a user entry: %s.

ID: 417

Severity: ERROR

Message: Could not map the provided certificate chain to a user entry because no peer certificate was available.

ID: 418

Severity: ERROR

Message: Could not map the provided certificate chain to a user because the peer certificate was not an X.509 certificate (peer certificate format was %s).

ID: 419

Severity: ERROR

Message: The certificate with subject %s could not be mapped to exactly one user. It maps to both %s and %s.

ID: 422

Severity: ERROR

Message: Configuration entry %s has value '%s' which violates the format required for attribute mappings. The expected format is 'certattr:userattr'.

ID: 423

Severity: ERROR

Message: Configuration entry %s contains multiple mappings for certificate attribute %s.

ID: 424

Severity: ERROR

Message: Mapping %s in configuration entry %s references attribute %s which is not defined in the server schema.

ID: 425

Severity: ERROR

Message: Configuration entry %s contains multiple mappings for user attribute %s.

ID: 429

Severity: ERROR

Message: Could not map the provided certificate chain to a user entry because no peer certificate was available.

ID: 430

Severity: ERROR

Message: Could not map the provided certificate chain to a user because the peer certificate was not an X.509 certificate (peer certificate format was %s).

ID: 431

Severity: ERROR

Message: Unable to decode peer certificate subject %s as a DN: %s.

ID: 432

Severity: ERROR

Message: Peer certificate subject %s does not contain any attributes for which a mapping has been established.

ID: 433

Severity: ERROR

Message: The certificate with subject %s could not be mapped to exactly one user. It maps to both %s and %s.

ID: 443

Severity: ERROR

Message: Could not map the provided certificate chain to a user entry because no peer certificate was available.

ID: 444

Severity: ERROR

Message: Could not map the provided certificate chain to a user because the peer certificate was not an X.509 certificate (peer certificate format was %s).

ID: 445

Severity: ERROR

Message: An error occurred while attempting to calculate the fingerprint for the peer certificate with subject %s: %s.

ID: 446

Severity: ERROR

Message: The certificate with fingerprint %s could not be mapped to exactly one user. It maps to both %s and %s.

ID: 447

Severity: ERROR

Message: Unable to decode value "%s" in entry "%s" as an LDAP URL: %s.

ID: 448

Severity: ERROR

Message: Dynamic groups do not support nested groups.

ID: 449

Severity: ERROR

Message: Dynamic groups do not support explicitly altering their membership.

ID: 451

Severity: ERROR

Message: An error occurred while attempting perform an internal search with base DN %s and filter %s to resolve the member list for dynamic group %s: result code %s, error message %s.

ID: 452

Severity: ERROR

Message: The server encountered a timeout while attempting to add user %s to the member list for dynamic group %s.

ID: 456

Severity: ERROR

Message: The provided password differs less than the minimum required difference of %d characters.

ID: 457

Severity: ERROR

Message: The provided password contained too many instances of the same character appearing consecutively. The maximum number of times the same character may appear consecutively in a password is %d.

ID: 458

Severity: ERROR

Message: The provided password does not contain enough unique characters. The minimum

number of unique characters that may appear in a user password is %d.

ID: 459

Severity: ERROR

Message: The %s attribute is not searchable and should not be included in otherwise unindexed search filters.

ID: 460

Severity: ERROR

Message: The provided password contained a word from the server's dictionary.

ID: 461

Severity: ERROR

Message: The specified dictionary file %s does not exist.

ID: 462

Severity: ERROR

Message: An error occurred while attempting to load the dictionary from file %s: %s.

ID: 463

Severity: ERROR

Message: The provided password was found in another attribute in the user entry.

ID: 464

Severity: ERROR

Message: The provided password contained character '%s' which is not allowed for use in passwords.

ID: 465

Severity: ERROR

Message: The provided password did not contain enough characters from the character set '%s'. The minimum number of characters from that set that must be present in user passwords is %d.

ID: 466

Severity: ERROR

Message: The provided character set definition '%s' is invalid because it does not contain a colon to separate the minimum count from the character set.

ID: 467

Severity: ERROR

Message: The provided character set definition '%s' is invalid because the provided character set

is empty.

ID: 468

Severity: ERROR

Message: The provided character set definition '%s' is invalid because the value before the colon must be an integer greater or equal to zero.

ID: 469

Severity: ERROR

Message: The provided character set definition '%s' is invalid because it contains character '%s' which has already been used.

ID: 470

Severity: ERROR

Message: The virtual static group defined in entry %s contains multiple target group DNs, but only one is allowed.

ID: 471

Severity: ERROR

Message: Unable to decode "%s" as the target DN for group %s: %s.

ID: 472

Severity: ERROR

Message: The virtual static group defined in entry %s does not contain a target group definition.

ID: 473

Severity: ERROR

Message: Virtual static groups do not support nesting.

ID: 474

Severity: ERROR

Message: Target group %s referenced by virtual static group %s does not exist.

ID: 475

Severity: ERROR

Message: Altering membership for virtual static group %s is not allowed.

ID: 476

Severity: ERROR

Message: Virtual static group %s references target group %s which is itself a virtual static group. One virtual static group is not allowed to reference another as its target group.

ID: 501

Severity: ERROR

Message: The %s attribute is not searchable and should not be included in otherwise unindexed search filters.

ID: 502

Severity: ERROR

Message: You do not have sufficient privileges to use the password policy state extended operation.

ID: 503

Severity: ERROR

Message: The provided password policy state extended request did not include a request value.

ID: 504

Severity: ERROR

Message: An unexpected error occurred while attempting to decode password policy state extended request value: %s.

ID: 505

Severity: ERROR

Message: Multiple entries were found with DN %s.

ID: 506

Severity: ERROR

Message: An unexpected error occurred while attempting to decode an operation from the password policy state extended request: %s.

ID: 507

Severity: ERROR

Message: No value was provided for the password policy state operation intended to set the disabled state for the user. Exactly one value (either 'true' or 'false') must be given.

ID: 508

Severity: ERROR

Message: Multiple values were provided for the password policy state operation intended to set the disabled state for the user. Exactly one value (either 'true' or 'false') must be given.

ID: 509

Severity: ERROR

Message: The value provided for the password policy state operation intended to set the disabled

state for the user was invalid. The value must be either 'true' or 'false'.

ID: 510

Severity: ERROR

Message: Multiple values were provided for the password policy state operation intended to set the account expiration time for the user. Exactly one value must be given.

ID: 511

Severity: ERROR

Message: The value %s provided for the password policy state operation used to set the account expiration time was invalid: %s. The value should be specified using the generalized time format.

ID: 512

Severity: ERROR

Message: Multiple values were provided for the password policy state operation intended to set the password changed time for the user. Exactly one value must be given.

ID: 513

Severity: ERROR

Message: The value %s provided for the password policy state operation used to set the password changed time was invalid: %s. The value should be specified using the generalized time format.

ID: 514

Severity: ERROR

Message: Multiple values were provided for the password policy state operation intended to set the password warned time for the user. Exactly one value must be given.

ID: 515

Severity: ERROR

Message: The value %s provided for the password policy state operation used to set the password warned time was invalid: %s. The value should be specified using the generalized time format.

ID: 516

Severity: ERROR

Message: Multiple values were provided for the password policy state operation intended to add an authentication failure time for the user. Exactly one value must be given.

ID: 517

Severity: ERROR

Message: The value %s provided for the password policy state operation used to update the authentication failure times was invalid: %s. The value should be specified using the generalized time format.

ID: 518

Severity: ERROR

Message: Multiple values were provided for the password policy state operation intended to set the last login time for the user. Exactly one value must be given.

ID: 519

Severity: ERROR

Message: The value %s provided for the password policy state operation used to set the last login time was invalid: %s. The value should be specified using the generalized time format.

ID: 520

Severity: ERROR

Message: No value was provided for the password policy state operation intended to set the reset state for the user. Exactly one value (either 'true' or 'false') must be given.

ID: 521

Severity: ERROR

Message: Multiple values were provided for the password policy state operation intended to set the reset state for the user. Exactly one value (either 'true' or 'false') must be given.

ID: 522

Severity: ERROR

Message: The value provided for the password policy state operation intended to set the reset state for the user was invalid. The value must be either 'true' or 'false'.

ID: 523

Severity: ERROR

Message: Multiple values were provided for the password policy state operation intended to add a grace login use time for the user. Exactly one value must be given.

ID: 524

Severity: ERROR

Message: The value %s provided for the password policy state operation used to update the grace login use times was invalid: %s. The value should be specified using the generalized time format.

ID: 525

Severity: ERROR

Message: Multiple values were provided for the password policy state operation intended to set the required change time for the user. Exactly one value must be given.

ID: 526

Severity: ERROR

Message: The value %s provided for the password policy state operation used to set the required change time was invalid: %s. The value should be specified using the generalized time format.

ID: 527

Severity: ERROR

Message: The password policy state extended request included an operation with an invalid or unsupported operation type of %s.

ID: 530

Severity: ERROR

Message: The provided new password was already contained in the password history.

ID: 531

Severity: ERROR

Message: The Directory Server is not configured with any SMTP servers. The SMTP alert handler cannot be used unless the Directory Server is configured with information about at least one SMTP server.

ID: 533

Severity: ERROR

Message: The provided match pattern "%s" could not be parsed as a regular expression: %s.

ID: 535

Severity: ERROR

Message: The processed ID string %s mapped to multiple users.

ID: 536

Severity: ERROR

Message: The internal search based on processed ID string %s could not be processed efficiently: %s. Check the server configuration to ensure that all associated backends are properly configured for these types of searches.

ID: 537

Severity: ERROR

Message: An internal failure occurred while attempting to resolve processed ID string %s to a user entry: %s.

ID: 538

Severity: ERROR

Message: Cannot add group %s as a new nested group of static group %s because that group is already in the nested group list for the group.

ID: 539

Severity: ERROR

Message: Cannot remove group %s as a nested group of static group %s because that group is not included in the nested group list for the group.

ID: 540

Severity: ERROR

Message: Group instance with DN %s has been deleted and is no longer valid.

ID: 541

Severity: ERROR

Message: The %s attribute is not searchable and should not be included in otherwise unindexed search filters.

ID: 542

Severity: ERROR

Message: The %s attribute is not searchable and should not be included in otherwise unindexed search filters.

ID: 543

Severity: ERROR

Message: The SMTP account status notification handler defined in configuration entry %s cannot be enabled unless the Directory Server is with information about one or more SMTP servers.

ID: 544

Severity: ERROR

Message: SMTP account status notification handler configuration entry '%s' does not include any email address attribute types or recipient addresses. At least one of these must be provided.

ID: 545

Severity: ERROR

Message: Unable to parse message subject value '%s' from configuration entry '%s' because the value does not contain a colon to separate the notification type from the subject.

ID: 546

Severity: ERROR

Message: Unable to parse message subject value '%s' from configuration entry '%s' because '%s' is not a valid account status notification type.

ID: 547

Severity: ERROR

Message: The message subject definitions contained in configuration entry '%s' have multiple subjects defined for notification type %s.

ID: 548

Severity: ERROR

Message: Unable to parse message template file path value '%s' from configuration entry '%s' because the value does not contain a colon to separate the notification type from the template file path.

ID: 549

Severity: ERROR

Message: Unable to parse message template file path value '%s' from configuration entry '%s' because '%s' is not a valid account status notification type.

ID: 550

Severity: ERROR

Message: The message template file path definitions contained in configuration entry '%s' have multiple template file paths defined for notification type %s.

ID: 551

Severity: ERROR

Message: The message template file '%s' referenced in configuration entry '%s' does not exist.

ID: 552

Severity: ERROR

Message: An unclosed token was found starting at column %d of line %d.

ID: 553

Severity: ERROR

Message: The notification-user-attr token starting at column %d of line %d references undefined attribute type %s.

ID: 554

Severity: ERROR

Message: The notification-property token starting at column %d of line %d references undefined notification property %s.

ID: 555

Severity: ERROR

Message: An unrecognized token %s was found at column %d of line %d.

ID: 556

Severity: ERROR

Message: An error occurred while attempting to parse message template file '%s' referenced in configuration entry '%s': %s.

ID: 558

Severity: ERROR

Message: An error occurred while attempting to send an account status notification message for notification type %s for user entry %s: %s.

ID: 559

Severity: ERROR

Message: An error occurred while trying to encrypt a value using password storage scheme %s: %s.

ID: 560

Severity: ERROR

Message: An error occurred while trying to decrypt a value using password storage scheme %s: %s.

ID: 561

Severity: ERROR

Message: Cannot decode the provided symmetric key extended operation because it does not have a value.

ID: 563

Severity: ERROR

Message: Cannot decode the provided symmetric key extended request: %s.

ID: 564

Severity: ERROR

Message: An unexpected error occurred while attempting to decode the symmetric key extended request sequence: %s.

ID: 565

Severity: ERROR

Message: The exact match identity mapper defined in configuration entry %s references

attribute type %s which is does not have an equality index defined in backend %s.

ID: 566

Severity: ERROR

Message: The regular expression identity mapper defined in configuration entry %s references attribute type %s which is does not have an equality index defined in backend %s.

ID: 572

Severity: ERROR

Message: Failed to create a SASL server for SASL mechanism %s using a server FQDN of %s.

ID: 573

Severity: ERROR

Message: GSSAPI SASL mechanism handler initalization failed because the keytab file %s does not exist.

ID: 576

Severity: ERROR

Message: The %s attribute is not searchable and should not be included in otherwise unindexed search filters.

ID: 577

Severity: ERROR

Message: The %s attribute is not searchable and should not be included in otherwise unindexed search filters.

ID: 578

Severity: ERROR

Message: The password value %s has been base64-decoded but is too short to be valid.

ID: 579

Severity: ERROR

Message: The provided minimum required number of character sets '%d' is invalid because it must at least include all mandatory character sets.

ID: 580

Severity: ERROR

Message: The provided minimum required number of character sets '%d' is invalid because it is greater than the total number of defined character sets.

ID: 581

Severity: ERROR

Message: The provided password did not contain characters from at least %d of the following character sets or ranges: %s.

ID: 582

Severity: ERROR

Message: An error occurred while attempting to decode member's DN %s of static group %s: %s.

ID: 583

Severity: ERROR

Message: SASL %s authentication is not supported for user %s because the account is not managed locally.

ID: 584

Severity: ERROR

Message: Password modification is not supported for user %s because the account is not managed locally.

ID: 585

Severity: ERROR

Message: The password policy state extended operation is not supported for user %s because the account is not managed locally.

ID: 586

Severity: ERROR

Message: The user "%s" could not be authenticated using LDAP PTA policy "%s" because the following mapping attributes were not found in the user's entry: %s.

ID: 587

Severity: ERROR

Message: The user "%s" could not be authenticated using LDAP PTA policy "%s" because the search of base DN "%s" returned more than one entry matching the filter "%s".

ID: 588

Severity: ERROR

Message: The user "%s" could not be authenticated using LDAP PTA policy "%s" because the search did not return any entries matching the filter "%s".

ID: 589

Severity: ERROR

Message: The user "%s" could not be authenticated using LDAP PTA policy "%s" because the search failed unexpectedly for the following reason: %s.

ID: 590

Severity: ERROR

Message: The user "%s" could not be authenticated using LDAP PTA policy "%s" because the bind failed unexpectedly for the following reason: %s.

ID: 591

Severity: ERROR

Message: A connection could not be established to the remote LDAP server at %s:%d for LDAP PTA policy "%s" because the host name "%s" could not be resolved to an IP address.

ID: 592

Severity: ERROR

Message: A connection could not be established to the remote LDAP server at %s:%d for LDAP PTA policy "%s" because the connection was refused. This may indicate that the server is either offline or it is not listening on port %d.

ID: 593

Severity: ERROR

Message: A connection could not be established to the remote LDAP server at %s:%d for LDAP PTA policy "%s" because the connection attempt timed out. This may indicate that the server is slow to respond, the network is slow, or that there is some other network problem.

ID: 594

Severity: ERROR

Message: A connection could not be established to the remote LDAP server at %s:%d for LDAP PTA policy "%s" because SSL negotiation failed for the following reason: %s.

ID: 595

Severity: ERROR

Message: A connection could not be established to the remote LDAP server at %s:%d for LDAP PTA policy "%s" because an unexpected error occurred: %s.

ID: 596

Severity: ERROR

Message: The connection to the remote LDAP server at %s:%d for LDAP PTA policy "%s" has failed unexpectedly: %s.

ID: 597

Severity: ERROR

Message: The connection to the remote LDAP server at %s:%d for LDAP PTA policy "%s" has been closed unexpectedly.

ID: 598

Severity: ERROR

Message: The connection to the remote LDAP server at %s:%d for LDAP PTA policy "%s" has timed out and will be closed. This may indicate that the server is slow to respond, the network is slow, or that there is some other network problem.

ID: 599

Severity: ERROR

Message: The connection to the remote LDAP server at %s:%d for LDAP PTA policy "%s" has encountered a protocol error while decoding a response from the server and will be closed. The decoding error was: %s.

ID: 600

Severity: ERROR

Message: The connection to the remote LDAP server at %s:%d for LDAP PTA policy "%s" has received an unexpected response from the server and will be closed. The unexpected response message was: %s.

ID: 601

Severity: ERROR

Message: The connection to the remote LDAP server at %s:%d for LDAP PTA policy "%s" has received a disconnect notification with response code %d (%s) and error message "%s".

ID: 602

Severity: ERROR

Message: The remote LDAP server at %s:%d for LDAP PTA policy "%s" has failed to authenticate user "%s", returning the response code %d (%s) and error message "%s".

ID: 603

Severity: ERROR

Message: The remote LDAP server at %s:%d for LDAP PTA policy "%s" returned multiple matching entries while searching "%s" using the filter "%s".

ID: 604

Severity: ERROR

Message: The remote LDAP server at %s:%d for LDAP PTA policy "%s" did not return any matching entries while searching "%s" using the filter "%s".

ID: 605

Severity: ERROR

Message: The remote LDAP server at %s:%d for LDAP PTA policy "%s" returned an error while searching "%s" using the filter "%s": response code %d (%s) and error message "%s".

ID: 606

Severity: ERROR

Message: The configuration of LDAP PTA policy "%s" is invalid because the remote LDAP server address "%s" specifies a port number which is invalid. Port numbers should be greater than 0 and less than 65536.

ID: 607

Severity: ERROR

Message: The configuration of LDAP PTA policy "%s" is invalid because the Java property %s which should contain the mapped search bind password is not set.

ID: 608

Severity: ERROR

Message: The configuration of LDAP PTA policy "%s" is invalid because the environment variable %s which should contain the mapped search bind password is not set.

ID: 609

Severity: ERROR

Message: The configuration of LDAP PTA policy "%s" is invalid because the file %s which should contain the mapped search bind password does not exist.

ID: 610

Severity: ERROR

Message: The configuration of LDAP PTA policy "%s" is invalid because the file %s which should contain the mapped search bind password cannot be read for the following reason: %s.

ID: 611

Severity: ERROR

Message: The configuration of LDAP PTA policy "%s" is invalid because the file %s which should contain the mapped search bind password is empty.

ID: 613

Severity: ERROR

Message: The configuration of LDAP PTA policy "%s" is invalid because it does not specify the a means for obtaining the mapped search bind password.

ID: 614

Severity: ERROR

Message: The %s attribute is not searchable and should not be included in otherwise unindexed search filters.

ID: 615

Severity: ERROR

Message: The %s attribute is not searchable and should not be included in otherwise unindexed search filters.

ID: 616

Severity: ERROR

Message: The certificate with subject %s mapped to multiple users.

ID: 617

Severity: ERROR

Message: The internal search based on the certificate with subject %s could not be processed efficiently: %s. Check the server configuration to ensure that all associated backends are properly configured for these types of searches.

ID: 618

Severity: ERROR

Message: An internal failure occurred while attempting to map the certificate with subject %s to a user entry: %s.

ID: 619

Severity: ERROR

Message: The certificate with subject %s mapped to multiple users.

ID: 620

Severity: ERROR

Message: The internal search based on the certificate with subject %s could not be processed efficiently: %s. Check the server configuration to ensure that all associated backends are properly configured for these types of searches.

ID: 621

Severity: ERROR

Message: An internal failure occurred while attempting to map the certificate with subject %s to a user entry: %s.

ID: 622

Severity: ERROR

Message: The certificate with fingerprint %s mapped to multiple users.

ID: 623

Severity: ERROR

Message: The internal search based on the certificate with fingerprint %s could not be processed efficiently: %s. Check the server configuration to ensure that all associated backends are properly configured for these types of searches.

ID: 624

Severity: ERROR

Message: An internal failure occurred while attempting to map the certificate with fingerprint %s to a user entry: %s.

ID: 625

Severity: ERROR

Message: The %s attribute is not searchable and should not be included in otherwise unindexed search filters.

ID: 626

Severity: ERROR

Message: The %s attribute is not searchable and should not be included in otherwise unindexed search filters.

ID: 627

Severity: ERROR

Message: The %s attribute is not searchable and should not be included in otherwise unindexed search filters.

ID: 628

Severity: ERROR

Message: The %s attribute is not searchable and should not be included in otherwise unindexed search filters.

ID: 629

Severity: ERROR

Message: The provided password did not contain enough characters from the character range '%s'. The minimum number of characters from that range that must be present in user passwords is %d.

ID: 630

Severity: ERROR

Message: The provided character range definition '%s' is invalid because it does not contain a colon to separate the minimum count from the character range.

ID: 631

Severity: ERROR

Message: The provided character range definition '%s' is invalid because it does not contain a colon to separate the minimum count from the character range.

ID: 632

Severity: ERROR

Message: The provided character range definition '%s' is invalid because the value before the colon must be an integer greater or equal to zero.

ID: 633

Severity: ERROR

Message: The provided character range definition '%s' is invalid because the range '%s' is reversed.

ID: 634

Severity: ERROR

Message: The provided character range definition '%s' is invalid because the range '%s' is missing the minus.

ID: 635

Severity: ERROR

Message: The provided character range definition '%s' is invalid because the range '%s' is too short.

ID: 636

Severity: ERROR

Message: There is no private key entry in keystore %s.

ID: 638

Severity: ERROR

Message: An error occurred while attempting to match a bcrypt hashed password value: %s.

