Microsoft

Azure Landing Zones

31st January 2023 - External Community Call

Registration:
https://aka.ms/ALZ/CommunityCallRegister

Agenda (please add suggestions):
https://aka.ms/ALZ/CommunityCallAgenda

Microsoft

This meeting is being recorded

Agenda

- Welcome
- What’s New Highlights
- Multi-Tenant ALZ Updates
- Updating ALZ (aka Evergreen) Updates
- AzGovViz & AzAdvertizer Updates
- Sub Vending Updates
- Contributing To ALZ (ESLZ) Repo
- CARML
- RBAC Constrained Delegation Overview
- Q & A

Before we get started...

At any point, if you have a question please put it in the chat!

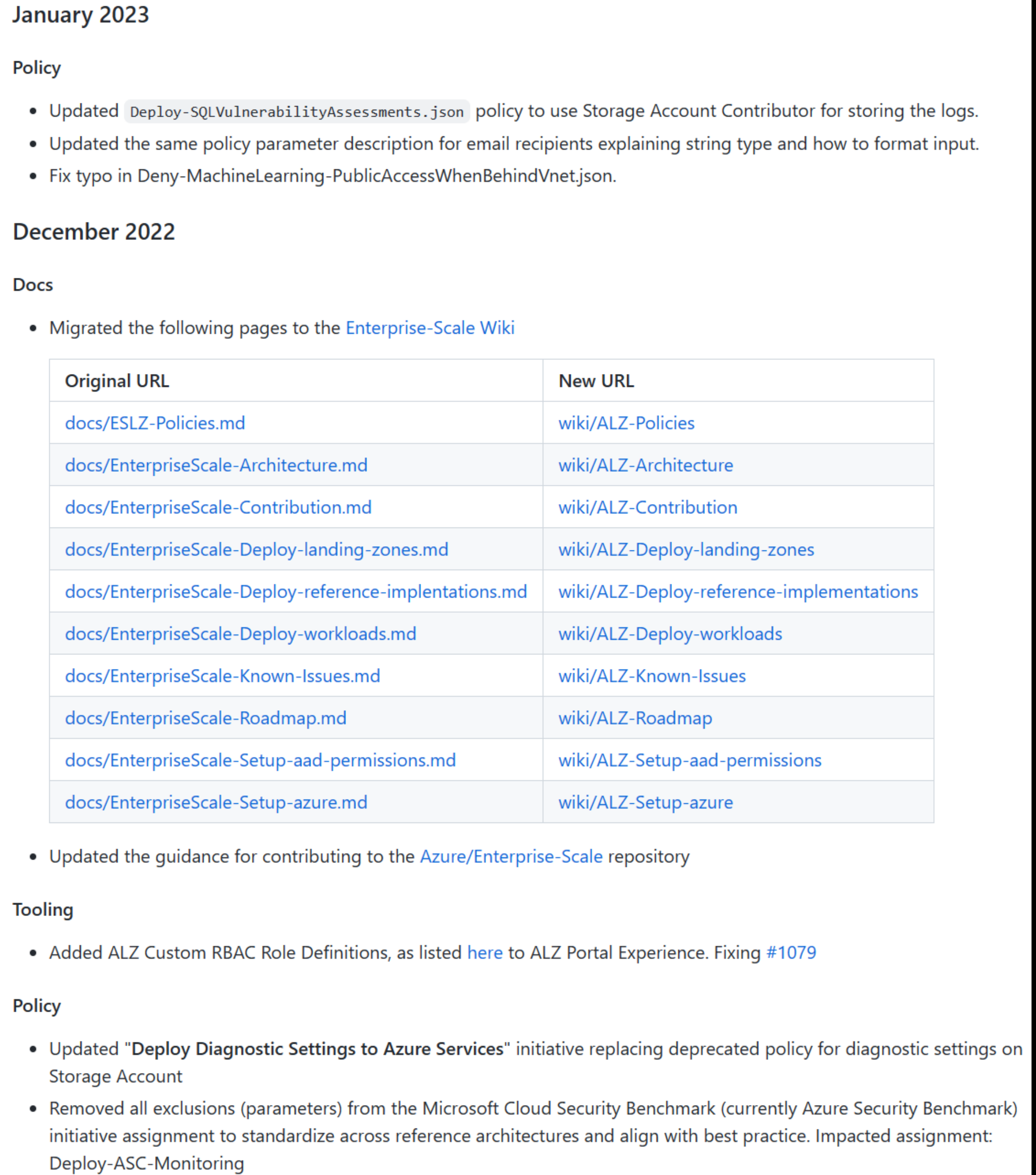
(we have members of the team here to help 😎)

Also we may stop and discuss your question/point at that time, we want this to be an open discussion with all of you ☺

ALZ What's New?

https://aka.ms/ALZ/WhatsNew

Single place to stay up-to-date



January 2023

Policy

- Updated `Deploy-SQLVulnerabilityAssessments.json` policy to use Storage Account Contributor for storing the logs.
- Updated the same policy parameter description for email recipients explaining string type and how to format input.
- Fix typo in Deny-MachineLearning-PublicAccessWhenBehindVnet.json.

