

## File integrity monitoring report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	wazuh_agent_ubuntu	172.20.0.8	Wazuh v4.9.0	wazuh-manager-4.9.0-7102	Ubuntu 22.04.3 LTS	May 14, 2024 @ 14:50:11.000	May 16, 2024 @ 15:11:57.000

Group: default

Alerts related to file changes, including permissions, content, ownership and attributes.

🕒 2024-04-16T17:12:02 to 2024-05-16T17:12:02

🔍 rule.groups: syscheck AND cluster.name: wazuh AND agent.id: 001

Last file integrity monitoring scan was executed from 2024-05-16T08:39:27+00:00 to 2024-05-16T08:39:37+00:00.

### Last 10 deleted files

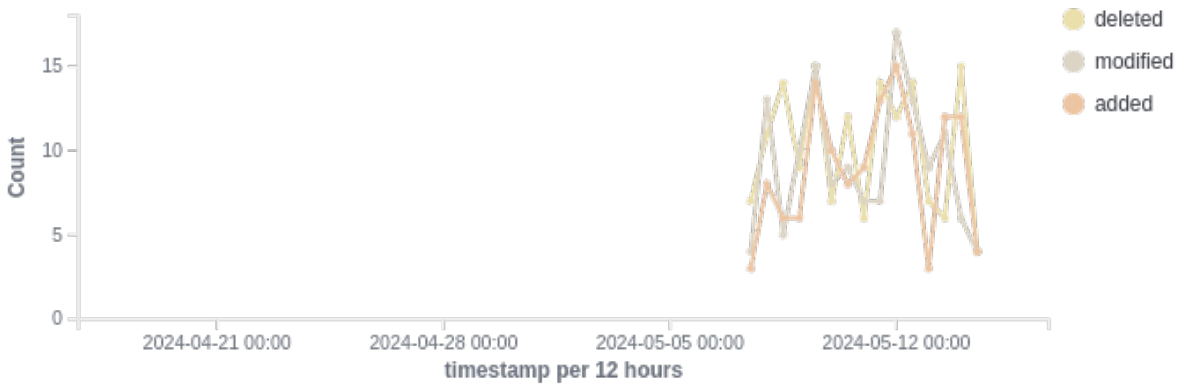
Path	Date
/etc/resolv.conf	2024-05-14T15:54:30.237Z
/var/osquery/osquery.db/CURRENT	2024-05-14T14:46:19.724Z
/var/wazuh/queue/fim/db/fim.db-journal	2024-05-14T11:17:36.700Z
/etc/elasticsearch/elasticsearch.yml	2024-05-14T08:43:36.912Z
/etc/filebeat/fields.yml	2024-05-14T08:13:12.874Z
/etc/sysconfig/network-scripts/ifcfg-eth1	2024-05-14T06:43:31.700Z
/var/log/lastlog	2024-05-14T06:30:46.057Z
/tmp/agent.conf	2024-05-14T03:49:24.778Z
/tmp/wazuh-config	2024-05-14T00:27:10.561Z
/run/utmp	2024-05-13T17:55:32.503Z

### Last 10 modified files

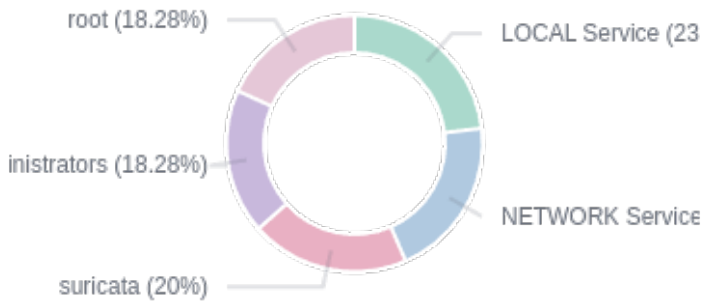
Path	Date
/tmp/wazuh-config	2024-05-14T15:53:36.893Z
/etc/sysconfig/network-scripts/ifcfg-eth1	2024-05-14T14:47:06.841Z
/var/log/lastlog	2024-05-14T13:53:28.541Z
/etc/elasticsearch/users	2024-05-14T12:05:31.982Z
/etc/filebeat/fields.yml	2024-05-14T08:04:28.521Z
/var/osquery/osquery.db/CURRENT	2024-05-14T06:13:20.503Z

Path	Date
/etc/resolv.conf	2024-05-14T03:15:32.591Z
/etc/elasticsearch/elasticsearch.yml	2024-05-13T20:16:06.012Z
/var/wazuh/queue/fim/db/fim.db-journal	2024-05-13T17:34:52.560Z
/etc/elasticsearch/config	2024-05-13T15:30:24.999Z