ID: 639

Severity: ERROR

Message: The mapped search filter template "%s" could not be parsed as a valid LDAP filter.

Log Message Category: LOGGER

ID: 1

Severity: ERROR

Message: Error occurred while writing log record for logger %s: %s. Any further write errors will be ignored.

ID: 2

Severity: ERROR

Message: Error occurred while opening log file %s for logger %s: %s.

ID: 3

Severity: ERROR

Message: Error occurred while closing log file for logger %s: %s.

ID: 4

Severity: ERROR

Message: Error occurred while flushing writer buffer for logger %s: %s.

ID: 10

Severity: ERROR

Message: Error occurred while listing log files named by policy with initial file name %s.

ID: 11

Severity: ERROR

Message: Error occurred while obtaining free disk space in the partition containing log file %s: %s.

ID: 12

Severity: ERROR

Message: Error occurred while enforcing retention policy %s for logger %s: %s.

ID: 13

Severity: ERROR

Message: Error occurred while creating common audit facility: %s.

ID: 14

Severity: ERROR

Message: Error while creating or updating common audit log publisher %s: %s.

ID: 15

Severity: ERROR

Message: Error while removing common audit log publisher %s: %s.

ID: 16

Severity: ERROR

Message: Error while adding common audit log publisher %s, the publisher has an unsupported

handler type.

ID: 17

Severity: ERROR

Message: Error while reading JSON configuration file %s while creating common audit external log publisher %s: %s.

ID: 18

Severity: ERROR

Message: Error while creating common audit external log publisher %s: %s.

ID: 19

Severity: ERROR

Message: Error while creating CSV log publisher %s: %s.

ID: 20

Severity: ERROR

Message: Error while adding common audit CSV log publisher %s, the publisher defines an unsupported log rotation policy %s.

ID: 21

Severity: ERROR

Message: Error while adding common audit CSV log publisher %s, the publisher defines an unsupported log retention policy %s.

ID: 22

Severity: ERROR

Message: Error while processing common audit log publisher %s, this type of log publisher is unsupported.

ID: 23

Severity: ERROR

Message: Error while processing common audit log publisher %s, delimiter char '%s' should not contains more than one character.

ID: 24

Severity: ERROR

Message: Error while processing common audit log publisher %s, quote char '%s' should not contains more than one character.

ID: 25

Severity: ERROR

Message: Error while processing common audit log publisher %s, time of the day value '%s' for fixed time log rotation policy is not valid, it should use a 24-hour format "HHmm" : %s.

ID: 26

Severity: ERROR

Message: Error while decoding a transaction id control received from a request: %s.

ID: 27

Severity: ERROR

Message: Error while processing a log event for common audit: %s.

ID: 28

Severity: ERROR

Message: Error while processing common audit log publisher %s, the keystore pin file %s is missing.

ID: 29

Severity: ERROR

Message: Error while processing common audit log publisher %s, the keystore pin file %s could not be read: %s.

ID: 30

Severity: ERROR

Message: Error while processing common audit log publisher %s, the keystore pin file %s contains an empty pin.

ID: 31

Severity: ERROR

Message: Error while processing common audit log publisher %s, the keystore file %s is missing.

ID: 32

Severity: ERROR

Message: Error while processing common audit log publisher %s, the keystore file %s could not be read: %s.

ID: 33

Severity: ERROR

Message: Error while processing common audit log publisher %s, the keystore file %s is empty.

Log Message Category: PLUGIN

ID: 3

Severity: ERROR

Message: The LDAP attribute description list plugin instance defined in configuration entry %s does not list any plugin types. This plugin must be configured to operate as a pre-parse search plugin.

ID: 4

Severity: ERROR

Message: The LDAP attribute description list plugin instance defined in configuration entry %s lists an invalid plugin type %s. This plugin can only be used as a pre-parse search plugin.

ID: 5

Severity: ERROR

Message: The Directory Server profiler plugin instance defined in configuration entry %s does not list any plugin types. This plugin must be configured to operate as a startup plugin.

ID: 6

Severity: ERROR

Message: The Directory Server profiler plugin instance defined in configuration entry %s lists an invalid plugin type %s. This plugin can only be used as a startup plugin.

ID: 9

Severity: ERROR

Message: An unexpected error occurred when the profiler plugin defined in configuration entry %s attempted to write the information captured to output file %s: %s.

ID: 30

Severity: ERROR

Message: The startup plugin defined in configuration entry %s threw an exception when it was invoked during the Directory Server startup process: %s. The server startup process has been aborted.

ID: 31

Severity: ERROR

Message: The startup plugin defined in configuration entry %s returned a null value when it was invoked during the Directory Server startup process. This is an illegal return value, and the server startup process has been aborted.

ID: 33

Severity: ERROR

Message: The startup plugin defined in configuration entry %s encountered an error when it was invoked during the Directory Server startup process: %s (error ID %d). The server startup

process has been aborted.

ID: 34

Severity: ERROR

Message: The shutdown plugin defined in configuration entry %s threw an exception when it was invoked during the Directory Server shutdown process: %s.

ID: 35

Severity: ERROR

Message: The post-connect plugin defined in configuration entry %s threw an exception when it was invoked for connection %d from %s: %s. The connection will be terminated.

ID: 36

Severity: ERROR

Message: The post-connect plugin defined in configuration entry %s returned null when invoked for connection %d from %s. This is an illegal response, and the connection will be terminated.

ID: 37

Severity: ERROR

Message: The post-disconnect plugin defined in configuration entry %s threw an exception when it was invoked for connection %d from %s: %s.

ID: 38

Severity: ERROR

Message: The post-disconnect plugin defined in configuration entry %s returned null when invoked for connection %d from %s. This is an illegal response.

ID: 39

Severity: ERROR

Message: The pre-parse %s plugin defined in configuration entry %s threw an exception when it was invoked for connection %d operation %d: %s. Processing on this operation will be terminated.

ID: 40

Severity: ERROR

Message: The pre-parse %s plugin defined in configuration entry %s returned null when invoked for connection %d operation %d. This is an illegal response, and processing on this operation will be terminated.

ID: 41

Severity: ERROR

Message: The pre-operation %s plugin defined in configuration entry %s threw an exception

when it was invoked for connection %d operation %d: %s. Processing on this operation will be terminated.

ID: 42

Severity: ERROR

Message: The pre-operation %s plugin defined in configuration entry %s returned null when invoked for connection %d operation %d. This is an illegal response, and processing on this operation will be terminated.

ID: 43

Severity: ERROR

Message: The post-operation %s plugin defined in configuration entry %s threw an exception when it was invoked for connection %d operation %d: %s. Processing on this operation will be terminated.

ID: 44

Severity: ERROR

Message: The post-operation %s plugin defined in configuration entry %s returned null when invoked for connection %d operation %d. This is an illegal response, and processing on this operation will be terminated.

ID: 45

Severity: ERROR

Message: The post-response %s plugin defined in configuration entry %s threw an exception when it was invoked for connection %d operation %d: %s. Processing on this operation will be terminated.

ID: 46

Severity: ERROR

Message: The post-response %s plugin defined in configuration entry %s returned null when invoked for connection %d operation %d. This is an illegal response, and processing on this operation will be terminated.

ID: 47

Severity: ERROR

Message: The search result entry plugin defined in configuration entry %s threw an exception when it was invoked for connection %d operation %d with entry %s: %s. Processing on this search operation will be terminated.

ID: 48

Severity: ERROR

Message: The search result entry plugin defined in configuration entry %s returned null when invoked for connection %d operation %d with entry %s. This is an illegal response, and

processing on this search operation will be terminated.

ID: 49

Severity: ERROR

Message: The search result reference plugin defined in configuration entry %s threw an exception when it was invoked for connection %d operation %d with referral URL(s) %s: %s. Processing on this search operation will be terminated.

ID: 50

Severity: ERROR

Message: The search result reference plugin defined in configuration entry %s returned null when invoked for connection %d operation %d with referral URL(s) %s. This is an illegal response, and processing on this search operation will be terminated.

ID: 51

Severity: ERROR

Message: An attempt was made to register the LastMod plugin to be invoked as a %s plugin. This plugin type is not allowed for this plugin.

ID: 55

Severity: ERROR

Message: An unexpected error occurred while attempting to initialize the command-line arguments: %s.

ID: 56

Severity: ERROR

Message: An error occurred while parsing the command-line arguments: %s.

ID: 57

Severity: ERROR

Message: An error occurred while trying to process the profile data in file %s: %s.

ID: 58

Severity: ERROR

Message: The LDIF import plugin defined in configuration entry %s threw an exception when it was invoked on entry %s: %s.

ID: 59

Severity: ERROR

Message: The LDIF import plugin defined in configuration entry %s returned null when invoked on entry %s. This is an illegal response.

ID: 60

Severity: ERROR

Message: The LDIF export plugin defined in configuration entry %s threw an exception when it was invoked on entry %s: %s.

ID: 61

Severity: ERROR

Message: The LDIF export plugin defined in configuration entry %s returned null when invoked on entry %s. This is an illegal response.

ID: 62

Severity: ERROR

Message: An attempt was made to register the EntryUUID plugin to be invoked as a %s plugin. This plugin type is not allowed for this plugin.

ID: 63

Severity: ERROR

Message: The intermediate response plugin defined in configuration entry %s threw an exception when it was invoked for connection %d operation %d: %s. Processing on this operation will be terminated.

ID: 64

Severity: ERROR

Message: The intermediate response plugin defined in configuration entry %s returned null when invoked for connection %d operation %d. This is an illegal response, and processing on this operation will be terminated.

ID: 65

Severity: ERROR

Message: An attempt was made to register the password policy import plugin to be invoked as a %s plugin. This plugin type is not allowed for this plugin.

ID: 66

Severity: ERROR

Message: An error occurred while attempting to encode a password value stored in attribute %s of user entry %s: %s. Password values for this user will not be encoded.

ID: 67

Severity: ERROR

Message: The plugin defined in configuration entry %s does not support the %s plugin type.

ID: 69

Severity: ERROR

Message: The password policy import plugin is not configured any default auth password schemes, and the server does not support the %s auth password scheme.

ID: 70

Severity: ERROR

Message: Auth password storage scheme %s referenced by the password policy import plugin is not configured for use in the server.

ID: 71

Severity: ERROR

Message: The password policy import plugin is not configured any default user password schemes, and the server does not support the %s auth password scheme.

ID: 72

Severity: ERROR

Message: User password storage scheme %s referenced by the password policy import plugin is not configured for use in the server.

ID: 75

Severity: ERROR

Message: The subordinate modify DN plugin defined in configuration entry %s threw an exception when it was invoked for connection %d operation %d: %s. Processing on this operation will be terminated.

ID: 76

Severity: ERROR

Message: The subordinate modify DN plugin defined in configuration entry %s returned null when invoked for connection %d operation %s. This is an illegal response, and processing on this operation will be terminated.

ID: 77

Severity: ERROR

Message: An attempt was made to register the Unique Attribute plugin to be invoked as a %s plugin. This plugin type is not allowed for this plugin.

ID: 81

Severity: ERROR

Message: An attempt was made to register the Referential Integrity plugin to be invoked as a %s plugin. This plugin type is not allowed for this plugin.

ID: 82

Severity: ERROR

Message: An error occurred during Referential Integity plugin initialization because log file creation failed: %s.

ID: 83

Severity: ERROR

Message: An error occurred closing the Referential Integrity plugin update log file: %s.

ID: 84

Severity: ERROR

Message: An error occurred replacing the Referential Integrity plugin update log file: %s.

ID: 89

Severity: ERROR

Message: The Referential Integrity plugin failed when performaing an internal search: %s.

ID: 90

Severity: ERROR

Message: The Referential Integrity plugin failed when performing an internal modify on entry %s: %s.

ID: 91

Severity: ERROR

Message: The Referential Integrity plugin failed to decode a entry DN from the update log: %s.

ID: 93

Severity: ERROR

Message: An error occurred in the Referential Integrity plugin while attempting to configure the attribute type %s which has a syntax OID of %s. A Referential Integrity attribute type must have a syntax OID of either 1.3.6.1.4.1.1466.115.121.1.12 (for the distinguished name syntax) or 1.3.6.1.4.1.1466.115.121.1.34 (for the name and optional uid syntax).

ID: 96

Severity: ERROR

Message: The 7-bit clean plugin is configured with invalid plugin type %s. Only the ldifImport, preOperationAdd, preOperationModify, and preOperationModifyDN plugin types are allowed.

ID: 97

Severity: ERROR

Message: An error occurred while trying to decode the DN of the target entry: %s.

ID: 98

Severity: ERROR

Message: An error occurred while trying to decode attribute %s in the target entry: %s.

ID: 99

Severity: ERROR

Message: An error occurred while trying to decode the new RDN: %s.

ID: 102

Severity: ERROR

Message: The modify DN operation would have resulted in a value for attribute %s that was not 7-bit clean.

ID: 103

Severity: ERROR

Message: The entry included a value for attribute %s that was not 7-bit clean.

ID: 104

Severity: ERROR

Message: The password policy import plugin references default auth password storage scheme %s which is not available for use in the server.

ID: 105

Severity: ERROR

Message: The post-synchronization %s plugin defined in configuration entry %s threw an exception when it was invoked for connection %d operation %d: %s.

ID: 106

Severity: ERROR

Message: A unique attribute conflict was detected for attribute %s: value %s already exists in entry %s.

ID: 107

Severity: ERROR

Message: A unique attribute conflict was detected for attribute %s during synchronization (connID=%d, opID=%d): value %s in entry %s conflicts with an existing value in entry %s. Manual interaction is required to eliminate the conflict.

ID: 108

Severity: ERROR

Message: An internal error occurred while attempting to determine whether the operation

would have resulted in a unique attribute conflict (result %s, message %s).

ID: 109

Severity: ERROR

Message: An internal error occurred while attempting to determine whether the synchronization operation (connID=%d, opID=%d) for entry %s would have resulted in a unique attribute conflict (result %s, message %s).

ID: 110

Severity: ERROR

Message: The referential integrity plugin defined in configuration entry %s is configured to operate on attribute %s but there is no equality index defined for this attribute in backend %s.

ID: 111

Severity: ERROR

Message: The unique attribute plugin defined in configuration entry %s is configured to operate on attribute %s but there is no equality index defined for this attribute in backend %s.

ID: 113

Severity: ERROR

Message: An attempt was made to register the Change Number Control plugin to be invoked as a %s plugin. This plugin type is not allowed for this plugin.

ID: 114

Severity: ERROR

Message: An attempt was made to register the Change Number Control plugin with the following plugin types : %s. However this plugin must be configured with all of the following plugin types : %s.

ID: 115

Severity: ERROR

Message: The subordinate delete plugin defined in configuration entry %s threw an exception when it was invoked for connection %d operation %d: %s. Processing on this operation will be terminated.

ID: 116

Severity: ERROR

Message: The subordinate delete plugin defined in configuration entry %s returned null when invoked for connection %d operation %s. This is an illegal response, and processing on this operation will be terminated.

ID: 117

Severity: ERROR

Message: An attempt was made to register the Samba password synchronization plugin to be invoked as a %s plugin. This plugin type is not allowed for this plugin.

ID: 118

Severity: ERROR

Message: The Samba password synchronization plugin could not encode a password for the following reasons: %s.

ID: 119

Severity: ERROR

Message: The Samba password synchronization plugin could not process a modification for the following reason: %s.

ID: 120

Severity: ERROR

Message: Invalid plugin type '%s' for the Attribute Cleanup plugin.

ID: 121

Severity: ERROR

Message: Attribute '%s' is not defined in the directory schema.

ID: 122

Severity: ERROR

Message: The attribute '%s' has already been defined in the configuration.

ID: 123

Severity: ERROR

Message: The mapping '%s:%s' maps the attribute to itself.

ID: 124

Severity: ERROR

Message: The property 'check-references-filter-criteria' specifies filtering criteria for attribute '%s', but this attribute is not listed in the 'attribute-type' property.

ID: 125

Severity: ERROR

Message: The filtering criteria '%s' specified in property 'check-references-filter-criteria' is invalid because the filter could not be decoded: '%s'.

ID: 126

Severity: ERROR

Message: The entry referenced by the value '%s' of the attribute '%s' in the entry '%s' does not exist in any of the configured naming contexts.

ID: 127

Severity: ERROR

Message: The entry referenced by the value '%s' of the attribute '%s' in the entry '%s' does not match the filter '%s'.

ID: 128

Severity: ERROR

Message: The entry referenced by the value '%s' of the attribute '%s' in the entry '%s' does not belong to any of the configured naming contexts.

ID: 129

Severity: ERROR

Message: The opration could not be processed due to an unexpected exception: '%s'.

Log Message Category: PROTOCOL

ID: 45

Severity: ERROR

Message: Cannot decode the provided ASN.1 sequence as an LDAP message because the sequence was null.

ID: 47

Severity: ERROR

Message: Cannot decode the provided ASN.1 sequence as an LDAP message because the first element of the sequence could not be decoded as an integer message ID: %s.

ID: 48

Severity: ERROR

Message: Cannot decode the provided ASN.1 sequence as an LDAP message because the second element of the sequence could not be decoded as the protocol op: %s.

ID: 49

Severity: ERROR

Message: Cannot decode the provided ASN.1 sequence as an LDAP message because the third element of the sequence could not be decoded as the set of controls: %s.

ID: 51

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP control because the element

could not be decoded as a sequence: %s.

ID: 53

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP control because the OID could not be decoded as a string: %s.

ID: 54

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP control because the criticality could not be decoded as Boolean value: %s.

ID: 55

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP control because the value could not be decoded as an octet string: %s.

ID: 58

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as a set of LDAP controls because the element could not be decoded as a sequence: %s.

ID: 59

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP abandon request protocol op because a problem occurred while trying to obtain the message ID of the operation to abandon: %s.

ID: 60

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP result protocol op because a problem occurred while trying to parse the result sequence: %s.

ID: 62

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP result protocol op because the first element in the result sequence could not be decoded as an integer result code: %s.

ID: 63

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP result protocol op because the second element in the result sequence could not be decoded as the matched DN: %s.

ID: 64

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP result protocol op because the third element in the result sequence could not be decoded as the error message: %s.

ID: 65

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP result protocol op because the fourth element in the result sequence could not be decoded as a set of referral URLs: %s.

ID: 67

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP bind response protocol op because the final element in the result sequence could not be decoded as the server SASL credentials: %s.

ID: 71

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP bind response protocol op because the response OID could not be decoded: %s.

ID: 72

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP bind response protocol op because the response value could not be decoded: %s.

ID: 74

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP unbind request protocol op: %s.

ID: 75

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP bind request protocol op because the element could not be decoded as a sequence: %s.

ID: 77

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP bind request protocol op because the protocol version could not be decoded as an integer: %s.

ID: 78

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP bind request protocol op because the bind DN could not be properly decoded: %s.

ID: 79

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP bind request protocol op because the password to use for simple authentication could not be decoded: %s.

ID: 80

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP bind request protocol op because the SASL authentication information could not be decoded: %s.

ID: 81

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP bind request protocol op because the authentication info element had an invalid BER type (expected 80 or A3, got %x).

ID: 82

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP bind request protocol op because an unexpected error occurred while trying to decode the authentication info element: %s.

ID: 83

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP compare request protocol op because the element could not be decoded as a sequence: %s.

ID: 85

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP compare request protocol op because the target DN could not be properly decoded: %s.

ID: 86

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP compare request protocol op because the attribute value assertion could not be decoded as a sequence: %s.

ID: 88

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP compare request protocol op because the attribute type could not be properly decoded: %s.

ID: 89

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP compare request protocol op because the assertion value could not be properly decoded: %s.

ID: 90

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP delete request protocol op because the target DN could not be properly decoded: %s.

ID: 91

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP extended request protocol op because the element could not be decoded as a sequence: %s.

ID: 93

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP extended request protocol op because the OID could not be properly decoded: %s.

ID: 94

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP extended request protocol op because the value could not be properly decoded: %s.

ID: 95

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP modify DN request protocol op because the element could not be decoded as a sequence: %s.

ID: 97

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP modify DN request protocol op because the entry DN could not be properly decoded: %s.

ID: 98

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP modify DN request protocol op because the new RDN could not be properly decoded: %s.

ID: 99

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP modify DN request protocol op because the deleteOldRDN flag could not be properly decoded: %s.

ID: 100

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP modify DN request protocol op because the new superior DN could not be properly decoded: %s.

ID: 101

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP attribute because the element could not be decoded as a sequence: %s.

ID: 103

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP attribute because the attribute type could not be decoded: %s.

ID: 104

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP attribute because the set of values could not be decoded: %s.

ID: 105

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP add request protocol op because the element could not be decoded as a sequence: %s.

ID: 107

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP add request protocol op because the entry DN could not be decoded: %s.

ID: 108

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP add request protocol op because the set of attributes could not be decoded: %s.

ID: 109

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP modification because the element could not be decoded as a sequence: %s.

ID: 111

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP modification because it contained an invalid modification type (%d).

ID: 112

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP modification because the modification type could not be decoded: %s.

ID: 113

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP modification because the attribute could not be decoded: %s.

ID: 114

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP modify request protocol op because the element could not be decoded as a sequence: %s.

ID: 116

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP modify request protocol op because the entry DN could not be decoded: %s.

ID: 117

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP modify request protocol op because the set of modifications could not be decoded: %s.

ID: 118

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search result entry protocol op because the element could not be decoded as a sequence: %s.

ID: 120

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search result entry protocol op because the entry DN could not be decoded: %s.

ID: 121

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search result entry protocol op because the set of attributes could not be decoded: %s.

ID: 122

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search result reference protocol op because the element could not be decoded as a sequence: %s.

ID: 123

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search result reference protocol op because a problem occurred while trying to decode the sequence elements as referral URLs: %s.

ID: 124

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search request protocol op because the element could not be decoded as a sequence: %s.

ID: 126

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search request protocol op because the base DN could not be decoded: %s.

ID: 127

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search request protocol op because the provided scope value (%d) is invalid.

ID: 128

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search request protocol op because the scope could not be decoded: %s.

ID: 129

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search request protocol op

because the provided alias dereferencing policy value (%d) is invalid.

ID: 130

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search request protocol op because the alias dereferencing policy could not be decoded: %s.

ID: 131

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search request protocol op because the size limit could not be decoded: %s.

ID: 132

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search request protocol op because the time limit could not be decoded: %s.

ID: 133

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search request protocol op because the typesOnly flag could not be decoded: %s.

ID: 134

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search request protocol op because the filter could not be decoded: %s.

ID: 135

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search request protocol op because the requested attribute set could not be decoded: %s.

ID: 136

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP protocol op because the element was null.

ID: 137

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP protocol op because the element had an invalid BER type (%x) for an LDAP protocol op.

ID: 138

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search filter because the element was null.

ID: 139

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search filter because the element had an invalid BER type (%x) for a search filter.

ID: 141

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search filter because an unexpected error occurred while trying to decode one of the compound filter components: %s.

ID: 143

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search filter because the NOT component element could not be decoded as an LDAP filter: %s.

ID: 144

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search filter because the element could not be decoded as a type-and-value sequence: %s.

ID: 146

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search filter because the attribute type could not be decoded from the type-and-value sequence: %s.

ID: 147

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search filter because the assertion value could not be decoded from the type-and-value sequence: %s.

ID: 148

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search filter because the element could not be decoded as a substring sequence: %s.

ID: 150

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search filter because the attribute type could not be decoded from the substring sequence: %s.

ID: 151

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search filter because the substring value sequence could not be decoded: %s.

ID: 152

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search filter because the substring value sequence did not contain any elements.

ID: 154

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search filter because a problem occurred while trying to parse the substring value elements: %s.

ID: 155

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search filter because the element could not be decoded as the presence attribute type: %s.

ID: 156

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search filter because the element could not be decoded as an extensible matching sequence: %s.

ID: 158

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP search filter because a problem occurred while trying to parse the extensible match sequence elements: %s.

ID: 159

Severity: ERROR

Message: The server attempted to send a response to the %s operation (conn=%d, op=%d), but the operation did not have a result code. This could indicate that the operation did not complete properly or that it is one that is not allowed to have a response. Using a generic 'Operations Error' response.

ID: 160

Severity: ERROR

Message: The server attempted to send a response to the %s operation (conn=%d, op=%d), but this type of operation is not allowed to have responses. Backtrace: %s.

ID: 177

Severity: ERROR

Message: The LDAP connection handler defined in configuration entry %s was unable to open a selector to allow it to multiplex the associated accept sockets: %s. This connection handler will be disabled.

ID: 178

Severity: ERROR

Message: The LDAP connection handler defined in configuration entry %s was unable to create a server socket channel to accept connections on %s:%d: %s. The Directory Server will not listen for new connections on that address.

ID: 179

Severity: ERROR

Message: The LDAP connection handler defined in configuration entry %s was unable to create any of the socket channels on any of the configured addresses. This connection handler will be disabled.

ID: 180

Severity: ERROR

Message: The connection attempt from client %s to %s has been rejected because the client was included in one of the denied address ranges.

ID: 181

Severity: ERROR

Message: The connection attempt from client %s to %s has been rejected because the client was not included in one of the allowed address ranges.

ID: 183

Severity: ERROR

Message: The %s defined in configuration entry %s was unable to accept a new client connection: %s.

ID: 184

Severity: ERROR

Message: The %s defined in configuration entry %s has experienced consecutive failures while trying to accept client connections: %s. This connection handler will be disabled.

ID: 185

Severity: ERROR

Message: The LDAP connection handler defined in configuration entry %s caught an unexpected error while trying to listen for new connections: %s. This connection handler will be disabled.

ID: 186

Severity: ERROR

Message: %s was unable to open a selector to multiplex reads from clients: %s. This request handler cannot continue processing.

ID: 187

Severity: ERROR

Message: %s was unable to register this client connection with the selector: %s.

ID: 188

Severity: ERROR

Message: This connection could not be registered with a request handler because the Directory Server is shutting down.

ID: 190

Severity: ERROR

Message: This client connection is being deregistered from the associated request handler because the Directory Server is shutting down.

ID: 192

Severity: ERROR

Message: Cannot decode the provided string as an LDAP search filter because the string was null.

ID: 193

Severity: ERROR

Message: Cannot decode the provided string %s as an LDAP search filter because an unexpected exception was thrown during processing: %s.

ID: 194

Severity: ERROR

Message: The provided search filter "%s" had mismatched parentheses around the portion between positions %d and %d.

ID: 195

Severity: ERROR

Message: The provided search filter "%s" was missing an equal sign in the suspected simple filter component between positions %d and %d.

ID: 196

Severity: ERROR

Message: The provided search filter "%s" had an invalid escaped byte value at position %d. A backslash in a value must be followed by two hexadecimal characters that define the byte that has been encoded.

ID: 197

Severity: ERROR

Message: The provided search filter "%s" could not be decoded because the compound filter between positions %d and %d did not start with an open parenthesis and end with a close parenthesis (they might be parentheses for different filter components).

ID: 198

Severity: ERROR

Message: The provided search filter "%s" could not be decoded because the closing parenthesis at position %d did not have a corresponding open parenthesis.

ID: 199

Severity: ERROR

Message: The provided search filter "%s" could not be decoded because the opening parenthesis at position %d did not have a corresponding close parenthesis.

ID: 200

Severity: ERROR

Message: The provided search filter "%s" could not be decoded because the assumed substring filter value between positions %d and %d did not have any asterisk wildcard characters.

ID: 201

Severity: ERROR

Message: The provided search filter "%s" could not be decoded because the extensible match component starting at position %d did not have a colon to denote the end of the attribute type name.

ID: 202

Severity: ERROR

Message: Terminating this connection because the client sent an invalid message of type %s (LDAP message ID %d) that is not allowed for request messages.

ID: 203

Severity: ERROR

Message: An unexpected failure occurred while trying to process a request of type %s (LDAP message ID %d): %s. The client connection will be terminated.

ID: 204

Severity: ERROR

Message: The bind request message (LDAP message ID %d) included an invalid authentication type of %s. This is a protocol error, and this connection will be terminated as per RFC 2251 section 4.2.3.

ID: 205

Severity: ERROR

Message: This client connection is being terminated because a protocol error occurred while trying to process a bind request. The LDAP message ID was %d and the error message for the bind response was %s.

ID: 206

Severity: ERROR

Message: An extended response message would have been sent to an LDAPv2 client (connection ID=%d, operation ID=%d): %s. LDAPv2 does not allow extended operations, so this response will not be sent.

ID: 207

Severity: ERROR

Message: A search performed by an LDAPv2 client (connection ID=%d, operation ID=%d) would have included a search result reference %s. Referrals are not allowed for LDAPv2 clients, so this search reference will not be sent.

ID: 208

Severity: ERROR

Message: The original result code for this message was 10 but this result is not allowed for LDAPv2 clients.

ID: 209

Severity: ERROR

Message: The response included one or more referrals, which are not allowed for LDAPv2 clients. The referrals included were: %s.

ID: 210

Severity: ERROR

Message: The Directory Server has been configured to deny access to LDAPv2 clients. This connection will be closed.

ID: 211

Severity: ERROR

Message: The client with connection ID %d authenticated to the Directory Server using LDAPv2,

but attempted to send an extended operation request (LDAP message ID %d), which is not allowed for LDAPv2 clients. The connection will be terminated.

ID: 212

Severity: ERROR

Message: An attempt was made to initialize the LDAP statistics monitor provider as defined in configuration entry %s. This monitor provider should only be dynamically created within the Directory Server itself and not from within the configuration.

ID: 213

Severity: ERROR

Message: The LDAP request handler thread "%s" encountered an unexpected error that would have caused the thread to die: %s. The error has been caught and the request handler should continue operating as normal.

ID: 214

Severity: ERROR

Message: The attempt to register this connection with the Directory Server was rejected. This might indicate that the server already has the maximum allowed number of concurrent connections established, or that it is in a restricted access mode.

ID: 264

Severity: ERROR

Message: An unexpected error occurred while trying to decode the DN %s used for internal operations as a root user: %s.

ID: 271

Severity: ERROR

Message: The TLS connection security provider cannot be enabled on this client connection because it is already using the %s provider. StartTLS can only be used on clear-text connections.

ID: 272

Severity: ERROR

Message: StartTLS cannot be enabled on this LDAP client connection because the corresponding LDAP connection handler is configured to reject StartTLS requests. The use of StartTLS can be enabled using the ds-cfg-allow-start-tls configuration attribute.

ID: 273

Severity: ERROR

Message: An error occurred while attempting to create a TLS connection security provider for this client connection for use with StartTLS: %s.

ID: 278

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP paged results control value because the element is null.

ID: 279

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP paged results control value because the element could not be decoded as a sequence: %s.

ID: 281

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP paged results control value because the size element could not be properly decoded: %s.

ID: 282

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP paged results control value because the cookie could not be properly decoded: %s.

ID: 283

Severity: ERROR

Message: Cannot decode the provided LDAP assertion control because the control does not have a value.

ID: 285

Severity: ERROR

Message: Cannot decode the provided LDAP pre-read request control because the control does not have a value.

ID: 286

Severity: ERROR

Message: Cannot decode the provided LDAP pre-read request control because an error occurred while trying to decode the control value: %s.

ID: 287

Severity: ERROR

Message: Cannot decode the provided LDAP post-read request control because the control does not have a value.

ID: 288

Severity: ERROR

Message: Cannot decode the provided LDAP post-read request control because an error occurred while trying to decode the control value: %s.

ID: 289

Severity: ERROR

Message: Cannot decode the provided LDAP pre-read response control because the control does not have a value.

ID: 290

Severity: ERROR

Message: Cannot decode the provided LDAP pre-read response control because an error occurred while trying to decode the control value: %s.

ID: 291

Severity: ERROR

Message: Cannot decode the provided LDAP post-read response control because the control does not have a value.

ID: 292

Severity: ERROR

Message: Cannot decode the provided LDAP post-read response control because an error occurred while trying to decode the control value: %s.

ID: 293

Severity: ERROR

Message: Cannot decode the provided proxied authorization V1 control because it does not have a value.

ID: 295

Severity: ERROR

Message: Cannot decode the provided proxied authorization V1 control because an error occurred while attempting to decode the control value: %s.

ID: 296

Severity: ERROR

Message: User %s specified in the proxied authorization V1 control does not exist in the Directory Server.

ID: 297

Severity: ERROR

Message: Cannot decode the provided proxied authorization V2 control because it does not have a value.

ID: 299

Severity: ERROR

Message: Unable to process proxied authorization V2 control because it contains an authorization ID based on a username and no proxied authorization identity mapper is configured in the Directory Server.

ID: 300

Severity: ERROR

Message: The authorization ID "%s" contained in the proxied authorization V2 control is invalid because it does not start with "dn:" to indicate a user DN or "u:" to indicate a username.

ID: 301

Severity: ERROR

Message: User %s specified in the proxied authorization V2 control does not exist in the Directory Server.

ID: 302

Severity: ERROR

Message: The provided integer value %d does not correspond to any persistent search change type.

ID: 303

Severity: ERROR

Message: The provided integer value indicated that there were no persistent search change types, which is not allowed.

ID: 304

Severity: ERROR

Message: The provided integer value %d was outside the range of acceptable values for an encoded change type set.

ID: 305

Severity: ERROR

Message: Cannot decode the provided persistent search control because it does not have a value.

ID: 307

Severity: ERROR

Message: Cannot decode the provided persistent search control because an error occurred while attempting to decode the control value: %s.

ID: 308

Severity: ERROR

Message: Cannot decode the provided entry change notification control because it does not have a value.

ID: 310

Severity: ERROR

Message: Cannot decode the provided entry change notification control because it contains a previous DN element but had a change type of %s. The previous DN element can only be provided with the modify DN change type.

ID: 312

Severity: ERROR

Message: Cannot decode the provided entry change notification control because an error occurred while attempting to decode the control value: %s.

ID: 313

Severity: ERROR

Message: Cannot decode the provided authorization identity response control because it does not have a value.

ID: 314

Severity: ERROR

Message: Cannot decode the provided ASN.1 element as an LDAP intermediate response protocol op because the element could not be decoded as a sequence: %s.

ID: 316

Severity: ERROR

Message: An error occurred while attempting to decode the intermediate response OID: %s.

ID: 317

Severity: ERROR

Message: An error occurred while attempting to decode the intermediate response value: %s.

ID: 321

Severity: ERROR

Message: The provided LDAP filter "%s" cannot be used as a matched values filter because filters of type %s are not allowed for use in matched values filters.

ID: 322

Severity: ERROR

Message: The provided LDAP filter "%s" cannot be used as a matched values filter because it is an extensible match filter that contains the dnAttributes flag, which is not allowed for matched values filters.

ID: 324

Severity: ERROR

Message: An error occurred while attempting to decode the attribute value assertion in the provided matched values filter: %s.

ID: 326

Severity: ERROR

Message: The provided matched values filter could not be decoded because there were no subInitial, subAny, or subFinal components in the substring filter.

ID: 330

Severity: ERROR

Message: The provided matched values filter could not be decoded because an error occurred while decoding the substring filter component: %s.

ID: 331

Severity: ERROR

Message: The provided matched values filter could not be decoded because an error occurred while decoding the presence filter component: %s.

ID: 337

Severity: ERROR

Message: The provided matched values filter could not be decoded because an error occurred while decoding the extensible match filter component: %s.

ID: 338

Severity: ERROR

Message: The provided matched values filter could not be decoded because it had an invalid BER type of %s.

ID: 339

Severity: ERROR

Message: Cannot decode the provided matched values control because it does not have a value.

ID: 340

Severity: ERROR

Message: Cannot decode the provided matched values control because an error occurred while attempting to decode the value as an ASN.1 sequence: %s.

ID: 341

Severity: ERROR

Message: Cannot decode the provided matched values control because the control value does not specify any filters for use in matching attribute values.

ID: 342

Severity: ERROR

Message: Cannot decode the provided control as a password expired control because the provided control had a value that could not be parsed as an integer.

ID: 343

Severity: ERROR

Message: Cannot decode the provided password expiring control because it does not have a value.

ID: 344

Severity: ERROR

Message: Cannot decode the provided control as a password expiring control because an error occurred while attempting to decode the number of seconds until expiration: %s.

ID: 354

Severity: ERROR

Message: Cannot decode the provided control as a password policy request control because the provided control had a value but the password policy request control should not have a value.

ID: 355

Severity: ERROR

Message: Cannot decode the provided password policy response control because it does not have a value.

ID: 356

Severity: ERROR

Message: Cannot decode the provided password policy response control because the warning element has an invalid type of %s.

ID: 357

Severity: ERROR

Message: Cannot decode the provided password policy response control because the error element has an invalid type of %d.

ID: 359

Severity: ERROR

Message: Cannot decode the provided password policy response control: %s.

ID: 372

Severity: ERROR

Message: Use of the proxied authorization V1 control for user %s is not allowed by the password policy configuration.

ID: 375

Severity: ERROR

Message: Cannot decode the provided control as an account availability request control because the provided control had a value but the account availability request control should not have a value.

ID: 376

Severity: ERROR

Message: Cannot decode the provided account availability response control because it does not have a value.

ID: 378

Severity: ERROR

Message: The account availability response control had an unknown ACCOUNT_USABLE_RESPONSE element type of %s.

ID: 379

Severity: ERROR

Message: Cannot decode the provided account availability response control: %s.

ID: 384

Severity: ERROR

Message: The provided LDAP attribute %s contains duplicate values.

ID: 385

Severity: ERROR

Message: The provided LDAP search filter references unknown matching rule %s.

ID: 386

Severity: ERROR

Message: The provided LDAP search filter has an assertion value but does not include either an attribute type or a matching rule ID.

ID: 387

Severity: ERROR

Message: Unable to call select() in the LDAP connection handler: %s. It appears that your JVM

may be susceptible to the issue described at http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6322825, and it is unable to handle LDAP requests in its current configuration. Please upgrade to a newer JVM that does not exhibit this behavior (Java 5.0 Update 8 or higher) or set the number of available file descriptors to a value greater than or equal to 8193 (e.g., by issuing the command 'ulimit -n 8193') before starting the Directory Server.

ID: 388

Severity: ERROR

Message: Unwilling to process the request because it contains a proxied authorization V1 control which is not marked critical. The proxied authorization control must always have a criticality of "true".

ID: 389

Severity: ERROR

Message: Unwilling to process the request because it contains a proxied authorization V2 control which is not marked critical. The proxied authorization control must always have a criticality of "true".

ID: 405

Severity: ERROR

Message: The provided search filter "%s" could not be decoded because the NOT filter between positions %d and %d did not contain exactly one filter component.

ID: 427

Severity: ERROR

Message: An LDAP filter enclosed in apostrophes is invalid: %s.

ID: 429

Severity: ERROR

Message: The provided search filter contains an invalid attribute type '%s' with invalid character '%s' at position %d.

ID: 430

Severity: ERROR

Message: The provided search filter "%s" could not be decoded because the extensible match component starting at position %d did not include either an attribute description or a matching rule ID. At least one of them must be provided.

ID: 431

Severity: ERROR

Message: LDAPv2 clients are not allowed to use request controls.

ID: 432

Severity: ERROR

Message: The %s connection handler defined in configuration entry %s was unable to bind to %s:%d: %s.

ID: 438

Severity: ERROR

Message: You do not have sufficient privileges to perform search operations through JMX.

ID: 439

Severity: ERROR

Message: You do not have sufficient privileges to establish the connection through JMX. At least JMX_READ privilege is required.

ID: 440

Severity: ERROR

Message: User %s does not exist in the directory.

ID: 441

Severity: ERROR

Message: This output stream has been closed.

ID: 442

Severity: ERROR

Message: The provided LDAP message had an invalid operation type (%s) for a request.

ID: 443

Severity: ERROR

Message: SASL bind operations are not supported over internal LDAP sockets.

ID: 444

Severity: ERROR

Message: StartTLS operations are not supported over internal LDAP sockets.

ID: 447

Severity: ERROR

Message: An error occurred while trying to read a change record from the LDIF file: %s. This change will be skipped but processing on the LDIF file will continue.

ID: 448

Severity: ERROR

Message: An error occurred while trying to read a change record from the LDIF file: %s. No further processing on this LDIF file can be performed.

ID: 454

Severity: ERROR

Message: An I/O error occurred while the LDIF connection handler was processing LDIF file %s: %s.

ID: 455

Severity: ERROR

Message: An error occurred while the LDIF connection handler was attempting to rename partially-processed file from %s to %s: %s.

ID: 456

Severity: ERROR

Message: An error occurred while the LDIF connection handler was attempting to delete processed file %s: %s.

ID: 457

Severity: ERROR

Message: Address already in use.

ID: 458

Severity: ERROR

Message: Cannot decode the provided subentries control because it does not have a value.

ID: 459

Severity: ERROR

Message: Cannot decode the provided subentries control because an error occurred while attempting to decode the control value: %s.

ID: 1462

Severity: ERROR

Message: No Configuration was defined for this connection handler. The configuration parameters ds-cfg-listen-port and ds-cfg-trap-port are required by the connection handler to start.

ID: 1463

Severity: ERROR

Message: Traps Destination %s is an unknown host. Traps will not be sent to this destination.

ID: 1464

Severity: ERROR

Message: You do not have the appropriate OpenDMK jar files to enable the SNMP Connection Handler. Please go under http://opendmk.dev.java.net and set the opendmk-jarfile configuration parameter to set the full path of the required jdmkrt.jar file. The SNMP connection Handler didn't started.

ID: 1465

Severity: ERROR

Message: Cannot initialize the SNMP Connection Handler. Please check the configuration attributes.

ID: 1466

Severity: ERROR

Message: No valid trap destinations has been found. No trap will be sent.

ID: 1503

Severity: ERROR

Message: Cannot decode the provided subtree delete control because it contains a value.

ID: 1504

Severity: ERROR

Message: An error occurred while attempting to initialize the SSL context for use in the LDAP Connection Handler: %s.

ID: 1505

Severity: ERROR

Message: The Directory Server does not support LDAP protocol version %d. This connection will be closed.

ID: 1506

Severity: ERROR

Message: The specified OpenDMK jar file '%s' could not be found. Verify that the value set in the opendmk-jarfile configuration parameter of the SNMP connection handler is the valid path to the jdmkrt.jar file and that the file is accessible.

ID: 1507

Severity: ERROR

Message: The required classes could not be loaded using jar file '%s'. Verify that the jar file is not corrupted.

ID: 1508

Severity: ERROR

Message: Cannot decode the provided control %s because an error occurred while attempting to decode the control value: %s.

ID: 1509

Severity: ERROR

Message: Cannot decode the provided entry changelog notification control because it does not have a value.

ID: 1510

Severity: ERROR

Message: Cannot decode the provided entry changelog notification control because an error occurred while attempting to decode the control value: %s.

ID: 1511

Severity: ERROR

Message: The connection to the Directory Server was closed while waiting for a response.

ID: 1513

Severity: ERROR

Message: An IO error occurred while reading a request from the client: %s.

ID: 1514

Severity: ERROR

Message: Connection reset by client.

ID: 1516

Severity: ERROR

Message: The server received configuration changes that require a restart of the %s connection handler to take effect.

ID: 1517

Severity: ERROR

Message: The GSER value does not contain a String matching the pattern %s at the current position: %s.

ID: 1518

Severity: ERROR

Message: The GSER value does not contain a separator at the current position: %s.

ID: 1519

Severity: ERROR

Message: The GSER value does not contain a valid String value at the current position: %s.

ID: 1520

Severity: ERROR

Message: The GSER value does not contain a valid integer value at the current position: %s.

ID: 1521

Severity: ERROR

Message: The GSER value does not contain a valid identifier at the current position: %s.

ID: 1522

Severity: ERROR

Message: The GSER value does not contain a whitespace character at the current position: %s.

ID: 1523

Severity: ERROR

Message: The GSER value does not contain a valid IdentifiedChoiceValue at the current position: %s.

ID: 1524

Severity: ERROR

Message: The keystore %s seems to be missing, this may render the secure port inoperative for '%s'. Verify the keystore setting in the configuration.

ID: 1525

Severity: ERROR

Message: Authorization as '%s' specified in the proxied authorization control is not permitted.