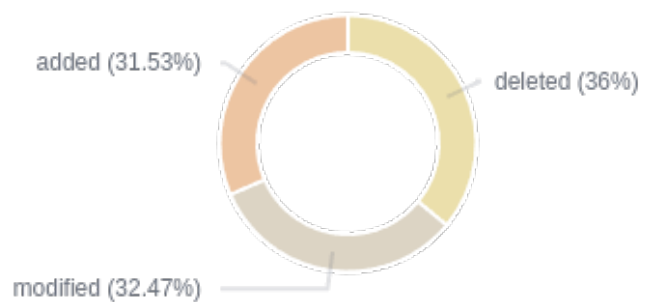
## Events



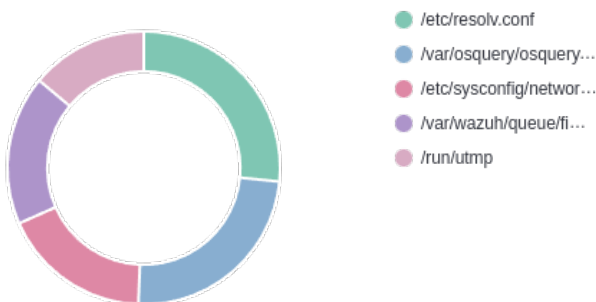
## Most active users



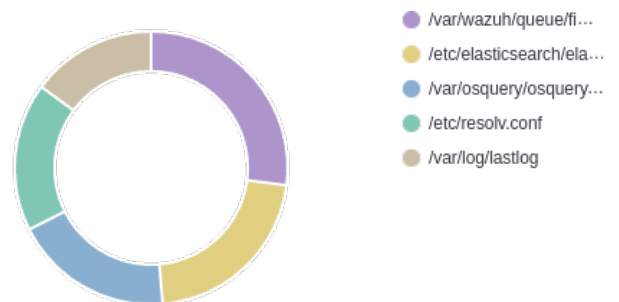
## Actions



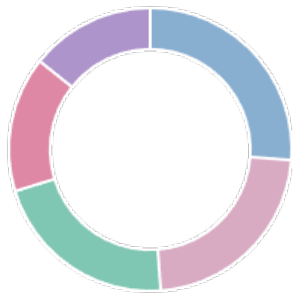
## Files added



## Files modified



## Files deleted



- /var/osquery/osquery...
- /run/utmp
- /etc/resolv.conf
- /etc/sysconfig/networ...
- /var/wazuh/queue/fi...

## Alerts summary

Path	Description	Count
/var/osquery/osquery.db/CURRENT	File deleted.	22
/etc/resolv.conf	File added to the system.	21
/var/wazuh/queue/fim/db/fim.db	Integrity checksum changed.	20
/var/osquery/osquery.db/CURRENT	File added to the system.	19
/run/utmp	File deleted.	19
/etc/resolv.conf	File deleted.	18
/etc/elasticsearch/elasticsearch.yml	Integrity checksum changed.	16
/var/osquery/osquery.db/CURRENT	Integrity checksum changed.	14
/var/wazuh/queue/fim/db/fim.db	File added to the system.	14
/etc/sysconfig/network-scripts/ifcfg-eth1	File added to the system.	14
/etc/resolv.conf	Integrity checksum changed.	13
/etc/sysconfig/network-scripts/ifcfg-eth1	File deleted.	13
/var/wazuh/queue/fim/db/fim.db	File deleted.	12
/run/utmp	File added to the system.	11
/var/log/lastlog	File added to the system.	11
/var/log/lastlog	Integrity checksum changed.	11
/tmp/agent.conf	File deleted.	11
/run/utmp	Integrity checksum changed.	10
/etc/elasticsearch/config	File deleted.	10
/etc/elasticsearch/config	Integrity checksum changed.	10
/etc/filebeat/fields.yml	File deleted.	10
/etc/elasticsearch/users	File deleted.	10
/tmp/agent.conf	File added to the system.	9
/var/wazuh/queue/fim/db/fim.db-journal	File added to the system.	9
/var/wazuh/queue/fim/db/fim.db-journal	Integrity checksum changed.	9
/etc/sysconfig/network-scripts/ifcfg-eth1	Integrity checksum changed.	8
/etc/elasticsearch/users	Integrity checksum changed.	8
/tmp/wazuh-config	File deleted.	8
/tmp/wazuh-config	Integrity checksum changed.	8
/etc/elasticsearch/elasticsearch.yml	File added to the system.	7
/etc/elasticsearch/elasticsearch.yml	File deleted.	7
/var/log/lastlog	File deleted.	7
/etc/filebeat/fields.yml	File added to the system.	7
/etc/filebeat/fields.yml	Integrity checksum changed.	7
/etc/elasticsearch/config	File added to the system.	6
/var/wazuh/queue/fim/db/fim.db-journal	File deleted.	6
-	Registry Entry Deleted.	6
/etc/elasticsearch/users	File added to the system.	5
/tmp/agent.conf	Integrity checksum changed.	4

Path	Description	Count
-	File deleted.	3
-	Registry Integrity Checksum Changed	2
/tmp/wazuh-config	File added to the system.	1
-	Integrity checksum changed.	1