ID: 1526

Severity: ERROR

Message: The key with alias '%s' was not found for '%s'. Verify that the keystore is properly configured.

ID: 1527

Severity: ERROR

Message: No usable key was found for '%s'. Verify the keystore content.

ID: 1529

Severity: ERROR

Message: Failed to initialize Http Connection Handler.

ID: 1530

Severity: ERROR

Message: No value was provided for the transaction id control, whereas an UTF-8 encoded value is expected.

ID: 1531

Severity: ERROR

Message: Exception on the underlying client connection: %s.

ID: 1532

Severity: ERROR

Message: The underlying client connection timed out or closed: %s.

ID: 1533

Severity: ERROR

Message: Use of the proxied authorization V2 control for user %s is not allowed: the account is disabled.

ID: 1534

Severity: ERROR

Message: Use of the proxied authorization V2 control for user %s is not allowed: the account is expired.

ID: 1535

Severity: ERROR

Message: Use of the proxied authorization V2 control for user %s is not allowed: the account is locked.

ID: 1536

Severity: ERROR

Message: Use of the proxied authorization V2 control for user %s is not allowed: the account's password is expired.

Log Message Category: QUICKSETUP

ID: N/A

Severity: ERROR

Message: The registration information of server %s and server %s could not be merged. Reasons:%n%s.

Log Message Category: REPLICATION

ID: 1

Severity: ERROR

Message: The configured DN is already used by another domain.

ID: 5

Severity: ERROR

Message: Replication Server failed to start because the hostname is unknown.

ID: 6

Severity: ERROR

Message: Replication Server failed to start : could not bind to the listen port : %d. Error : %s.

ID: 7

Severity: ERROR

Message: Unknown operation type : %s.

ID: 9

Severity: ERROR

Message: Internal Error : Operation %s change number %s was not found in pending list.

ID: 11

Severity: ERROR

Message: The replication server failed to start because the database %s could not be read : %s.

ID: 12

Severity: ERROR

Message: An Exception was caught while replaying operation %s : %s.

ID: 15

Severity: ERROR

Message: Error %s when searching for server state %s : %s base dn : %s.

ID: 20

Severity: ERROR

Message: Caught IOException while sending topology info (for update) on domain %s for %s server %s : %s.

ID: 21

Severity: ERROR

Message: Error when searching old changes from the database for base DN %s.

ID: 25

Severity: ERROR

Message: Error trying to replay %s, operation could not be decoded :.

ID: 26

Severity: ERROR

Message: Error trying to use the underlying database. The Replication Server is going to shut down: %s.

ID: 29

Severity: ERROR

Message: Error during the Replication Server database trimming or flush process. The Changelog service is going to shutdown: %s.

ID: 32

Severity: ERROR

Message: An unexpected error happened handling connection with %s. This connection is going to be closed.

ID: 33

Severity: ERROR

Message: In replication server %s: an unexpected error occurred while sending an ack to server id %s for change number %s in domain %s . This connection is going to be closed and reopened.

ID: 35

Severity: ERROR

Message: A loop was detected while replaying operation: %s error %s.

ID: 36

Severity: ERROR

Message: An Exception was caught while testing existence or trying to create the directory for the Replication Server database : %s.

ID: 44

Severity: ERROR

Message: The current request is rejected due to an import or an export already in progress for the same data.

ID: 45

Severity: ERROR

Message: On domain %s, initialization of server with serverId:%s has been requested from a server with an invalid serverId:%s. %s.

ID: 46

Severity: ERROR

Message: Invalid target for the export.

ID: 47

Severity: ERROR

Message: Domain %s: the server with serverId=%s is unreachable.

ID: 48

Severity: ERROR

Message: No domain matches the provided base DN '%s'.

ID: 49

Severity: ERROR

Message: Multiple domains match the base DN provided.

ID: 50

Severity: ERROR

Message: The provider class does not allow the operation requested.

ID: 51

Severity: ERROR

Message: The hostname %s could not be resolved as an IP address.

ID: 54

Severity: ERROR

Message: In Replication server %s: servers %s and %s have the same ServerId : %d.

ID: 55

Severity: ERROR

Message: In Replication server %s: replication servers %s and %s have the same ServerId : %d.

ID: 56

Severity: ERROR

Message: Entry %s was containing some unknown historical information, This may cause some inconsistency for this entry.

ID: 57

Severity: ERROR

Message: A conflict was detected but the conflict information could not be added. Operation: %s, Result: %s.

ID: 58

Severity: ERROR

Message: An error happened trying to rename a conflicting entry. DN: %s, Operation: %s, Result: %s.

ID: 61

Severity: ERROR

Message: The Replication is configured for suffix %s but was not able to connect to any Replication Server.

ID: 65

Severity: ERROR

Message: An unexpected error occurred while sending an Error Message to %s. This connection is going to be closed and reopened.

ID: 66

Severity: ERROR

Message: An unexpected error occurred while sending a Message to %s. This connection is going to be closed and reopened.

ID: 67

Severity: ERROR

Message: Could not replay operation %s with ChangeNumber %s error %s %s.

ID: 68

Severity: ERROR

Message: The entry %s has historical information for attribute %s which is not defined in the schema. This information will be ignored.

ID: 70

Severity: ERROR

Message: The Replication Server socket could not be closed : %s.

ID: 71

Severity: ERROR

Message: The thread listening on the replication server port could not be stopped : %s.

ID: 73

Severity: ERROR

Message: An unexpected error occurred when searching for generation id for domain "%s": %s.

ID: 74

Severity: ERROR

Message: An unexpected error occurred when looking for the replicated backend : %s. It may be not configured or disabled.

ID: 75

Severity: ERROR

Message: An unexpected error occurred when searching in %s for the generation ID : %s.

ID: 76

Severity: ERROR

Message: An unexpected error occurred when updating generation ID for domain "%s": %s.

ID: 79

Severity: ERROR

Message: The following error has been received : %s.

ID: 82

Severity: ERROR

Message: Initialization cannot be done because import is not supported by the backend %s.

ID: 83

Severity: ERROR

Message: Initialization cannot be done because export is not supported by the backend %s.

ID: 84

Severity: ERROR

Message: Initialization cannot be done because the following error occurred while locking the backend %s : %s.

ID: 86

Severity: ERROR

Message: Replication server caught exception while listening for client connections %s.

ID: 87

Severity: ERROR

Message: While clearing the database %s , the following error happened: %s.

ID: 89

Severity: ERROR

Message: An unexpected error occurred when testing existence or creating the replication backend : %s.

ID: 93

Severity: ERROR

Message: An error occurred when searching for %s : %s.

ID: 95

Severity: ERROR

Message: The base DN %s is not stored by any of the Directory Server backend.

ID: 107

Severity: ERROR

Message: Monitor data of remote servers are missing due to a processing error : %s.

ID: 108

Severity: ERROR

Message: Unable to send monitor data request for domain "%s" to replication server RS(%d) due to the following error: %s.

ID: 109

Severity: ERROR

Message: An Exception was caught while replaying replication message : %s.

ID: 114

Severity: ERROR

Message: Caught exception publishing fake operations for domain %s : %s.

ID: 115

Severity: ERROR

Message: Caught exception computing fake operations for domain %s for replication server %s : %s.

ID: 118

Severity: ERROR

Message: For replicated domain %s, in server with serverId=%s, the generation ID could not be set to value %s in the rest of the topology because this server is NOT connected to any replication

server. You should check in the configuration that the domain is enabled and that there is one replication server up and running.

ID: 121

Severity: ERROR

Message: DN sent by remote replication server: %s does not match local replication server one: %s.

ID: 122

Severity: ERROR

Message: DN sent by replication server: %s does not match local directory server one: %s.

ID: 123

Severity: ERROR

Message: Caught IOException while forwarding ResetGenerationIdMsg to peer replication servers for domain %s : %s.

ID: 124

Severity: ERROR

Message: Computed invalid initial status: %s in DS replication domain %s with server id %s.

ID: 125

Severity: ERROR

Message: Replication server received invalid initial status: %s for replication domain %s from server id %s.

ID: 126

Severity: ERROR

Message: Received invalid requested status %s in DS replication domain %s with server id %s.

ID: 127

Severity: ERROR

Message: Could not compute new status in RS replication domain %s for server id %s. Was in %s status and received %s event.

ID: 128

Severity: ERROR

Message: Could not compute new status in DS replication domain %s with server id %s. Was in %s status and received %s event.

ID: 129

Severity: ERROR

Message: Caught IOException while changing status for domain %s and serverId: %s after reset for generation id: %s.

ID: 130

Severity: ERROR

Message: Received change status message does not come from a directory server (dn: %s, server id: %s, msg: %s).

ID: 132

Severity: ERROR

Message: Received invalid new status %s in RS for replication domain %s and directory server id %s.

ID: 134

Severity: ERROR

Message: Replication broker with dn %s and server id %s failed to signal status change because of: %s.

ID: 139

Severity: ERROR

Message: Caught IOException while changing status for domain %s and serverId: %s from status analyzer: %s.

ID: 149

Severity: ERROR

Message: In directory server %s, received unknown assured update mode: %s, for domain %s. Message: %s.

ID: 150

Severity: ERROR

Message: In replication server %s, received unknown assured update mode: %s, for domain %s. Message: %s.

ID: 151

Severity: ERROR

Message: In replication server %s, received a safe data assured update message with incoherent level: %s, this is for domain %s. Message: %s.

ID: 152

Severity: ERROR

Message: The generation ID could not be reset for domain %s.

ID: 154

Severity: ERROR

Message: The Replication was not started on base-dn %s : %s.

ID: 157

Severity: ERROR

Message: Replication protocol error. Bad message type. %s received, %s required.

ID: 159

Severity: ERROR

Message: The Server Handler byte count is not correct Byte Count=%s (Fixed).

ID: 168

Severity: ERROR

Message: The fractional replication ldif import plugin is configured with invalid plugin type %s. Only the ldifImport plugin type is allowed.

ID: 173

Severity: ERROR

Message: An error occurred when accessing the change number database : %s.

ID: 174

Severity: ERROR

Message: The initialization failed because the domain %s is not connected to a replication server.

ID: 175

Severity: ERROR

Message: Could not retrieve the configuration for a replication domain matching the entry %s.

ID: 178

Severity: ERROR

Message: Directory server %s was attempting to connect to replication server %s but has disconnected in handshake phase. Error: %s.

ID: 179

Severity: ERROR

Message: Replication server %s was attempting to connect to replication server %s but has disconnected in handshake phase. Error: %s.

ID: 181

Severity: ERROR

Message: The connection from this replication server RS(%d) to replication server RS(%d) at %s for domain "%s" has failed.

ID: 185

Severity: ERROR

Message: Full resync required. Reason: The provided cookie contains unknown replicated domain %s. Current starting cookie <%s>.

ID: 186

Severity: ERROR

Message: Full resync required. Reason: The provided cookie is older than the start of historical in the server for the replicated domain : %s.

ID: 187

Severity: ERROR

Message: Invalid syntax for the provided cookie '%s'.

ID: 189

Severity: ERROR

Message: Domain %s (server id: %s) : remote exporter server disconnection (server id: %s) detected during initialization.

ID: 190

Severity: ERROR

Message: During initialization from a remote server, the following error occurred : %s.

ID: 191

Severity: ERROR

Message: Connection failure with Replication Server %s during import.

ID: 192

Severity: ERROR

Message: Bad msg id sequence during import. Expected:%s Actual:%s.

ID: 193

Severity: ERROR

Message: The following servers did not acknowledge initialization in the expected time for domain %s. They are potentially down or too slow. Servers list: %s.

ID: 194

Severity: ERROR

Message: The following servers did not end initialization being connected with the right generation (%s). They are potentially stopped or too slow. Servers list: %s.

ID: 195

Severity: ERROR

Message: When initializing remote server(s), connection to Replication Server with serverId=%s is lost.

ID: 196

Severity: ERROR

Message: When initializing remote server(s), the initialized server with serverId=%s is potentially stopped or too slow.

ID: 197

Severity: ERROR

Message: When sending a new initialization request for an initialization from a remote server, the following error occurred %s. The initial error was : %s.

ID: 201

Severity: ERROR

Message: Processing two different changes with same CSN=%s. Previous msg=<%s>, New msg=<%s>.

ID: 202

Severity: ERROR

Message: Error while trying to solve conflict with DN : %s ERROR : %s.

ID: 211

Severity: ERROR

Message: The connection from this replication server RS(%d) to directory server DS(%d) at %s for domain "%s" has failed.

ID: 216

Severity: ERROR

Message: %s was interrupted in the startup phase.

ID: 235

Severity: ERROR

Message: Could not create replica database because the changelog database is shutting down.

ID: 236

Severity: ERROR

Message: An unexpected error forced the %s thread to shutdown: %s. The changeNumber attribute will not move forward anymore. You can reenable this thread by first setting the "compute-change-number" property to false and then back to true.

ID: 240

Severity: ERROR

Message: Could not add change %s to replicaDB %s %s because flushing thread is shutting down.

ID: 243

Severity: ERROR

Message: Error when retrieving changelog state from root path '%s' : IO error on domain directory '%s' when retrieving list of server ids.

ID: 244

Severity: ERROR

Message: Could not get or create replica DB for baseDN '%s', serverId '%d', generationId '%d': %s.

ID: 245

Severity: ERROR

Message: Could not get or create change number index DB in root path '%s', using path '%s'.

ID: 246

Severity: ERROR

Message: Could not retrieve generation id file '%s' for DN '%s' to delete it.

ID: 247

Severity: ERROR

Message: Could not create directory '%s' for server id %d.

ID: 248

Severity: ERROR

Message: Could not create generation id file '%s'.

ID: 250

Severity: ERROR

Message: Could not read server id filename because it uses a wrong format, expecting '[id].server' where [id] is numeric but got '%s'.

ID: 251

Severity: ERROR

Message: Could not read generation id because it uses a wrong format, expecting a number but got '%s'.

ID: 252

Severity: ERROR

Message: Could not open log file '%s' for write.

ID: 253

Severity: ERROR

Message: Could not open a reader on log file '%s'.

ID: 254

Severity: ERROR

Message: Could not decode a record from data read in log file '%s'.

ID: 255

Severity: ERROR

Message: Could not delete log file '%s'.

ID: 256

Severity: ERROR

Message: Could not create log file '%s'.

ID: 258

Severity: ERROR

Message: Could not add record '%s' in log file '%s'.

ID: 259

Severity: ERROR

Message: Could not synchronize written records to file system for log file '%s'.

ID: 260

Severity: ERROR

Message: Could not seek to position %d for reader on log file '%s'.

ID: 261

Severity: ERROR

Message: Could not create root directory '%s' for log file.

ID: 262

Severity: ERROR

Message: Could not decode DN from domain state file '%s', from line '%s'.

ID: 263

Severity: ERROR

Message: Could not read domain state file '%s'.

ID: 264

Severity: ERROR

Message: There is a mismatch between domain state file and actual domain directories found in file system. Expected domain ids : '%s'. Actual domain ids found in file system: '%s'.

ID: 265

Severity: ERROR

Message: Could not create a new domain id %s for domain DN %s and save it in domain state file '%s".

ID: 266

Severity: ERROR

Message: Could not get reader position for cursor in log file '%s'.

ID: 267

Severity: ERROR

Message: Could not decode the key from string [%s].

ID: 269

Severity: ERROR

Message: When closing log '%s', found %d cursor(s) still opened on the log.

ID: 270

Severity: ERROR

Message: Could not initialize the log '%s'.

ID: 271

Severity: ERROR

Message: Could not retrieve key bounds from log file '%s'.

ID: 272

Severity: ERROR

Message: Could not retrieve read-only log files from log '%s'.

ID: 273

Severity: ERROR

Message: While purging log, could not delete log file(s): '%s'.

ID: 274

Severity: ERROR

Message: The following log '%s' must be released but it is not referenced.

ID: 275

Severity: ERROR

Message: Could not rename head log file from '%s' to '%s'.

ID: 278

Severity: ERROR

Message: Could not write offline replica information for domain %s and server id %d, using path '%s' (offline CSN is %s).

ID: 279

Severity: ERROR

Message: Could not read replica offline state file '%s' for domain %s, it should contain exactly one line corresponding to the offline CSN.

ID: 280

Severity: ERROR

Message: Could not read content of replica offline state file '%s' for domain %s.

ID: 281

Severity: ERROR

Message: Could not delete replica offline state file '%s' for domain %s and server id %d.

ID: 282

Severity: ERROR

Message: Could not retrieve file length of log file '%s'.

ID: 283

Severity: ERROR

Message: An error occurred while recovering the replication change log file '%s'. The recovery has been aborted and this replication server will be removed from the replication topology. The change log file system may be read-only, full, or corrupt and must be fixed before this

replication server can be used. The underlying error was: %s.

ID: 286

Severity: ERROR

Message: An error occurred when searching base DN '%s' with filter '%s' in changelog backend : %s.

ID: 287

Severity: ERROR

Message: An error occurred when retrieving attribute value for attribute '%s' for entry DN '%s' in changelog backend : %s.

ID: 288

Severity: ERROR

Message: Could not create file '%s' to store last log rotation time %d.

ID: 289

Severity: ERROR

Message: Could not delete file '%s' that stored the previous last log rotation time.

ID: 290

Severity: ERROR

Message: Cursor on log '%s' has been aborted after a purge or a clear.

ID: 291

Severity: ERROR

Message: Could not position and read newest record from log file '%s'.

ID: 293

Severity: ERROR

Message: The change number index could not be reset to start with %d in base DN '%s' because starting CSN '%s' does not exist in the change log.

ID: 294

Severity: ERROR

Message: The change number could not be reset to %d because the associated change with CSN '%s' has already been purged from the change log. Try resetting to a more recent change.

ID: 295

Severity: ERROR

Message: Change number indexing is disabled for replication domain '%s'.

ID: 297

Severity: ERROR

Message: Cannot decode change-log record with version %x.

ID: 300

Severity: ERROR

Message: New replication connection from %s started with unexpected message %s and is being closed.

ID: 305

Severity: ERROR

Message: Invalid operator '%s' specified in historicalCsnRangeMatch extensible matching rule assertion.

ID: 306

Severity: ERROR

Message: Specified assertion '%s' for historicalCsnRangeMatch extensible matching rule does not conform to expected syntax. The assertion must specify a CSN range.

ID: 307

Severity: ERROR

Message: Specified CSNs '%s' and '%s' have two different server ids. The historicalCsnRangeMatch extensible matching rule requires CSNs to have the same server id.

ID: 308

Severity: ERROR

Message: Specified operators '%s' and '%s' do not specify a range for historicalCsnRangeMatch extensible matching rule.

ID: 309

Severity: ERROR

Message: Could not restart the Replication Server, bind to listen port %d failed : %s.

ID: 310

Severity: ERROR

Message: The replication server has detected that the file system containing the changelog is full. In order to prevent further problems, the replication server will disconnect from the replication topology and wait for sufficient disk space to be recovered, at which point it will reconnect.

Log Message Category: SCHEMA

ID: 26

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because the last non-space character was a comma or semicolon.

ID: 28

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because character '%c' at position %d is not allowed in an attribute name.

ID: 29

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because the underscore character is not allowed in an attribute name unless the %s configuration option is enabled.

ID: 30

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because the hyphen character is not allowed as the first character of an attribute name.

ID: 31

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because the underscore character is not allowed as the first character of an attribute name even if the %s configuration option is enabled.

ID: 32

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because the digit '%c' is not allowed as the first character of an attribute name unless the name is specified as an OID or the %s configuration option is enabled.

ID: 33

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because it contained an RDN containing an empty attribute name.

ID: 34

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because the parsed attribute name %s included a period but that name did not appear to be a valid OID.

ID: 35

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because the last non-space character was part of the attribute name '%s'.

ID: 36

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because the next non-space character after attribute name "%s" should have been an equal sign but instead was '%c'.

ID: 37

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because character '%c' at position %d is not valid.

ID: 38

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because an attribute value started with an octothorpe (#) but was not followed by a positive multiple of two hexadecimal digits.

ID: 39

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because an attribute value started with an octothorpe (#) but contained a character %c that was not a valid hexadecimal digit.

ID: 40

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because an unexpected failure occurred while attempting to parse an attribute value from one of the RDN components: "%s".

ID: 41

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because one of the RDN components included a quoted value that did not have a corresponding closing quotation mark.

ID: 42

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because one of the RDN components included a value with an escaped hexadecimal digit that was not followed by a second hexadecimal digit.

ID: 52

Severity: ERROR

Message: The provided value could not be parsed as a valid attribute type description because it was empty or contained only whitespace.

ID: 69

Severity: ERROR

Message: The provided value could not be parsed as a valid objectclass description because it was empty or contained only whitespace.

ID: 70

Severity: ERROR

Message: The provided value "%s" could not be parsed as an objectclass description because an open parenthesis was expected at position %d but instead a '%s' character was found.

ID: 71

Severity: ERROR

Message: The provided value "%s" could not be parsed as an objectclass description because the end of the value was encountered while the Directory Server expected more data to be provided.

ID: 72

Severity: ERROR

Message: The provided value "%s" could not be parsed as an objectclass description because the numeric OID contained two consecutive periods at position %d.

ID: 73

Severity: ERROR

Message: The provided value "%s" could not be parsed as an objectclass description because the numeric OID contained an illegal character %s at position %d.

ID: 74

Severity: ERROR

Message: The provided value "%s" could not be parsed as an objectclass description because the non-numeric OID contained an illegal character %s at position %d.

ID: 75

Severity: ERROR

Message: The provided value "%s" could not be parsed as an objectclass description because it

contained an illegal character %s at position %d.

ID: 76

Severity: ERROR

Message: The provided value "%s" could not be parsed as an objectclass description because it contained an unexpected closing parenthesis at position %d.

ID: 119

Severity: ERROR

Message: The provided value could not be parsed as a valid DIT content rule description because it was empty or contained only whitespace.

ID: 120

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT content rule description because an open parenthesis was expected at position %d but instead a '%s' character was found.

ID: 121

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT content rule description because the end of the value was encountered while the Directory Server expected more data to be provided.

ID: 122

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT content rule description because the numeric OID contained two consecutive periods at position %d.

ID: 123

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT content rule description because the numeric OID contained an illegal character %s at position %d.

ID: 124

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT content rule description because the non-numeric OID contained an illegal character %s at position %d.

ID: 125

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT content rule description because it contained an unexpected closing parenthesis at position %d.

ID: 126

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT content rule description because it contained an illegal character %s at position %d.

ID: 127

Severity: ERROR

Message: The DIT content rule "%s" is associated with a structural objectclass %s that is not defined in the server schema.

ID: 128

Severity: ERROR

Message: The DIT content rule "%s" is associated with the objectclass with OID %s (%s). This objectclass exists in the server schema but is defined as %s rather than structural.

ID: 129

Severity: ERROR

Message: The DIT content rule "%s" is associated with an auxiliary objectclass %s that is not defined in the server schema.

ID: 130

Severity: ERROR

Message: The DIT content rule "%s" is associated with an auxiliary objectclass %s. This objectclass exists in the server schema but is defined as %s rather than auxiliary.

ID: 131

Severity: ERROR

Message: The DIT content rule "%s" is associated with a required attribute type %s that is not defined in the server schema.

ID: 132

Severity: ERROR

Message: The DIT content rule "%s" is associated with an optional attribute type %s that is not defined in the server schema.

ID: 133

Severity: ERROR

Message: The DIT content rule "%s" is associated with a prohibited attribute type %s that is not defined in the server schema.

ID: 134

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT content rule description because a single quote was expected at position %d but the %s character was found instead.

ID: 135

Severity: ERROR

Message: The provided value could not be parsed as a valid name form description because it was empty or contained only whitespace.

ID: 136

Severity: ERROR

Message: The provided value "%s" could not be parsed as a name form description because an open parenthesis was expected at position %d but instead a '%c' character was found.

ID: 137

Severity: ERROR

Message: The provided value "%s" could not be parsed as a name form description because the end of the value was encountered while the Directory Server expected more data to be provided.

ID: 138

Severity: ERROR

Message: The provided value "%s" could not be parsed as a name form description because the numeric OID contained two consecutive periods at position %d.

ID: 139

Severity: ERROR

Message: The provided value "%s" could not be parsed as a name form description because the numeric OID contained an illegal character %c at position %d.

ID: 140

Severity: ERROR

Message: The provided value "%s" could not be parsed as a name form description because the non-numeric OID contained an illegal character %c at position %d.

ID: 141

Severity: ERROR

Message: The provided value "%s" could not be parsed as a name form description because it contained an unexpected closing parenthesis at position %d.

ID: 142

Severity: ERROR

Message: The provided value "%s" could not be parsed as a name form description because it contained an illegal character %c at position %d.

ID: 143

Severity: ERROR

Message: The name form description "%s" is associated with a structural objectclass %s that is not defined in the server schema.

ID: 144

Severity: ERROR

Message: The name form description "%s" is associated with the objectclass with OID %s (%s). This objectclass exists in the server schema but is defined as %s rather than structural.

ID: 145

Severity: ERROR

Message: The definition for the name form with OID %s declared that it should include required attribute "%s". No attribute type matching this name or OID exists in the server schema.

ID: 146

Severity: ERROR

Message: The definition for the name form with OID %s declared that it should include optional attribute "%s". No attribute type matching this name or OID exists in the server schema.

ID: 147

Severity: ERROR

Message: The provided value "%s" could not be parsed as a name form description because it does not specify the structural objectclass with which it is associated.

ID: 148

Severity: ERROR

Message: The provided value "%s" could not be parsed as a name form description because a single quote was expected at position %d but the %c character was found instead.

ID: 160

Severity: ERROR

Message: The provided value could not be parsed as a valid matching rule use description because it was empty or contained only whitespace.

ID: 161

Severity: ERROR

Message: The provided value "%s" could not be parsed as a matching rule use description because an open parenthesis was expected at position %d but instead a '%s' character was found.

ID: 162

Severity: ERROR

Message: The provided value "%s" could not be parsed as a matching rule use description because the end of the value was encountered while the Directory Server expected more data to be provided.

ID: 163

Severity: ERROR

Message: The provided value "%s" could not be parsed as a matching rule use description because the numeric OID contained two consecutive periods at position %d.

ID: 164

Severity: ERROR

Message: The provided value "%s" could not be parsed as a matching rule use description because the numeric OID contained an illegal character %s at position %d.

ID: 165

Severity: ERROR

Message: The provided value "%s" could not be parsed as a matching rule use description because the non-numeric OID contained an illegal character %s at position %d.

ID: 166

Severity: ERROR

Message: The provided value "%s" could not be parsed as a matching rule use description because the specified matching rule %s is unknown.

ID: 167

Severity: ERROR

Message: The provided value "%s" could not be parsed as a matching rule use description because it contained an unexpected closing parenthesis at position %d.

ID: 168

Severity: ERROR

Message: The provided value "%s" could not be parsed as a matching rule use description because it contained an illegal character %s at position %d.

ID: 169

Severity: ERROR

Message: The matching rule use description "%s" is associated with attribute type %s that is not defined in the server schema.

ID: 170

Severity: ERROR

Message: The provided value "%s" could not be parsed as a matching rule description because it does not specify the set of attribute types that may be used with the associated OID.

ID: 171

Severity: ERROR

Message: The provided value "%s" could not be parsed as a matching rule use description because a single quote was expected at position %d but the %s character was found instead.

ID: 172

Severity: ERROR

Message: The provided value could not be parsed as a valid DIT structure rule description because it was empty or contained only whitespace.

ID: 173

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT structure rule description because an open parenthesis was expected at position %d but instead a '%s' character was found.

ID: 174

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT structure rule description because the end of the value was encountered while the Directory Server expected more data to be provided.

ID: 175

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT structure rule description because the rule ID contained an illegal character %s at position %d.

ID: 176

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT structure rule description because it contained an unexpected closing parenthesis at position %d.

ID: 177

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT structure rule description because it contained an illegal character %s at position %d.

ID: 178

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT structure rule description because it referenced an unknown name form %s.

ID: 179

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT structure rule description because it referenced an unknown rule ID %d for a superior DIT structure rule.

ID: 180

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT structure rule description because it did not specify the name form for the rule.

ID: 181

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT structure rule description because a single quote was expected at position %d but the %s character was found instead.

ID: 182

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT structure rule description because the numeric OID contained two consecutive periods at position %d.

ID: 183

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT structure rule description because the numeric OID contained an illegal character %s at position %d.

ID: 184

Severity: ERROR

Message: The provided value "%s" could not be parsed as a DIT structure rule description because the non-numeric OID contained an illegal character %s at position %d.

ID: 206

Severity: ERROR

Message: The provided value "%s" could not be parsed as a guide value because the criteria portion %s contained an illegal character %c at position %d.

ID: 207

Severity: ERROR

Message: The provided value "%s" could not be parsed as a guide value because the criteria portion %s did not contain a close parenthesis that corresponded to the initial open parenthesis.

ID: 208

Severity: ERROR

Message: The provided value "%s" could not be parsed as a guide value because the criteria portion %s started with a question mark but was not followed by the string "true" or "false".

ID: 209

Severity: ERROR

Message: The provided value "%s" could not be parsed as a guide value because the criteria portion %s did not contain a dollar sign to separate the attribute type from the match type.

ID: 210

Severity: ERROR

Message: The provided value "%s" could not be parsed as a guide value because the criteria portion %s did not specify an attribute type before the dollar sign.

ID: 211

Severity: ERROR

Message: The provided value "%s" could not be parsed as a guide value because the criteria portion %s did not specify a match type after the dollar sign.

ID: 212

Severity: ERROR

Message: The provided value "%s" could not be parsed as a guide value because the criteria portion %s had an invalid match type starting at position %d.

ID: 243

Severity: ERROR

Message: The provided authPassword value had an invalid scheme character at position %d.

ID: 244

Severity: ERROR

Message: The provided authPassword value had a zero-length scheme element.

ID: 245

Severity: ERROR

Message: The provided authPassword value was missing the separator character or had an illegal character between the scheme and authInfo elements.

ID: 246

Severity: ERROR

Message: The provided authPassword value had an invalid authInfo character at position %d.

ID: 247

Severity: ERROR

Message: The provided authPassword value had a zero-length authInfo element.

ID: 248

Severity: ERROR

Message: The provided authPassword value was missing the separator character or had an illegal character between the authInfo and authValue elements.

ID: 253

Severity: ERROR

Message: No value was given to decode by the user password attribute syntax.

ID: 254

Severity: ERROR

Message: Unable to decode the provided value according to the user password syntax because the value does not start with the opening curly brace ("{") character.

ID: 255

Severity: ERROR

Message: Unable to decode the provided value according to the user password syntax because the value does not contain a closing curly brace ("}") character.

ID: 256

Severity: ERROR

Message: Unable to decode the provided value according to the user password syntax because the value does not contain a storage scheme name.

ID: 257

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid RFC 3672 subtree specification.

ID: 261

Severity: ERROR

Message: The provided authPassword value had an invalid authValue character at position %d.

ID: 262

Severity: ERROR

Message: The provided authPassword value had a zero-length authValue element.

ID: 263

Severity: ERROR

Message: The provided authPassword value had an invalid trailing character at position %d.

ID: 269

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid subtree specification.

ID: 271

Severity: ERROR

Message: The DIT content rule "%s" is not valid because it prohibits the use of attribute type %s which is required by the associated structural object class %s.

ID: 272

Severity: ERROR

Message: The DIT content rule "%s" is not valid because it prohibits the use of attribute type %s which is required by the associated auxiliary object class %s.

ID: 282

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid distinguished name because an attribute value started with a character at position %d that needs to be escaped.

ID: 288

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid object class definition because character '%c' at position %d is not allowed in an object class name.

ID: 289

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid object class definition because the underscore character is not allowed in an object class name unless the %s configuration option is enabled.

ID: 290

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid object class definition because

the hyphen character is not allowed as the first character of an object class name.

ID: 291

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid object class definition because the underscore character is not allowed as the first character of an object class name even if the %s configuration option is enabled.

ID: 292

Severity: ERROR

Message: The provided value "%s" could not be parsed as a valid object class definition because the digit '%c' is not allowed as the first character of an object class name unless the name is specified as an OID or the %s configuration option is enabled.

ID: 306

Severity: ERROR

Message: The provided value "%s" could not be parsed as an ldap syntax because it contains an unrecognized extension %s at position %d.

ID: 317

Severity: ERROR

Message: The provided value could not be parsed as a valid ldap syntax description because it was empty or contained only whitespace.

ID: 318

Severity: ERROR

Message: The provided value "%s" could not be parsed as an ldap syntax description because an open parenthesis was expected at position %d but instead a '%s' character was found.

ID: 319

Severity: ERROR

Message: The provided value "%s" could not be parsed as an ldap syntax description because the end of the value was encountered while the Directory Server expected more data to be provided.

ID: 320

Severity: ERROR

Message: The provided value "%s" could not be parsed as an ldap syntax description because the numeric OID contained two consecutive periods at position %d.

ID: 321

Severity: ERROR

Message: The provided value "%s" could not be parsed as an ldap syntax description because the

numeric OID contained an illegal character %s at position %d.

ID: 322

Severity: ERROR

Message: The provided value "%s" could not be parsed as an ldap syntax description because the non-numeric OID contained an illegal character %s at position %d.

ID: 323

Severity: ERROR

Message: The provided value "%s" could not be parsed as an ldap syntax description because it contained an unexpected closing parenthesis at position %d.

ID: 324

Severity: ERROR

Message: The provided value "%s" could not be parsed as an ldap syntax description because it contains more than one form of constructor.

ID: 325

Severity: ERROR

Message: The definition for the ldap syntax with OID %s declared that it’s a substitute for a syntax with OID %s. No such syntax is configured for use in the Directory Server.

ID: 326

Severity: ERROR

Message: The provided value "%s" could not be parsed as an enumeration syntax, because there is no value.

ID: 327

Severity: ERROR

Message: The provided value "%s" could not be parsed as an ldap syntax extension because an invalid character was found at position %d.

ID: 329

Severity: ERROR

Message: The provided value "%s" could not be parsed as an ldap syntax description because a single quote was expected at position %d but the character %s was found instead.

ID: 334

Severity: ERROR

Message: The provided value "%s" is not safe for X-SCHEMA-FILE.

ID: 340

Severity: ERROR

Message: Attribute type could not be registered from definition: %s.

ID: 341

Severity: ERROR

Message: There should be no warnings on the schema, but instead got %d warnings: %s.

ID: 342

Severity: ERROR

Message: Matching rule use could not be registered from definition: %s.

ID: 343

Severity: ERROR

Message: Object class could not be registered from definition: %s.

ID: 344

Severity: ERROR

Message: Unable to parse the OID from the provided definition of objectclass: '%s'.

ID: 345

Severity: ERROR

Message: Unable to parse the OID from the provided definition of attribute type: '%s'.

ID: 346

Severity: ERROR

Message: Unable to parse the OID from the provided definition of ldap syntax: '%s'.

ID: 347

Severity: ERROR

Message: Unable to parse the OID from the provided definition of matching rule use: '%s' .

ID: 348

Severity: ERROR

Message: DIT content rule could not be registered from definition: %s.

ID: 349

Severity: ERROR

Message: Name form could not be registered from definition: %s.

ID: 350

Severity: ERROR

Message: Unable to parse the OID from the provided definition of name form: '%s'.

ID: 351

Severity: ERROR

Message: Unable to parse the OID from the provided definition of DIT content rule: '%s'.

ID: 352

Severity: ERROR

Message: Unable to parse the rule ID from the provided definition of DIT structure rule: '%s' .

Log Message Category: TASK

ID: 1

Severity: ERROR

Message: The task could not enable a backend: %s.

ID: 2

Severity: ERROR

Message: The task could not disable a backend: %s.

ID: 5

Severity: ERROR

Message: Unable to add one or more files to the server schema because no schema file names were provided in attribute %s of task entry %s.

ID: 6

Severity: ERROR

Message: Unable to add one or more files to the server schema because the specified schema file %s does not exist in schema directory %s.

ID: 7

Severity: ERROR

Message: Unable to add one or more files to the server schema because an error occurred while attempting to determine whether file %s exists in schema directory %s: %s.

ID: 8

Severity: ERROR

Message: An error occurred while attempting to load the contents of schema file %s into the server schema: %s.

ID: 9

Severity: ERROR

Message: Unable to add one or more files to the server schema because the server was unable to obtain a write lock on the schema entry %s after multiple attempts.

ID: 10

Severity: ERROR

Message: You do not have sufficient privileges to modify the server schema.

ID: 11

Severity: ERROR

Message: You do not have sufficient privileges to initiate a Directory Server backup.

ID: 12

Severity: ERROR

Message: You do not have sufficient privileges to initiate a Directory Server restore.

ID: 13

Severity: ERROR

Message: You do not have sufficient privileges to initiate an LDIF import.

ID: 14

Severity: ERROR

Message: You do not have sufficient privileges to initiate an LDIF export.

ID: 15

Severity: ERROR

Message: You do not have sufficient privileges to initiate a Directory Server restart.

ID: 16

Severity: ERROR

Message: You do not have sufficient privileges to initiate a Directory Server shutdown.

ID: 17

Severity: ERROR

Message: An error occurred while attempting to notify a synchronization provider of type %s about the schema changes made by the add schema file task: %s.

ID: 18

Severity: ERROR

Message: You do not have sufficient privileges to initiate an index rebuild.

ID: 20

Severity: ERROR

Message: Invalid DN provided with the Initialize task.

ID: 21

Severity: ERROR

Message: Only users with the SERVER_LOCKDOWN privilege may place the server in lockdown mode.

ID: 22

Severity: ERROR

Message: Only users with the SERVER_LOCKDOWN privilege connected from a loopback address may place the server in lockdown mode.

ID: 23

Severity: ERROR

Message: Only users with the SERVER_LOCKDOWN privilege may cause the server to leave lockdown mode.

ID: 24

Severity: ERROR

Message: Only users with the SERVER_LOCKDOWN privilege connected from a loopback address may cause the server to leave lockdown mode.

ID: 25

Severity: ERROR

Message: You do not have sufficient privileges to terminate client connections.

ID: 26

Severity: ERROR

Message: Unable to decode value %s as an integer connection ID.

ID: 27

Severity: ERROR

Message: Attribute %s must be provided to specify the connection ID for the client to disconnect.

ID: 28

Severity: ERROR

Message: Unable to decode value %s as an indication of whether to notify the client before

disconnecting it. The provided value should be either 'true' or 'false'.

ID: 30

Severity: ERROR

Message: There is no client connection with connection ID %s.

ID: 103

Severity: ERROR

Message: Invalid generation ID provided with the task.

ID: 106

Severity: ERROR

Message: Unable to connect to the server at %s on port %s. Check this port is an administration port.

ID: 108

Severity: ERROR

Message: Index option cannot be specified when the rebuildAll or rebuildDegraded option is used.

ID: 110

Severity: ERROR

Message: Attribute %s has an invalid value. Reason: %s.

ID: 112

Severity: ERROR

Message: No changelog database was found for baseDN '%s'. Either the baseDN is not replicated or its changelog has not been enabled in this server.

ID: 113

Severity: ERROR

Message: The change number index cannot be reset because this OpenDJ instance does not appear to be a replication server.

ID: 114

Severity: ERROR

Message: Invalid change number (%d) specified, it must be greater than zero.

ID: 115

Severity: ERROR

Message: Unable to reset the change number index: %s.

Log Message Category: TOOL

ID: 1

Severity: ERROR

Message: Unable to create an SSL connection to the server: %s.

ID: 2

Severity: ERROR

Message: Unable to create an SSL connection to the server because the connection factory has not been initialized.

ID: 3

Severity: ERROR

Message: Cannot load the key store file: %s.

ID: 4

Severity: ERROR

Message: Cannot initialize the key manager for the key store:%s.

ID: 5

Severity: ERROR

Message: Cannot load the key store file: %s.

ID: 6

Severity: ERROR

Message: Cannot initialize the key manager for the key store:%s.

ID: 16

Severity: ERROR

Message: An unexpected error occurred while attempting to initialize the command-line arguments: %s.

ID: 17

Severity: ERROR

Message: An error occurred while parsing the command-line arguments: %s.

ID: 18

Severity: ERROR

Message: No clear-text password was specified. Use --%s, --%s or --%s to specify the password to encode.

ID: 19

Severity: ERROR

Message: No password storage scheme was specified. Use the --%s argument to specify the storage scheme.

ID: 20

Severity: ERROR

Message: An unexpected error occurred while attempting to bootstrap the Directory Server client-side code: %s.

ID: 21

Severity: ERROR

Message: An error occurred while trying to load the Directory Server configuration: %s.

ID: 22

Severity: ERROR

Message: An error occurred while trying to load the Directory Server schema: %s.

ID: 23

Severity: ERROR

Message: An error occurred while trying to initialize the core Directory Server configuration: %s.

ID: 24

Severity: ERROR

Message: An error occurred while trying to initialize the Directory Server password storage schemes: %s.

ID: 25

Severity: ERROR

Message: No password storage schemes have been configured for use in the Directory Server.

ID: 26

Severity: ERROR

Message: Password storage scheme "%s" is not configured for use in the Directory Server.

ID: 29

Severity: ERROR

Message: Encoded Password: "%s".

ID: 30

Severity: ERROR

Message: An error occurred while attempting to encode the clear-text password: %s.

ID: 52

Severity: ERROR

Message: Unable to decode exclude filter string "%s" as a valid search filter: %s.

ID: 53

Severity: ERROR

Message: Unable to decode include filter string "%s" as a valid search filter: %s.

ID: 54

Severity: ERROR

Message: Unable to decode base DN string "%s" as a valid distinguished name: %s.

ID: 55

Severity: ERROR

Message: Multiple Directory Server backends are configured with the requested backend ID "%s".

ID: 56

Severity: ERROR

Message: None of the Directory Server backends are configured with the requested backend ID "%s".

ID: 57

Severity: ERROR

Message: Unable to decode exclude branch string "%s" as a valid distinguished name: %s.

ID: 58

Severity: ERROR

Message: Unable to decode wrap column value "%s" as an integer.

ID: 59

Severity: ERROR

Message: An error occurred while attempting to process the LDIF export: %s.

ID: 60

Severity: ERROR

Message: Unable to decode the backend configuration base DN string "%s" as a valid DN: %s.

ID: 61

Severity: ERROR

Message: Unable to retrieve the backend configuration base entry "%s" from the server configuration: %s.

ID: 62

Severity: ERROR

Message: Cannot determine the name of the Java class providing the logic for the backend defined in configuration entry %s: %s.

ID: 63

Severity: ERROR

Message: Unable to load class %s referenced in configuration entry %s for use as a Directory Server backend: %s.

ID: 64

Severity: ERROR

Message: Unable to create an instance of class %s referenced in configuration entry %s as a Directory Server backend: %s.

ID: 65

Severity: ERROR

Message: No base DNs have been defined in backend configuration entry %s. This backend will not be evaluated.

ID: 66

Severity: ERROR

Message: Unable to determine the set of base DNs defined in backend configuration entry %s: %s.

ID: 89

Severity: ERROR

Message: Unable to decode exclude filter string "%s" as a valid search filter: %s.

ID: 90

Severity: ERROR

Message: Unable to decode include filter string "%s" as a valid search filter: %s.

ID: 92

Severity: ERROR

Message: Imported branches or backend IDs can not span across multiple Directory Server backends.

ID: 93

Severity: ERROR

Message: None of the Directory Server backends are configured with the requested backend ID or base DNs that include the specified branches.

ID: 94

Severity: ERROR

Message: Unable to decode exclude branch string "%s" as a valid distinguished name: %s.

ID: 95

Severity: ERROR

Message: An error occurred while trying to open the rejects file %s for writing: %s.

ID: 96

Severity: ERROR

Message: An error occurred while attempting to process the LDIF import: %s.

ID: 136

Severity: ERROR

Message: Cannot send the simple bind request: %s.

ID: 137

Severity: ERROR

Message: Cannot read the bind response from the server. The port you are using may require a secured communication (--useSSL). %s.

ID: 138

Severity: ERROR

Message: The Directory Server indicated that it was closing the connection to the client (result code %d, message "%s".

ID: 139

Severity: ERROR

Message: The Directory Server sent an unexpected extended response message to the client: %s.

ID: 140

Severity: ERROR

Message: The Directory Server sent an unexpected response message to the client: %s.

ID: 141

Severity: ERROR

Message: The simple bind attempt failed.

ID: 142

Severity: ERROR

Message: A SASL bind was requested but no SASL mechanism was specified.

ID: 143

Severity: ERROR

Message: The requested SASL mechanism "%s" is not supported by this client.

ID: 144

Severity: ERROR

Message: The trace SASL property may only be given a single value.

ID: 145

Severity: ERROR

Message: Property "%s" is not allowed for the %s SASL mechanism.

ID: 146

Severity: ERROR

Message: Cannot send the SASL %S bind request: %s.

ID: 147

Severity: ERROR

Message: The SASL %s bind attempt failed.

ID: 148

Severity: ERROR

Message: No SASL properties were provided for use with the %s mechanism.

ID: 149

Severity: ERROR

Message: The "authid" SASL property only accepts a single value.

ID: 150

Severity: ERROR

Message: The "authid" SASL property is required for use with the %s mechanism.

ID: 151

Severity: ERROR

Message: Cannot send the initial bind request in the multi-stage %s bind to the server: %s.

ID: 152

Severity: ERROR

Message: Cannot read the initial %s bind response from the server: %s.

ID: 153

Severity: ERROR

Message: The client received an unexpected intermediate bind response. The "SASL bind in progress" result was expected for the first response in the multi-stage %s bind process, but the bind response had a result code of %d (%s) and an error message of "%s".

ID: 154

Severity: ERROR

Message: The initial bind response from the server did not include any server SASL credentials containing the challenge information needed to complete the CRAM-MD5 authentication.

ID: 155

Severity: ERROR

Message: An unexpected error occurred while trying to initialize the MD5 digest generator: %s.

ID: 156

Severity: ERROR

Message: Cannot send the second bind request in the multi-stage %s bind to the server: %s.

ID: 157

Severity: ERROR

Message: Cannot read the second %s bind response from the server: %s.

ID: 158

Severity: ERROR

Message: One or more SASL properties were provided, but the %s mechanism does not take any SASL properties.

ID: 159

Severity: ERROR

Message: The "authzid" SASL property only accepts a single value.

ID: 160

Severity: ERROR

Message: The "realm" SASL property only accepts a single value.

ID: 161

Severity: ERROR

Message: The "qop" SASL property only accepts a single value.

ID: 162

Severity: ERROR

Message: The "%s" QoP mode is not supported by this client. Only the "auth" mode is currently available for use.

ID: 163

Severity: ERROR

Message: The specified DIGEST-MD5 quality of protection mode "%s" is not valid. The only QoP mode currently supported is "auth".

ID: 164

Severity: ERROR

Message: The "digest-uri" SASL property only accepts a single value.

ID: 165

Severity: ERROR

Message: The initial bind response from the server did not include any server SASL credentials containing the challenge information needed to complete the DIGEST-MD5 authentication.

ID: 166

Severity: ERROR

Message: The DIGEST-MD5 credentials provided by the server contained an invalid token of "%s" starting at position %d.

ID: 167

Severity: ERROR

Message: The DIGEST-MD5 credentials provided by the server specified the use of the "%s" character set. The character set that may be specified in the DIGEST-MD5 credentials is "utf-8".

ID: 168

Severity: ERROR

Message: The requested QoP mode of "%s" is not listed as supported by the Directory Server. The Directory Server's list of supported QoP modes is: "%s".

ID: 169

Severity: ERROR

Message: The server SASL credentials provided in response to the initial DIGEST-MD5 bind request did not include the nonce to use to generate the authentication digests.

ID: 170

Severity: ERROR

Message: An error occurred while attempting to generate the response digest for the DIGEST-MD5 bind request: %s.

ID: 171

Severity: ERROR

Message: The DIGEST-MD5 bind response from the server did not include the "rspauth" element to provide a digest of the response authentication information.

ID: 172

Severity: ERROR

Message: An error occurred while trying to decode the rspauth element of the DIGEST-MD5 bind response from the server as a hexadecimal string: %s.

ID: 173

Severity: ERROR

Message: An error occurred while trying to calculate the expected rspauth element to compare against the value included in the DIGEST-MD5 response from the server: %s.

ID: 174

Severity: ERROR

Message: The rpsauth element included in the DIGEST-MD5 bind response from the Directory Server was different from the expected value calculated by the client.

ID: 175

Severity: ERROR

Message: The DIGEST-MD5 response challenge could not be parsed because it had an invalid quotation mark at position %d.

ID: 184

Severity: ERROR

Message: The "kdc" SASL property only accepts a single value.

ID: 185

Severity: ERROR

Message: The specified GSSAPI quality of protection mode "%s" is not valid. The only QoP mode currently supported is "auth".

ID: 186

Severity: ERROR

Message: An error occurred while trying to create the temporary JAAS configuration for GSSAPI authentication: %s.

ID: 187

Severity: ERROR

Message: An error occurred while attempting to perform local authentication to the Kerberos realm: %s.

ID: 188

Severity: ERROR

Message: An error occurred while attempting to perform GSSAPI authentication to the Directory Server: %s.

ID: 189

Severity: ERROR

Message: The LDAPAuthenticationHandler.run() method was called for a non-SASL bind. The backtrace for this call is %s.

ID: 190

Severity: ERROR

Message: The LDAPAuthenticationHandler.run() method was called for a SASL bind with an unexpected mechanism of "%s". The backtrace for this call is %s.

ID: 191

Severity: ERROR

Message: An error occurred while attempting to create a SASL client to process the GSSAPI authentication: %s.

ID: 192

Severity: ERROR

Message: An error occurred while attempting to create the initial challenge for GSSAPI authentication: %s.

ID: 193

Severity: ERROR

Message: An error occurred while trying to validate the SASL credentials provided by the Directory Server in the GSSAPI bind response: %s.

ID: 194

Severity: ERROR

Message: The Directory Server unexpectedly returned a success response to the client even though the client does not believe that the GSSAPI negotiation is complete.

ID: 195

Severity: ERROR

Message: The GSSAPI bind attempt failed.

ID: 196

Severity: ERROR

Message: The LDAPAuthenticationHandler.handle() method was called for a non-SASL bind. The backtrace for this call is %s.

ID: 197

Severity: ERROR

Message: The LDAPAuthenticationHandler.handle() method was called during a GSSAPI bind attempt with an unexpected callback type of %s.

ID: 198

Severity: ERROR

Message: The LDAPAuthenticationHandler.handle() method was called for an unexpected SASL mechanism of %s. The backtrace for this call is %s.

ID: 201

Severity: ERROR

Message: Invalid LDAP version number '%s'. Allowed values are 2 and 3.

ID: 202

Severity: ERROR

Message: Cannot send the 'Who Am I?' request to the Directory Server: %s.

ID: 203

Severity: ERROR

Message: Cannot read the 'Who Am I?' response from the Directory Server: %s.

ID: 204

Severity: ERROR

Message: The 'Who Am I?' request was rejected by the Directory Server.

ID: 205

Severity: ERROR

Message: Invalid scope '%s' specified for the search request.

ID: 206

Severity: ERROR

Message: No filters specified for the search request.

ID: 210

Severity: ERROR

Message: An error occurred while attempting to perform index verification: %s.

ID: 211

Severity: ERROR

Message: Only one index at a time may be verified for cleanliness.

ID: 212

Severity: ERROR

Message: The backend does not support indexing.

ID: 213

Severity: ERROR

Message: The Directory Server backend with backend ID "%s" does not provide a mechanism for performing LDIF exports.

ID: 214

Severity: ERROR

Message: The Directory Server backend with backend ID %s does not provide a mechanism for performing LDIF imports.

ID: 217

Severity: ERROR

Message: Cannot determine the backend ID for the backend defined in configuration entry %s: %s.

ID: 218

Severity: ERROR

Message: Unable to decode include branch string "%s" as a valid distinguished name: %s.

ID: 219

Severity: ERROR

Message: Provided include base DN "%s" is not handled by the backend with backend ID %s.

ID: 230

Severity: ERROR

Message: Multiple Directory Server backends are configured to support base DN "%s".

ID: 231

Severity: ERROR

Message: None of the Directory Server backends are configured to support the requested base DN "%s".

ID: 242

Severity: ERROR

Message: Provided include base DN "%s" is not handled by the backend with backend ID %s.

ID: 261

Severity: ERROR

Message: None of the Directory Server backends are configured with the requested backend ID "%s".

ID: 264

Severity: ERROR

Message: The target backend %s cannot be backed up using the requested configuration.

ID: 265

Severity: ERROR

Message: An error occurred while attempting to back up backend %s with the requested configuration: %s.

ID: 275

Severity: ERROR

Message: The %s and %s arguments may not be used together. Exactly one of them must be provided.

ID: 276

Severity: ERROR

Message: Neither the %s argument nor the %s argument was provided. Exactly one of them is required.

ID: 277

Severity: ERROR

Message: An error occurred while attempting to create the backup directory %s: %s.

ID: 281

Severity: ERROR

Message: An error occurred while attempting to parse the backup descriptor file %s: %s.

ID: 284

Severity: ERROR

Message: An error occurred while attempting to initialize the crypto manager: %s.

ID: 285

Severity: ERROR

Message: An error occurred while attempting to initialize the subentry manager: %s.

ID: 286

Severity: ERROR

Message: An error occurred while attempting to initialize the root DN manager: %s.

ID: 288

Severity: ERROR

Message: The use of the %s argument requires that the %s argument is also provided.

ID: 304

Severity: ERROR

Message: An error occurred while attempting to examine the set of backups contained in backup directory %s: %s.

ID: 313

Severity: ERROR

Message: The requested backup ID %s does not exist in %s.

ID: 314

Severity: ERROR

Message: There are no Directory Server backups contained in %s.

ID: 315

Severity: ERROR

Message: The backups contained in directory %s were taken from a Directory Server backend defined in configuration entry %s but no such backend is available.

ID: 316

Severity: ERROR

Message: The Directory Server backend configured with backend ID %s does not provide a mechanism for restoring backups.

ID: 317

Severity: ERROR

Message: An unexpected error occurred while attempting to restore backup %s from %s: %s.

ID: 318

Severity: ERROR

Message: Restoring an encrypted or signed backup requires a connection to an online server.

ID: 325

Severity: ERROR

Message: The use of the %s argument or the %s argument requires a connection to an online server instance.

ID: 326

Severity: ERROR

Message: The use of the %s argument requires that the %s argument is also provided.

ID: 328

Severity: ERROR

Message: An error occurred while attempting to acquire a shared lock for backend %s: %s. This generally means that some other process has exclusive access to this backend (e.g., a restore or an LDIF import). This backend will not be archived.

ID: 330

Severity: ERROR

Message: An error occurred while attempting to acquire an exclusive lock for backend %s: %s. This generally means some other process is still using this backend (e.g., it is in use by the Directory Server or a backup or LDIF export is in progress). The restore cannot continue.

ID: 332

Severity: ERROR

Message: An error occurred while attempting to acquire an exclusive lock for backend %s: %s. This generally means some other process is still using this backend (e.g., it is in use by the Directory Server or a backup or LDIF export is in progress). The LDIF import cannot continue.

ID: 334

Severity: ERROR

Message: An error occurred while attempting to acquire a shared lock for backend %s: %s. This generally means that some other process has an exclusive lock on this backend (e.g., an LDIF import or a restore). The LDIF export cannot continue.

ID: 336

Severity: ERROR

Message: An error occurred while attempting to acquire a shared lock for backend %s: %s. This generally means that some other process has an exclusive lock on this backend (e.g., an LDIF import or a restore). The index verification cannot continue.

ID: 343

Severity: ERROR

Message: The search filter provided for the LDAP assertion control was invalid: %s.

ID: 349

Severity: ERROR

Message: An error occurred while trying to decode the entry contained in the value of the pre-read response control: %s.

ID: 352

Severity: ERROR

Message: An error occurred while trying to decode the entry contained in the value of the post-read response control: %s.

ID: 356

Severity: ERROR

Message: The request to use the persistent search control did not include a descriptor that indicates the options to use with that control.

ID: 357

Severity: ERROR

Message: The persistent search descriptor %s did not start with the required 'ps' string.

ID: 358

Severity: ERROR

Message: The provided change type value %s is invalid. The recognized change types are add, delete, modify, modifydn, and any.

ID: 359

Severity: ERROR

Message: The provided changesOnly value %s is invalid. Allowed values are 1 to only return matching entries that have changed since the beginning of the search, or 0 to also include

existing entries that match the search criteria.

ID: 360

Severity: ERROR

Message: The provided returnECs value %s is invalid. Allowed values are 1 to request that the entry change notification control be included in updated entries, or 0 to exclude the control from matching entries.

ID: 365

Severity: ERROR

Message: The provided matched values filter was invalid: %s.

ID: 366

Severity: ERROR

Message: An error occurred while attempting to open the LDIF file %s for reading: %s.

ID: 367

Severity: ERROR

Message: An error occurred while attempting to read the contents of LDIF file %s: %s.

ID: 368

Severity: ERROR

Message: Error at or near line %d in LDIF file %s: %s.

ID: 371

Severity: ERROR

Message: Authentication password storage scheme "%s" is not configured for use in the Directory Server.

ID: 372

Severity: ERROR

Message: The provided password is not a valid encoded authentication password value: %s.

ID: 373

Severity: ERROR

Message: An error occurred while attempting to initialize the password policy components: %s.

ID: 395

Severity: ERROR

Message: ERROR: You may not provide both the %s and the %s arguments.

ID: 396

Severity: ERROR

Message: ERROR: Unable to decode the provided stop time. It should be in the form YYYYMMDDhhmmssZ for UTC time or YYYYMMDDhhmmss for local time.

ID: 397

Severity: ERROR

Message: ERROR: Unable to perform SSL initialization: %s.

ID: 398

Severity: ERROR

Message: ERROR: The provided SASL option string "%s" could not be parsed in the form "name=value".

ID: 399

Severity: ERROR

Message: ERROR: One or more SASL options were provided, but none of them were the "mech" option to specify which SASL mechanism should be used.

ID: 400

Severity: ERROR

Message: ERROR: Cannot parse the value of the %s argument as an integer value between 1 and 65535: %s.

ID: 401

Severity: ERROR

Message: ERROR: Cannot establish a connection to the Directory Server %s. Verify that the server is running and that the provided credentials are valid. Details: %s.

ID: 402

Severity: ERROR

Message: NOTICE: The connection to the Directory Server was closed while waiting for a response to the shutdown request. This likely means that the server has started the shutdown process.

ID: 403

Severity: ERROR

Message: ERROR: An I/O error occurred while attempting to communicate with the Directory Server: %s.

ID: 404

Severity: ERROR

Message: ERROR: An error occurred while trying to decode the response from the server: %s.

ID: 405

Severity: ERROR

Message: ERROR: Expected an add response message but got a %s message instead.

ID: 428

Severity: ERROR

Message: No search filter was specified. Either a filter file or an individual search filter must be provided.

ID: 429

Severity: ERROR

Message: An error occurred while attempting to process the Directory Server configuration file %s: %s.

ID: 430

Severity: ERROR

Message: An error occurred while attempting to initialize the Directory Server schema based on the information in configuration file %s: %s.

ID: 431

Severity: ERROR

Message: An error occurred while attempting to parse search filter '%s': %s.

ID: 432

Severity: ERROR

Message: An error occurred while attempting to parse base DN '%s': %s.

ID: 433

Severity: ERROR

Message: An error occurred while attempting to parse the time limit as an integer: %s.

ID: 434

Severity: ERROR

Message: An error occurred while attempting to parse the size limit as an integer: %s.

ID: 435

Severity: ERROR

Message: An error occurred while attempting to create the LDIF reader: %s.

ID: 436

Severity: ERROR

Message: An error occurred while attempting to create the LDIF writer used to return matching entries: %s.

ID: 439

Severity: ERROR

Message: An error occurred while attempting to read an entry from the LDIF content: %s. Skipping this entry and continuing processing.

ID: 440

Severity: ERROR

Message: An error occurred while attempting to read an entry from the LDIF content: %s. Unable to continue processing.

ID: 441

Severity: ERROR

Message: An unexpected error occurred during search processing: %s.

ID: 442

Severity: ERROR

Message: An error occurred while attempting to initialize the Directory Server JMX subsystem based on the information in configuration file %s: %s.

ID: 452

Severity: ERROR

Message: An error occurred while attempting to initialize the Directory Server JMX subsystem based on the information in configuration file %s: %s.

ID: 453

Severity: ERROR

Message: An error occurred while attempting to process the Directory Server configuration file %s: %s.

ID: 454

Severity: ERROR

Message: An error occurred while attempting to initialize the Directory Server schema based on the information in configuration file %s: %s.

ID: 455

Severity: ERROR

Message: An error occurred while attempting to open source LDIF %s: %s.

ID: 456

Severity: ERROR

Message: An error occurred while reading the contents of source LDIF %s: %s.

ID: 457

Severity: ERROR

Message: An error occurred while attempting to open target LDIF %s: %s.

ID: 458

Severity: ERROR

Message: An error occurred while reading the contents of target LDIF %s: %s.

ID: 459

Severity: ERROR

Message: An error occurred while attempting to open the LDIF writer for the diff output: %s.

ID: 461

Severity: ERROR

Message: An error occurred while attempting to write the diff output: %s.

ID: 472

Severity: ERROR

Message: An error occurred while attempting to acquire the server-wide lock file %s: %s. This generally means that the Directory Server is running, or another tool that requires exclusive access to the server is in use.

ID: 473

Severity: ERROR

Message: An error occurred while attempting to initialize the Directory Server JMX subsystem based on the information in configuration file %s: %s.

ID: 474

Severity: ERROR

Message: An error occurred while attempting to process the Directory Server configuration file %s: %s.

ID: 475

Severity: ERROR

Message: An error occurred while attempting to initialize the Directory Server schema based on

the information in configuration file %s: %s.

ID: 476

Severity: ERROR

Message: An error occurred while attempting to parse base DN value "%s" as a DN: %s.

ID: 477

Severity: ERROR

Message: An error occurred while attempting to parse root DN value "%s" as a DN: %s.

ID: 478

Severity: ERROR

Message: The DN for the initial root user was provided, but no corresponding password was given. If the root DN is specified then the password must also be provided.

ID: 480

Severity: ERROR

Message: An error occurred while attempting to update the port on which to listen for LDAP communication: %s.

ID: 481

Severity: ERROR

Message: An error occurred while attempting to update the entry for the initial Directory Server root user: %s.

ID: 482

Severity: ERROR

Message: An error occurred while writing the updated Directory Server configuration: %s.

ID: 483

Severity: ERROR

Message: ERROR: No configuration changes were specified.

ID: 503

Severity: ERROR

Message: An error occurred while attempting to parse the string "%s" as a valid DN: %s.

ID: 510

Severity: ERROR

Message: ERROR: Unable to bind to port %d. This port may already be in use, or you may not have permission to bind to it. On UNIX-based operating systems, non-root users may not be

allowed to bind to ports 1 through 1024.

ID: 511

Severity: ERROR

Message: ERROR: Unable to bind to port %d. This port may already be in use, or you may not have permission to bind to it.

ID: 513

Severity: ERROR

Message: Unable to authenticate using simple authentication.

ID: 524

Severity: ERROR

Message: ERROR: The provided response could not be interpreted as an integer. Please provide the response as an integer value.

ID: 525

Severity: ERROR

Message: ERROR: The provided value is less than the lowest allowed value of %d.

ID: 526

Severity: ERROR

Message: ERROR: The provided value is greater than the largest allowed value of %d.

ID: 527

Severity: ERROR

Message: ERROR: The provided response could not be interpreted as an LDAP DN.

ID: 530

Severity: ERROR

Message: ERROR: The provided password values do not match.

ID: 535

Severity: ERROR

Message: Invalid number of arguments provided for tag %s on line number %d of the template file: expected %d, got %d.

ID: 536

Severity: ERROR

Message: Invalid number of arguments provided for tag %s on line number %d of the template file: expected between %d and %d, got %d.

ID: 537

Severity: ERROR

Message: Undefined attribute %s referenced on line %d of the template file.

ID: 538

Severity: ERROR

Message: Value %d is below the lowest allowed value of %d for tag %s on line %d of the template file.

ID: 539

Severity: ERROR

Message: Cannot parse value "%s" as an integer for tag %s on line %d of the template file.

ID: 540

Severity: ERROR

Message: Value %d is above the largest allowed value of %d for tag %s on line %d of the template file.

ID: 542

Severity: ERROR

Message: Cannot parse value "%s" as a Boolean value for tag %s on line %d of the template file. The value must be either 'true' or 'false'.

ID: 543

Severity: ERROR

Message: The branch with entry DN '%s' references a subordinate template named '%s' which is not defined in the template file.

ID: 544

Severity: ERROR

Message: Unable to load class %s for use as a MakeLDIF tag.

ID: 545

Severity: ERROR

Message: Cannot instantiate class %s as a MakeLDIF tag.

ID: 546

Severity: ERROR

Message: Cannot register the tag defined in class %s because the tag name %s conflicts with the name of another tag that has already been registered.

ID: 548

Severity: ERROR

Message: The constant definition on line %d is missing an equal sign to delimit the constant name from the value.

ID: 549

Severity: ERROR

Message: The constant definition on line %d does not include a name for the constant.

ID: 550

Severity: ERROR

Message: The definition for constant %s on line %d conflicts with an earlier constant definition included in the template.

ID: 551

Severity: ERROR

Message: Constant %s defined on line %d has not been assigned a value.

ID: 552

Severity: ERROR

Message: The branch definition %s starting on line %d conflicts with an earlier branch definition contained in the template file.

ID: 553

Severity: ERROR

Message: The template definition %s starting on line %d conflicts with an earlier template definition contained in the template file.

ID: 554

Severity: ERROR

Message: Unexpected template line "%s" encountered on line %d of the template file.

ID: 555

Severity: ERROR

Message: The template named %s references a subordinate template named %s which is not defined in the template file.

ID: 556

Severity: ERROR

Message: Unable to decode branch DN "%s" on line %d of the template file.

ID: 557

Severity: ERROR

Message: Subordinate template definition on line %d for branch %s is missing a colon to separate the template name from the number of entries.

ID: 558

Severity: ERROR

Message: Subordinate template definition on line %d for branch %s specified invalid number of entries %d for template %s.

ID: 560

Severity: ERROR

Message: Unable to parse the number of entries for template %s as an integer for the subordinate template definition on line %d for branch %s.

ID: 561

Severity: ERROR

Message: Subordinate template definition on line %d for template %s is missing a colon to separate the template name from the number of entries.

ID: 562

Severity: ERROR

Message: Subordinate template definition on line %d for template %s specified invalid number of entries %d for subordinate template %s.

ID: 564

Severity: ERROR

Message: Unable to parse the number of entries for template %s as an integer for the subordinate template definition on line %d for template %s.

ID: 565

Severity: ERROR

Message: The template named %s includes RDN attribute %s that is not assigned a value in that template.

ID: 566

Severity: ERROR

Message: There is no colon to separate the attribute name from the value pattern on line %d of the template file in the definition for branch %s.

ID: 567

Severity: ERROR

Message: There is no attribute name before the colon on line %d of the template file in the definition for branch %s.

ID: 569

Severity: ERROR

Message: There is no colon to separate the attribute name from the value pattern on line %d of the template file in the definition for template %s.

ID: 570

Severity: ERROR

Message: There is no attribute name before the colon on line %d of the template file in the definition for template %s.

ID: 572

Severity: ERROR

Message: An undefined tag %s is referenced on line %d of the template file.

ID: 573

Severity: ERROR

Message: An unexpected error occurred while trying to create a new instance of tag %s referenced on line %d of the template file: %s.

ID: 582

Severity: ERROR

Message: An error occurred while attempting to initialize the Directory Server JMX subsystem based on the information in configuration file %s: %s.

ID: 583

Severity: ERROR

Message: An error occurred while attempting to process the Directory Server configuration file %s: %s.

ID: 584

Severity: ERROR

Message: An error occurred while attempting to initialize the Directory Server schema based on the information in configuration file %s: %s.

ID: 585

Severity: ERROR

Message: An error occurred while attempting to read the template file: %s.

ID: 586

Severity: ERROR

Message: An error occurred while attempting to parse the template file: %s.

ID: 587

Severity: ERROR

Message: Cannot parse value "%s" as an valid format string for tag %s on line %d of the template file.

ID: 588

Severity: ERROR

Message: The random tag on line %d of the template file does not include an argument to specify the type of random value that should be generated.

ID: 590

Severity: ERROR

Message: The random tag on line %d of the template file references an unknown random type of %s.

ID: 592

Severity: ERROR

Message: Could not find template file %s.

ID: 593

Severity: ERROR

Message: The specified resource directory %s could not be found.

ID: 595

Severity: ERROR

Message: Cannot find file %s referenced by tag %s on line %d of the template file.

ID: 596

Severity: ERROR

Message: Invalid file access mode %s for tag %s on line %d of the template file. It must be either "sequential" or "random".

ID: 597

Severity: ERROR

Message: An error occurred while trying to read file %s referenced by tag %s on line %d of the template file: %s.

ID: 598

Severity: ERROR

Message: An error occurred while attempting to open LDIF file %s for writing: %s.

ID: 599

Severity: ERROR

Message: An error occurred while writing data to LDIF file %s: %s.

ID: 601

Severity: ERROR

Message: An error occurred while attempting to write entry %s to LDIF: %s.

ID: 605

Severity: ERROR

Message: Neither the %s or the %s argument was provided. One of these arguments must be given to specify the source for the LDIF data to be imported.

ID: 606

Severity: ERROR

Message: Unable to parse the specified file %s as a MakeLDIF template file: %s.

ID: 607

Severity: ERROR

Message: Line %d of the template file contains an incomplete tag that starts with either '<' or '{' but does get closed.

ID: 608

Severity: ERROR

Message: The provided passwords do not match.

ID: 610

Severity: ERROR

Message: Entry %s is added twice in the set of changes to apply, which is not supported by the LDIF modify tool.

ID: 611

Severity: ERROR

Message: Entry %s cannot be deleted because it was previously added in the set of changes. This is not supported by the LDIF modify tool.

ID: 612

Severity: ERROR

Message: Cannot modify entry %s because it was previously added or deleted in the set of changes. This is not supported by the LDIF modify tool.

ID: 613

Severity: ERROR

Message: The modify DN operation targeted at entry %s cannot be processed because modify DN operations are not supported by the LDIF modify tool.

ID: 614

Severity: ERROR

Message: Entry %s has an unknown changetype of %s.

ID: 615

Severity: ERROR

Message: Unable to add entry %s because it already exists in the data set.

ID: 616

Severity: ERROR

Message: Unable to delete entry %s because it does not exist in the data set.

ID: 617

Severity: ERROR

Message: Unable to modify entry %s because it does not exist in the data set.

ID: 626

Severity: ERROR

Message: An error occurred while attempting to initialize the Directory Server JMX subsystem based on the information in configuration file %s: %s.

ID: 627

Severity: ERROR

Message: An error occurred while attempting to process the Directory Server configuration file %s: %s.

ID: 628

Severity: ERROR

Message: An error occurred while attempting to initialize the Directory Server schema based on the information in configuration file %s: %s.

ID: 629

Severity: ERROR

Message: The source LDIF file %s does not exist.

ID: 630

Severity: ERROR

Message: Unable to open the source LDIF file %s: %s.

ID: 631

Severity: ERROR

Message: The changes LDIF file %s does not exist.

ID: 632

Severity: ERROR

Message: Unable to open the changes LDIF file %s: %s.

ID: 633

Severity: ERROR

Message: Unable to open the target LDIF file %s for writing: %s.

ID: 634

Severity: ERROR

Message: An error occurred while processing the requested changes: %s.

ID: 657

Severity: ERROR

Message: If either a bind DN or bind password is provided, then the other must be given as well.

ID: 658

Severity: ERROR

Message: If a bind DN and password are not provided, then an authorization ID and current password must be given.

ID: 659

Severity: ERROR

Message: If the %s argument is provided, then the %s argument must also be given.

ID: 660

Severity: ERROR

Message: Unable to initialize SSL/TLS support: %s.

ID: 661

Severity: ERROR

Message: An error occurred while attempting to connect to the Directory Server: %s.

ID: 662

Severity: ERROR

Message: Unable to send the LDAP password modify request: %s.

ID: 663

Severity: ERROR

Message: Unable to read the LDAP password modify response: %s.

ID: 664

Severity: ERROR

Message: The LDAP password modify operation failed with result code %d.

ID: 665

Severity: ERROR

Message: Error Message: %s.

ID: 666

Severity: ERROR

Message: Matched DN: %s.

ID: 670

Severity: ERROR

Message: Unable to decode the password modify response value because it contained an invalid element type of %s.

ID: 671

Severity: ERROR

Message: Unable to decode the password modify response value: %s.

ID: 682

Severity: ERROR

Message: No entry DNs provided for the compare operation.

ID: 703

Severity: ERROR

Message: No attribute was specified to use as the target for the comparison.

ID: 704

Severity: ERROR

Message: Invalid attribute string '%s'. The attribute string must be in one of the following forms: 'attribute:value', 'attribute::base64value', or 'attribute:<valueFilePath'.

ID: 705

Severity: ERROR

Message: Invalid control specification '%s'.

ID: 706

Severity: ERROR

Message: SASL EXTERNAL authentication may only be requested if SSL or StartTLS is used.

ID: 707

Severity: ERROR

Message: SASL EXTERNAL authentication may only be used if a client certificate key store is specified.

ID: 734

Severity: ERROR

Message: An error occurred while trying to read backend information from the server configuration: %s.

ID: 735

Severity: ERROR

Message: The provided base DN value '%s' could not be parsed as a valid DN: %s.

ID: 742

Severity: ERROR

Message: There is no backend with ID '%s' in the server configuration.

ID: 743

Severity: ERROR

Message: None of the provided backend IDs exist in the server configuration.

ID: 748

Severity: ERROR

Message: The provided password is not a valid encoded user password value: %s.

ID: 780

Severity: ERROR

Message: ERROR: The specified LDIF file %s does not exist.

ID: 788

Severity: ERROR

Message: Unable to decode the password policy response control: %s.

ID: 789

Severity: ERROR

Message: The connection to the Directory Server was closed before the bind response could be read.

ID: 791

Severity: ERROR

Message: The simple paged results control may only be used with a single search filter.

ID: 792

Severity: ERROR

Message: Unable to decode the simple paged results control from the search response: %s.

ID: 793

Severity: ERROR

Message: The simple paged results response control was not found in the search result done message from the server.

ID: 795

Severity: ERROR

Message: Rejecting client certificate chain because the prompt trust manager may only be used to trust server certificates.

ID: 801

Severity: ERROR

Message: The server certificate has been rejected by the user.

ID: 807

Severity: ERROR

Message: An error occurred while attempting to update the port on which to listen for JMX communication: %s.

ID: 810

Severity: ERROR

Message: Result Code: %d (%s).

ID: 811

Severity: ERROR

Message: Additional Information: %s.

ID: 812

Severity: ERROR

Message: Matched DN: %s.

ID: 813

Severity: ERROR

Message: Could not find the service name for the server.

ID: 814

Severity: ERROR

Message: An unexpected error occurred starting the server as a windows service.

ID: 815

Severity: ERROR

Message: An unexpected error occurred stopping the server windows service.

ID: 823

Severity: ERROR

Message: You can only provide one of the following arguments: enableService, disableService, serviceState or cleanupService.

ID: 824

Severity: ERROR

Message: You must provide at least one of the following arguments: enableService, disableService or serviceState or cleanupService.

ID: 829

Severity: ERROR

Message: The server could not be enabled to run as a Windows service. The service name is already in use.

ID: 830

Severity: ERROR

Message: ERROR: Unable to bind to port %d. This port may already be in use, or you may not have permission to bind to it.

ID: 834

Severity: ERROR

Message: An unexpected error occurred trying to disable the server as a Windows service%nCheck that you have administrator rights (only Administrators can disable the server as a Windows Service).

ID: 837

Severity: ERROR

Message: An unexpected error occurred trying to retrieve the state of the server as a Windows service.

ID: 846

Severity: ERROR

Message: Could not find the service with name %s.

ID: 848

Severity: ERROR

Message: An unexpected error occurred cleaning up the service %s.

ID: 852

Severity: ERROR

Message: An error occurred while attempting to perform index rebuild: %s.

ID: 853

Severity: ERROR

Message: The backend does not support rebuilding of indexes.

ID: 854

Severity: ERROR

Message: At least one index must be specified for the rebuild process.

ID: 855

Severity: ERROR

Message: An error occurred while attempting to acquire a exclusive lock for backend %s: %s. This generally means that some other process has an lock on this backend or the server is running with this backend online. The rebuild process cannot continue.

ID: 857

Severity: ERROR

Message: An error occurred while attempting to acquire a shared lock for backend %s: %s. This generally means that some other process has an exclusive lock on this backend (e.g., an LDIF

import or a restore). The rebuild process cannot continue.

ID: 859

Severity: ERROR

Message: An error occurred while attempting to update the port on which to listen for LDAPS communication: %s.

ID: 863

Severity: ERROR

Message: An error occurred while attempting to parse key manager provider DN value "%s" as a DN: %s.

ID: 864

Severity: ERROR

Message: An error occurred while attempting to parse trust manager provider DN value "%s" as a DN: %s.

ID: 865

Severity: ERROR

Message: An error occurred while attempting to enable StartTLS: %s.

ID: 866

Severity: ERROR

Message: An error occurred while attempting to enable key manager provider entry: %s.

ID: 867

Severity: ERROR

Message: An error occurred while attempting to enable trust manager provider entry: %s.

ID: 868

Severity: ERROR

Message: An error occurred while attempting to update the key manager provider DN used for LDAPS communication: %s.

ID: 869

Severity: ERROR

Message: An error occurred while attempting to update the trust manager provider DN used for LDAPS communication: %s.

ID: 872

Severity: ERROR

Message: ERROR: You must provide the %s argument when providing the %s argument.

ID: 873

Severity: ERROR

Message: An error occurred while attempting to update the nickname of the certificate that the connection handler should use when accepting SSL-based connections or performing StartTLS negotiation: %s.

ID: 875

Severity: ERROR

Message: The parent template %s referenced on line %d for template %s is invalid because the referenced parent template is not defined before the template that extends it.

ID: 877

Severity: ERROR

Message: The provided sort order was invalid: %s.

ID: 879

Severity: ERROR

Message: If the --%s argument is provided, then the --%s argument must also be given.

ID: 880

Severity: ERROR

Message: The provided virtual list view descriptor was invalid. It must be a value in the form 'beforeCount:afterCount:offset:contentCount' (where offset specifies the index of the target entry and contentCount specifies the estimated total number of results or zero if it is not known), or 'beforeCount:afterCount:assertionValue' (where the entry should be the first entry whose primary sort value is greater than or equal to the provided assertionValue). In either case, beforeCount is the number of entries to return before the target value and afterCount is the number of entries to return after the target value.

ID: 887

Severity: ERROR

Message: The specified LDIF file %s cannot be read.

ID: 890

Severity: ERROR

Message: The authorization ID "%s" contained in the geteffectiverights control is invalid because it does not start with "dn:" to indicate a user DN.

ID: 1155

Severity: ERROR

Message: No subcommand was provided to indicate which password policy state operation should be performed.

ID: 1156

Severity: ERROR

Message: The provided value '%s' was invalid for the requested operation. A Boolean value of either 'true' or 'false' was expected.

ID: 1157

Severity: ERROR

Message: No value was specified, but the requested operation requires a Boolean value of either 'true' or 'false'.

ID: 1158

Severity: ERROR

Message: Unrecognized subcommand '%s'.

ID: 1159

Severity: ERROR

Message: An error occurred while attempting to send the request to the server: %s.

ID: 1160

Severity: ERROR

Message: The Directory Server closed the connection before the response could be read.

ID: 1161

Severity: ERROR

Message: The server was unable to process the request: result code %d (%s), error message '%s'.

ID: 1162

Severity: ERROR

Message: Unable to decode the response message from the server: %s.

ID: 1163

Severity: ERROR

Message: Unable to decode information about an operation contained in the response: %s.

ID: 1183

Severity: ERROR

Message: Unrecognized or invalid operation type: %s.

ID: 1184

Severity: ERROR

Message: ERROR: You may not provide both the %s and the %s arguments.

ID: 1185

Severity: ERROR

Message: ERROR: Unable to perform SSL initialization: %s.

ID: 1186

Severity: ERROR

Message: ERROR: The provided SASL option string "%s" could not be parsed in the form "name=value".

ID: 1187

Severity: ERROR

Message: ERROR: One or more SASL options were provided, but none of them were the "mech" option to specify which SASL mechanism should be used.

ID: 1188

Severity: ERROR

Message: ERROR: Cannot parse the value of the %s argument as an integer value between 1 and 65535: %s.

ID: 1189

Severity: ERROR

Message: ERROR: Cannot establish a connection to the Directory Server %s. Verify that the server is running and that the provided credentials are valid. Details: %s.

ID: 1198

Severity: ERROR

Message: An error occurred while trying to open the skip file %s for writing: %s.

ID: 1211

Severity: ERROR

Message: ERROR: You have specified the value %s for different ports.

ID: 1252

Severity: ERROR

Message: Neither the %s or the %s argument was provided. One of these arguments must be given to specify the backend for the LDIF data to be imported to.

ID: 1291

Severity: ERROR

Message: The list tag on line %d of the template file does not contain any arguments to specify the list values. At least one list value must be provided.

ID: 1293

Severity: ERROR

Message: An unexpected error occurred attempting to set the server's root directory to %s: %s.

ID: 1295

Severity: ERROR

Message: ERROR: Unable to perform SSL initialization: %s.

ID: 1296

Severity: ERROR

Message: ERROR: The provided SASL option string "%s" could not be parsed in the form "name=value".

ID: 1297

Severity: ERROR

Message: ERROR: One or more SASL options were provided, but none of them were the "mech" option to specify which SASL mechanism should be used.

ID: 1315

Severity: ERROR

Message: NOTICE: The connection to the Directory Server was closed while waiting for a response to the shutdown request. This likely means that the server has started the shutdown process.

ID: 1316

Severity: ERROR

Message: ERROR: An I/O error occurred while attempting to communicate with the Directory Server: %s.

ID: 1317

Severity: ERROR

Message: ERROR: An error occurred while trying to decode the response from the server: %s.

ID: 1318

Severity: ERROR

Message: ERROR: Expected an add response message but got a %s message instead.

ID: 1320

Severity: ERROR

Message: ERROR: argument %s is incompatible with use of this tool to interact with the directory as a client.

ID: 1321

Severity: ERROR

Message: This tool may only be used on UNIX-based systems.

ID: 1324

Severity: ERROR

Message: Unable to determine the path to the server root directory. Please ensure that the %s system property or the %s environment variable is set to the path of the server root directory.

ID: 1325

Severity: ERROR

Message: An error occurred while attempting to generate the RC script: %s.

ID: 1347

Severity: ERROR

Message: None of the Directory Server backends are configured with the requested backend ID %s.

ID: 1348

Severity: ERROR

Message: None of the entry containers are configured with the requested base DN %s in backend %s.

ID: 1352

Severity: ERROR

Message: Unable to decode base DN string "%s" as a valid distinguished name: %s.

ID: 1363

Severity: ERROR

Message: An error occurred while attempting to acquire a shared lock for backend %s: %s. This generally means that some other process has exclusive access to this backend (e.g., a restore or an LDIF import).

ID: 1374

Severity: ERROR

Message: A sub-command must be specified.

ID: 1378

Severity: ERROR

Message: The directory %s specified as the OPENDJ_JAVA_HOME path does not exist or is not a directory.

ID: 1394

Severity: ERROR

Message: The provided certificate nickname could not be found. The key store contains the following certificate nicknames: %s.

ID: 1395

Severity: ERROR

Message: The key store contains the following certificate nicknames: %s.%nYou have to provide the nickname of the certificate you want to use.

ID: 1406

Severity: ERROR

Message: You have specified several certificate types to be used. Only one certificate type (self-signed, JKS, JCEKS, PKCS#12 or PCKS#11) is allowed.

ID: 1407

Severity: ERROR

Message: You have chosen to enable SSL or StartTLS. You must specify which type of certificate you want the server to use.

ID: 1408

Severity: ERROR

Message: You must provide the PIN of the keystore to retrieve the certificate to be used by the server. You can use {%s} or {%s}.

ID: 1410

Severity: ERROR

Message: You have specified to use a certificate as server certificate. You must enable SSL (using option {%s}) or Start TLS (using option %s).

ID: 1411

Severity: ERROR

Message: The argument '%s' is incompatible with '%s'.

ID: 1422

Severity: ERROR

Message: Invalid menu item or task number '%s'.

ID: 1437

Severity: ERROR

Message: Error retrieving task entry %s: %s.

ID: 1438

Severity: ERROR

Message: There are no tasks with ID %s.

ID: 1446

Severity: ERROR

Message: Options '%s' and '%s' are incompatible with each other and cannot be used together.

ID: 1448

Severity: ERROR

Message: Error canceling task '%s': %s.

ID: 1449

Severity: ERROR

Message: Error accessing logs for task '%s': %s.

ID: 1450

Severity: ERROR

Message: Task at index %d is not cancelable.

ID: 1453

Severity: ERROR

Message: There are no tasks defined with ID '%s'.

ID: 1454

Severity: ERROR

Message: Task '%s' has finished and cannot be canceled.

ID: 1455

Severity: ERROR

Message: State for task '%s' cannot be determined.

ID: 1457

Severity: ERROR

Message: The start date/time must in YYYYMMDDhhmmssZ format for UTC time or YYYYMMDDhhmmss for local time.

ID: 1459

Severity: ERROR

Message: You have provided options for scheduling this operation as a task but options provided for connecting to the server's tasks backend resulted in the following error: '%s'.

ID: 1473

Severity: ERROR

Message: The option %s is only applicable when scheduling this operation as a task.

ID: 1474

Severity: ERROR

Message: The value %s for option %s is not a valid email address.

ID: 1475

Severity: ERROR

Message: The failed dependency action value %s is invalid. The value must be one of %s.

ID: 1476

Severity: ERROR

Message: The failed dependency action option is to be used in conjunction with one or more dependencies.

ID: 1477

Severity: ERROR

Message: Error: task %s is not in a cancelable state.

ID: 1480

Severity: ERROR

Message: Cannot write to rejected entries file %s. Verify that you have enough write rights on the file.

ID: 1483

Severity: ERROR

Message: Cannot write to skipped entries file %s. Verify that you have enough write rights on the file.

ID: 1485

Severity: ERROR

Message: The maximum number of tries to provide the certificate key store PIN is %s. Install canceled.

ID: 1491

Severity: ERROR

Message: The file properties "%s" cannot be read. Check that it exists and that you have read rights to it.

ID: 1492

Severity: ERROR

Message: The destination file "%s" cannot be written. Check that you have write rights to it.

ID: 1493

Severity: ERROR

Message: The destination file "%s" cannot be written. Check that you have right reads to it.

ID: 1497

Severity: ERROR

Message: The backend ID '%s' has been specified several times.

ID: 1498

Severity: ERROR

Message: ERROR: The empty LDAP DN is not a valid value.

ID: 1607

Severity: ERROR

Message: An error occurred while attempting to update the crypto manager in the Directory Server: %s.

ID: 1610

Severity: ERROR

Message: Cannot access trust store '%s'. Verify that the provided trust store exists and that you have read access rights to it.

ID: 1611

Severity: ERROR

Message: Cannot access key store '%s'. Verify that the provided key store exists and that you have read access rights to it.

ID: 1614

Severity: ERROR

Message: An error occurred while attempting to read the file '%s' containing the list of ignored entries: %s.

ID: 1615

Severity: ERROR

Message: An error occurred while attempting to read the file '%s' containing the list of ignored attributes: %s.

ID: 1620

Severity: ERROR

Message: An error occurred while attempting to update the administration connector port: %s.

ID: 1621

Severity: ERROR

Message: Error connecting to the directory server at %s on %s. Check this port is an administration port.

ID: 1626

Severity: ERROR

Message: Error creating JCEKS Key Provider configuration: %s.

ID: 1628

Severity: ERROR

Message: ERROR: Cannot establish a connection to the Directory Server at %s on port %s. Check this port is an administration port.

ID: 1629

Severity: ERROR

Message: ERROR: Cannot establish a connection to the Directory Server at %s on port %s. Check this port is an administration port.

ID: 1650

Severity: ERROR

Message: The target backend %s cannot be backed up to the backup directory %s: this directory is already a backup location for backend %s.

ID: 1652

Severity: ERROR

Message: An error occurred while attempting to initialize server components to run the tool: %s.

ID: 1653

Severity: ERROR

Message: The %s argument is not supported for online imports.

ID: 1667

Severity: ERROR

Message: The specified start time '%s' has already passed.

ID: 1668

Severity: ERROR

Message: An error occurred reading file '%s'. Check that the file exists and that you have read access rights to it. Details: %s.

ID: 1669

Severity: ERROR

Message: The specified stop time '%s' has already passed.

ID: 1670

Severity: ERROR

Message: Both entry DNs and a file name were provided for the compare operation. These arguments are not compatible.

ID: 1680

Severity: ERROR

Message: The timeout of '%d' seconds to start the server has been reached. You can use the argument '--%s' to increase this timeout.

ID: 1688

Severity: ERROR

Message: The value %s for threadCount cannot be parsed: %s.

ID: 1693

Severity: ERROR

Message: Provided passwords don’t matched.

ID: 1694

Severity: ERROR

Message: Cannot read password from the input: %s.

ID: 1699

Severity: ERROR

Message: Index "-i" option cannot be specified with the "--rebuildAll" option.

ID: 1701

Severity: ERROR

Message: You have specified not to create a base DN. If no base DN is to be created you cannot specify argument '%s'.

ID: 1709

Severity: ERROR

Message: The Windows Service was successfully configured but there was an error starting it. Error code starting Windows Service: %d.

ID: 1713

Severity: ERROR

Message: An error occurred while attempting to write entry to LDIF: Could not calculate the DN for the entry (no value found for the RDN attribute %s).

ID: 1714

Severity: ERROR

Message: A client side timeout occurred.%nAdditional Information: %s.

ID: 1718

Severity: ERROR

Message: The provided schedule value has an invalid format. The schedule must be expressed using a crontab(5) format. Error details: %s.

ID: 1721

Severity: ERROR

Message: Option "--rebuildDegraded" cannot be specified with the "--%s" option.

ID: 1722

Severity: ERROR

Message: Option "--rebuildAll" cannot be specified with the "--%s" option.

ID: 1733

Severity: ERROR

Message: An error occurred while attempting to update the FQDN for the DIGEST-MD5 SASL mechanism: %s.

ID: 1737

Severity: ERROR

Message: The version of the installed OpenDJ could not be determined because the version file '%s' could not be found. Restore it from backup before continuing.

ID: 1738

Severity: ERROR

Message: The version of the installed OpenDJ could not be determined because the version file '%s' exists but contains invalid data. Restore it from backup before continuing.

ID: 1739

Severity: ERROR

Message: The OpenDJ binary version '%s' does not match the installed version '%s'. Please run upgrade before continuing.

ID: 1800

Severity: ERROR

Message: The upgrade failed to complete for the following reason: %s.

ID: 1805

Severity: ERROR

Message: OpenDJ cannot be upgraded because the server is currently running. Please stop the server and try again.

ID: 1806

Severity: ERROR

Message: OpenDJ has already been upgraded to version %s.

ID: 1807

Severity: ERROR

Message: An unexpected error occurred while attempting to display a notification: %s.

ID: 1808

Severity: ERROR

Message: An unexpected error occurred while attempting to display a confirmation : %s.

ID: 1812

Severity: ERROR

Message: An error occurred while performing an upgrade task: %s.

ID: 1816

Severity: ERROR

Message: No %s with OID %s exists in the schema.

ID: 1817

Severity: ERROR

Message: An error occurred when trying to upgrade the config/upgrade folder: %s.

ID: 1827

Severity: ERROR

Message: The upgrade failed because %d errors were encountered. Please check log for further details.

ID: 1828

Severity: ERROR

Message: An error occurred while copying the schema file '%s': %s.

ID: 1829

Severity: ERROR

Message: An error occurred while adding one or more attributes to the schema file '%s': %s.

ID: 1830

Severity: ERROR

Message: An error occurred while adding one or more object classes to the schema file '%s': %s.

ID: 1835

Severity: ERROR

Message: An error occurred while adding configuration file '%s': %s.

ID: 1838

Severity: ERROR

Message: An error occurred when trying to rename the SNMP security config file: %s.

ID: 1843

Severity: ERROR

Message: An error occurred during post upgrade task. Process aborted. Please check log for further details.

ID: 1846

Severity: ERROR

Message: Invalid log file %s.

ID: 1850

Severity: ERROR

Message: '%s' is missing or empty, it is probably corrupted.

ID: 1853

Severity: ERROR

Message: The dsjavaproperties tool failed to run. Please rerun dsjavaproperties manually.

ID: 1863

Severity: ERROR

Message: An error occurred while listing the base DNs: %s.

ID: 1864

Severity: ERROR

Message: An error occurred while listing indexes: %s.

ID: 1865

Severity: ERROR

Message: An unexpected error occurred while attempting to initialize the backend '%s': %s.

ID: 1866

Severity: ERROR

Message: An unexpected error occurred while attempting to read and/or decode records from an index: %s.

ID: 1868

Severity: ERROR

Message: No index exists with the requested name '%s' in base DN '%s' and backend '%s'.

ID: 1869

Severity: ERROR

Message: Cannot specify a minimum key both as a string and as an hexadecimal string.

ID: 1870

Severity: ERROR

Message: Cannot specify a maximum key both as a string and as an hexadecimal string.

ID: 1871

Severity: ERROR

Message: An error occurred while processing arguments: %s.

ID: 1872

Severity: ERROR

Message: An error occurred while trying to execute %s: %s.

ID: 1881

Severity: ERROR

Message: Cannot configure backend %s: %s.

ID: 1887

Severity: ERROR

Message: At key number %d, %s:.

ID: 1890

Severity: ERROR

Message: Data decoder for printing is not available, should use hex dump.

ID: 1891

Severity: ERROR

Message: No storage index exists with the requested name %s in backend %s.

ID: 1897

Severity: ERROR

Message: An error occurred while initializing server backends: %s.

ID: 1898

Severity: ERROR

Message: An error occurred while initializing plugins: %s.

ID: 1899

Severity: ERROR

Message: Subsystem %s should be initialized first.

ID: 1901

Severity: ERROR

Message: StartTLS failed: the connection has been closed without receiving a response. This may indicate you tried to connect to an LDAPS port instead of the LDAP port, or that the network is down.

ID: 10020

Severity: ERROR

Message: ERROR: The server rejected the task for the following reason: %s.

ID: 10055

Severity: ERROR

Message: Unable to access the LDIF file %s to import. Please check that the file is local to the server and the path correct.

ID: 20009

Severity: ERROR

Message: The backend type '%s' is not recognized. The supported backend types are %s.

ID: 20010

Severity: ERROR

Message: The backend type '%s' is not recognized. The supported backend types are %s.

ID: 20011

Severity: ERROR

Message: An error occurred while trying to create userRoot backend type %s. Error message: %s.

ID: 20013

Severity: ERROR

Message: The local instance is not configured or you do not have permissions to access it.

ID: 20014

Severity: ERROR

Message: Invalid deref alias specified: %s.

ID: 20015

Severity: ERROR

Message: Could not completely read file '%s'.

Log Message Category: UTILITY

ID: 1

Severity: ERROR

Message: The value %s cannot be base64-decoded because it does not have a length that is a multiple of four bytes.

ID: 2

Severity: ERROR

Message: The value %s cannot be base64-decoded because it contains an illegal character %c that is not allowed in base64-encoded values.

ID: 3

Severity: ERROR

Message: The value %s cannot be decoded as a hexadecimal string because it does not have a length that is a multiple of two bytes.

ID: 4

Severity: ERROR

Message: The value %s cannot be decoded as a hexadecimal string because it contains an illegal character %c that is not a valid hexadecimal digit.

ID: 5

Severity: ERROR

Message: Unable to parse line %d ("%s") from the LDIF source because the line started with a space but there were no previous lines in the entry to which this line could be appended.

ID: 6

Severity: ERROR

Message: Unable to parse LDIF entry starting at line %d because the line "%s" does not include an attribute name.

ID: 7

Severity: ERROR

Message: Unable to parse LDIF entry starting at line %d because the first line does not contain a DN (the first line was "%s".

ID: 9

Severity: ERROR

Message: Unable to parse LDIF entry starting at line %d because an error occurred while trying to parse the value of line "%s" as a distinguished name: %s.

ID: 11

Severity: ERROR

Message: Unable to parse LDIF entry starting at line %d because it was not possible to base64-decode the DN on line "%s": %s.

ID: 12

Severity: ERROR

Message: Unable to parse LDIF entry %s starting at line %d because it was not possible to base64-decode the attribute on line "%s": %s.

ID: 15

Severity: ERROR

Message: Entry %s starting at line %d includes multiple values for single-valued attribute %s.

ID: 17

Severity: ERROR

Message: Entry %s read from LDIF starting at line %d is not valid because it violates the server's schema configuration: %s.

ID: 18

Severity: ERROR

Message: The specified LDIF file %s already exists and the export configuration indicates that no attempt should be made to append to or replace the file.

ID: 19

Severity: ERROR

Message: Unable to parse LDIF entry %s starting at line %d because the value of attribute %s was to be read from a URL but the URL was invalid: %s.

ID: 20

Severity: ERROR

Message: Unable to parse LDIF entry %s starting at line %d because the value of attribute %s was to be read from URL %s but an error occurred while trying to read that content: %s.

ID: 21

Severity: ERROR

Message: The specified reject file %s already exists and the import configuration indicates that no attempt should be made to append to or replace the file.

ID: 22

Severity: ERROR

Message: An error occurred while attempting to determine whether LDIF entry "%s" starting at line %d should be imported as a result of the include and exclude filter configuration: %s.

ID: 23

Severity: ERROR

Message: An error occurred while attempting to determine whether LDIF entry "%s" should be exported as a result of the include and exclude filter configuration: %s.

ID: 24

Severity: ERROR

Message: Error in the LDIF change record entry. Invalid attributes specified for the delete operation.

ID: 25

Severity: ERROR

Message: Error in the LDIF change record entry. No attributes specified for the mod DN operation.

ID: 26

Severity: ERROR

Message: Error in the LDIF change record entry. No delete old RDN attribute specified for the mod DN operation.

ID: 27

Severity: ERROR

Message: Error in the LDIF change record entry. Invalid value "%s" for the delete old RDN attribute specified for the mod DN operation.

ID: 28

Severity: ERROR

Message: Error in the LDIF change record entry. Invalid attribute "%s" specified. Expecting attribute "%s".

ID: 29

Severity: ERROR

Message: Error in the LDIF change record entry. Invalid attribute "%s" specified. Expecting one of the following attributes "%s".

ID: 30

Severity: ERROR

Message: Error in the LDIF change record entry. Invalid value "%s" for the changetype specified. Expecting one of the following values "%s".

ID: 32

Severity: ERROR

Message: The provided value could not be parsed to determine whether it contained a valid schema element name or OID because it was null or empty.

ID: 33

Severity: ERROR

Message: The provided value "%s" does not contain a valid schema element name or OID because it contains an illegal character %c at position %d.

ID: 34

Severity: ERROR

Message: The provided value "%s" does not contain a valid schema element name or OID because the numeric OID contains two consecutive periods at position %d.

ID: 72

Severity: ERROR

Message: The file to move %s does not exist.

ID: 73

Severity: ERROR

Message: The file to move %s exists but is not a file.

ID: 74

Severity: ERROR

Message: The target directory %s does not exist.

ID: 75

Severity: ERROR

Message: The target directory %s exists but is not a directory.

ID: 76

Severity: ERROR

Message: The provided sender address %s is invalid: %s.

ID: 77

Severity: ERROR

Message: The provided recipient address %s is invalid: %s.

ID: 78

Severity: ERROR

Message: The specified e-mail message could not be sent using any of the configured mail servers.

ID: 110

Severity: ERROR

Message: The provided string "%s" cannot be decoded as an LDAP URL because it does not contain the necessary :// component to separate the scheme from the rest of the URL.

ID: 111

Severity: ERROR

Message: The provided string "%s" cannot be decoded as an LDAP URL because it does not contain a protocol scheme.

ID: 112

Severity: ERROR

Message: The provided string "%s" cannot be decoded as an LDAP URL because it does not contain a host before the colon to specify the port number.

ID: 113

Severity: ERROR

Message: The provided string "%s" cannot be decoded as an LDAP URL because it does not contain a port number after the colon following the host.

ID: 114

Severity: ERROR

Message: The provided string "%s" cannot be decoded as an LDAP URL because the port number portion %s cannot be decoded as an integer.

ID: 115

Severity: ERROR

Message: The provided string "%s" cannot be decoded as an LDAP URL because the provided port number %d is not within the valid range between 1 and 65535.

ID: 116

Severity: ERROR

Message: The provided string "%s" cannot be decoded as an LDAP URL because the scope string %s was not one of the allowed values of base, one, sub, or subordinate.

ID: 117

Severity: ERROR

Message: The provided URL component "%s" could not be decoded because the percent character at byte %d was not followed by two hexadecimal digits.

ID: 118

Severity: ERROR

Message: The provided URL component "%s" could not be decoded because the character at byte %d was not a valid hexadecimal digit.

ID: 119

Severity: ERROR

Message: An error occurred while attempting to represent a byte array as a UTF-8 string during the course of decoding a portion of an LDAP URL: %s.

ID: 120

Severity: ERROR

Message: Cannot decode value "%s" as a named character set because it does not contain a colon to separate the name from the set of characters.

ID: 121

Severity: ERROR

Message: The named character set is invalid because it does not contain a name.

ID: 122

Severity: ERROR

Message: The named character set is invalid because the provide name "%s" has an invalid character at position %d. Only ASCII alphabetic characters are allowed in the name.

ID: 123

Severity: ERROR

Message: Cannot decode value "%s" as a named character set because it does not contain a name to use for the character set.

ID: 124

Severity: ERROR

Message: Cannot decode value "%s" as a named character set because there are no characters to include in the set.

ID: 141

Severity: ERROR

Message: Unable to set permissions for file %s because it does not exist.

ID: 143

Severity: ERROR

Message: One or more exceptions were thrown in the process of updating the file permissions for %s. Some of the permissions for the file may have been altered.

ID: 146

Severity: ERROR

Message: The provided string %s does not represent a valid UNIX file mode. UNIX file modes must be a three-character string in which each character is a numeric digit between zero and seven.

ID: 147

Severity: ERROR

Message: The %s command will not be allowed because the Directory Server has been configured to refuse the use of the exec method.

ID: 157

Severity: ERROR

Message: Failed to rename file %s to %s.

ID: 158

Severity: ERROR

Message: Failed to delete target file %s. Make sure the file is not currently in use by this or another application.

ID: 159

Severity: ERROR

Message: Refusing to trust client or issuer certificate '%s' because it expired on %s.

ID: 160

Severity: ERROR

Message: Refusing to trust client or issuer certificate '%s' because it is not valid until %s.

ID: 161

Severity: ERROR

Message: Refusing to trust server or issuer certificate '%s' because it expired on %s.

ID: 162

Severity: ERROR

Message: Refusing to trust server or issuer certificate '%s' because it is not valid until %s.

ID: 164

Severity: ERROR

Message: The specified skip file %s already exists and the import configuration indicates that no attempt should be made to append to or replace the file.

ID: 165

Severity: ERROR

Message: Skipping entry %s because the DN is not one that should be included based on the include and exclude branches.

ID: 167

Severity: ERROR

Message: The Directory Server cannot be started because it is already running.

ID: 181

Severity: ERROR

Message: The file %s specified as the body file for the e-mail message does not exist.

ID: 182

Severity: ERROR

Message: An error occurred while attempting to process message body file %s: %s.

ID: 183

Severity: ERROR

Message: The attachment file %s does not exist.

ID: 184

Severity: ERROR

Message: An error occurred while trying to attach file %s: %s.

ID: 185

Severity: ERROR

Message: An error occurred while trying to send the e-mail message: %s.

ID: 196

Severity: ERROR

Message: An error occurred while attempting to read the raw data to encode: %s.

ID: 197

Severity: ERROR

Message: An error occurred while attempting to write the encoded data: %s.

ID: 198

Severity: ERROR

Message: An error occurred while attempting to read the base64-encoded data: %s.

ID: 199

Severity: ERROR

Message: An error occurred while attempting to write the decoded data: %s.

ID: 200

Severity: ERROR

Message: Unknown subcommand %s.

ID: 224

Severity: ERROR

Message: Rejecting entry %s because it was rejected by a plugin.

ID: 225

Severity: ERROR

Message: Rejecting entry %s because it was rejected by a plugin: %s.

ID: 237

Severity: ERROR

Message: The hostname "%s" could not be resolved. Please check you have provided the correct address.

ID: 238

Severity: ERROR

Message: Invalid port number "%s". Please enter a valid port number between 1 and 65535.

ID: 244

Severity: ERROR

Message: The provided path is not valid.

ID: 267

Severity: ERROR

Message: Confirmation tries limit reached (%d).

ID: 268

Severity: ERROR

Message: Unexpected error. Details: %s.

ID: 269

Severity: ERROR

Message: Input tries limit reached (%d).

ID: 271

Severity: ERROR

Message: Unable to parse LDIF entry %s starting at line %d because it has an invalid binary option for attribute %s.

ID: 272

Severity: ERROR

Message: Invalid key store path for PKCS11 keystore, it must be %s.

ID: 273

Severity: ERROR

Message: Key store path %s exists but is not a file.

ID: 274

Severity: ERROR

Message: Parent directory for key store path %s does not exist or is not a directory.

ID: 275

Severity: ERROR

Message: Invalid key store type, it must be one of the following: %s, %s, %s or %s.

ID: 276

Severity: ERROR

Message: Keystore does not exist, it must exist to retrieve an alias, delete an alias or generate a certificate request.

ID: 277

Severity: ERROR

Message: Validity value %d is invalid, it must be a positive integer.

ID: 278

Severity: ERROR

Message: A certificate with the alias %s already exists in the key store.

ID: 279

Severity: ERROR

Message: The following error occurred when adding a certificate with alias %s to the keystore: %s.

ID: 280

Severity: ERROR

Message: The alias %s cannot be added to the keystore for one of the following reasons: it already exists in the keystore, or, it is not an instance of a trusted certificate class.

ID: 281

Severity: ERROR

Message: The alias %s is an instance of a private key entry, which is not supported being added to the keystore at this time.

ID: 282

Severity: ERROR

Message: The following error occurred when deleting a certificate with alias %s from the

keystore: %s.

ID: 284

Severity: ERROR

Message: The following error occurred when generating a self-signed certificate using the alias %s: %s.

ID: 285

Severity: ERROR

Message: The certificate file %s is invalid because it does not exists, or exists, but is not a file.

ID: 286

Severity: ERROR

Message: The alias %s cannot be deleted from the keystore because it does not exist.

ID: 292

Severity: ERROR

Message: The trusted certificate associated with alias %s could not be added to keystore because of the following reason: %s.

ID: 293

Severity: ERROR

Message: The %s is invalid because it is null.

ID: 294

Severity: ERROR

Message: The argument %s is invalid because it is either null, or has zero length.

ID: 295

Severity: ERROR

Message: A security class cannot be found in this JVM because of the following reason: %s.

ID: 296

Severity: ERROR

Message: The security classes could not be initialized because of the following reason: %s.

ID: 297

Severity: ERROR

Message: A method needed in the security classes could not be located because of the following reason: %s.

ID: 298

Severity: ERROR

Message: The CertAndKeyGen security class cannot be found, consider setting -D%s=.

ID: 301

Severity: ERROR

Message: Skipping entry %s because the following error was received when reading its attributes: %s.

ID: 305

Severity: ERROR

Message: An error occurred while attempting to obtain the %s MAC provider to create the signed hash for the backup: %s.

ID: 306

Severity: ERROR

Message: An error occurred while attempting to obtain the %s message digest to create the hash for the backup: %s.

ID: 307

Severity: ERROR

Message: An error occurred while trying to create the archive file %s in directory %s for the backup %s: %s.

ID: 308

Severity: ERROR

Message: An error occurred while attempting to obtain the cipher to use to encrypt the backup: %s.

ID: 309

Severity: ERROR

Message: %s backup %s.

ID: 310

Severity: ERROR

Message: An error occurred while attempting to obtain a list of the files in directory %s to include in the backup: %s.

ID: 311

Severity: ERROR

Message: An error occurred while attempting to back up file %s of backup %s: %s.

ID: 312

Severity: ERROR

Message: An error occurred while trying to close the archive file %s in directory %s: %s.

ID: 313

Severity: ERROR

Message: The computed hash of backup %s is different to the value computed at time of backup.

ID: 314

Severity: ERROR

Message: The computed signed hash of backup %s is different to the value computed at time of backup.

ID: 315

Severity: ERROR

Message: The directory %s, containing the files restored from backup, could not be renamed to the directory %s.

ID: 316

Severity: ERROR

Message: An error occurred while attempting to update the backup descriptor file %s with information about the backup: %s.

ID: 317

Severity: ERROR

Message: An error occurred while attempting to restore the files from backup %s: %s.

ID: 323

Severity: ERROR

Message: An error occurred while attempting to obtain the MAC key ID to create the signed hash for the backup %s : %s.

ID: 324

Severity: ERROR

Message: An error occurred while attempting to create a directory to restore the file %s for backup of %s.

ID: 325

Severity: ERROR

Message: An error occurred while attempting to save files from root directory %s to target directory %s, for backup of %s : %s.

ID: 326

Severity: ERROR

Message: An error occurred while attempting to create a save directory with base path %s before restore of backup of %s: %s.