December 2022

Docs

- Migrated the following pages to the Enterprise-Scale Wiki

Original URL	New URL
docs/ESLZ-Policies.md	wiki/ALZ-Policies
docs/EnterpriseScale-Architecture.md	wiki/ALZ-Architecture
docs/EnterpriseScale-Contribution.md	wiki/ALZ-Contribution
docs/EnterpriseScale-Deploy-landing-zones.md	wiki/ALZ-Deploy-landing-zones
docs/EnterpriseScale-Deploy-reference-implentations.md	wiki/ALZ-Deploy-reference-implementations
docs/EnterpriseScale-Deploy-workloads.md	wiki/ALZ-Deploy-workloads
docs/EnterpriseScale-Known-Issues.md	wiki/ALZ-Known-Issues
docs/EnterpriseScale-Roadmap.md	wiki/ALZ-Roadmap
docs/EnterpriseScale-Setup-aad-permissions.md	wiki/ALZ-Setup-aad-permissions
docs/EnterpriseScale-Setup-azure.md	wiki/ALZ-Setup-azure

- Updated the guidance for contributing to the Azure/Enterprise-Scale repository

Tooling

- Added ALZ Custom RBAC Role Definitions, as listed here to ALZ Portal Experience. Fixing #1079

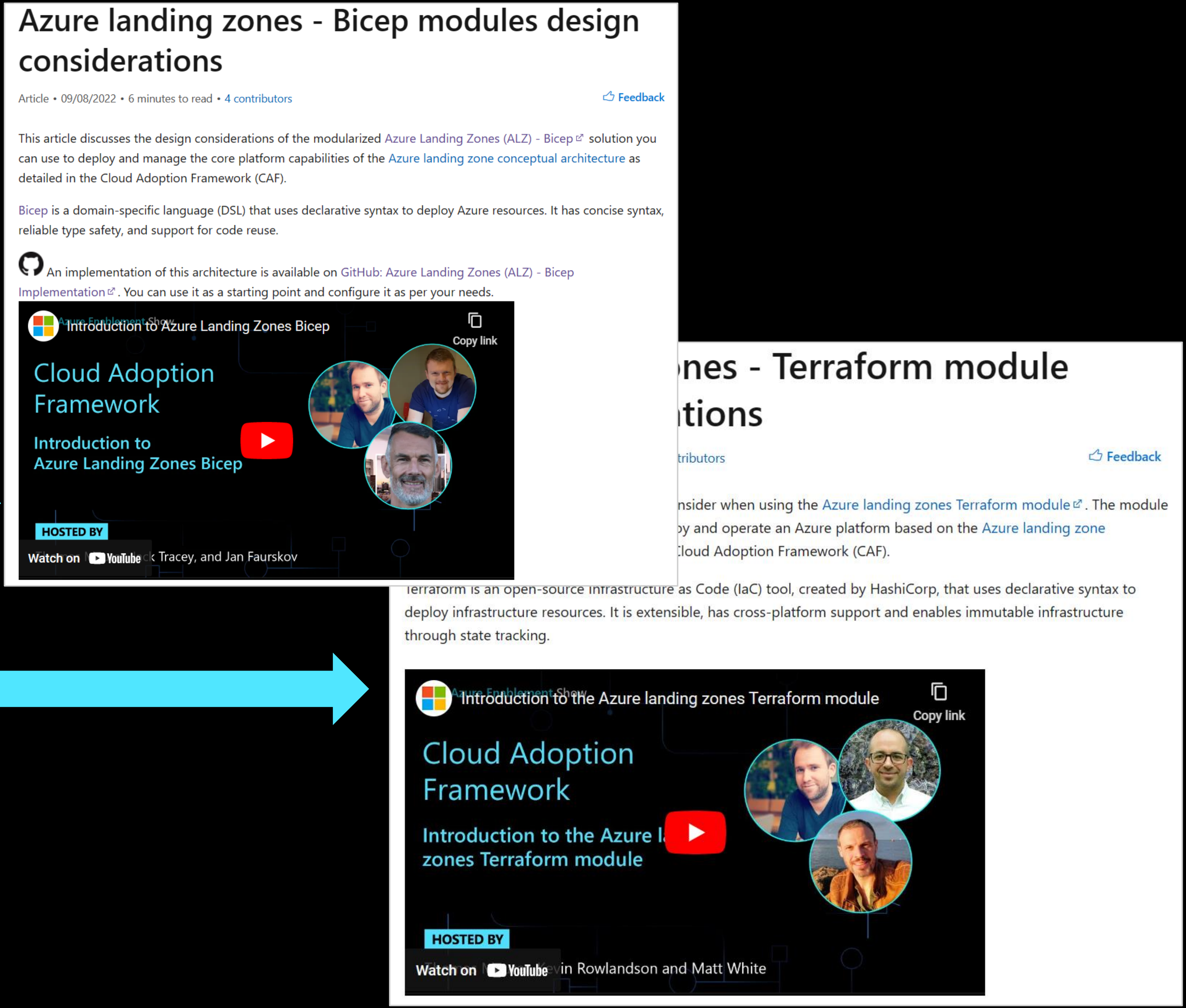
Policy

- Updated "**Deploy Diagnostic Settings to Azure Services**" initiative replacing deprecated policy for diagnostic settings on Storage Account
- Removed all exclusions (parameters) from the Microsoft Cloud Security Benchmark (currently Azure Security Benchmark) initiative assignment to standardize across reference architectures and align with best practice. Impacted assignment: Deploy-ASC-Monitoring

AAC & Azure Enablement Shows

ALZ Bicep AAC & Azure Enablement Show
aka.ms/alz/aac/bicep

ALZ Terraform AAC & Azure Enablement Show
aka.ms/alz/aac/tf



Azure landing zones - Bicep modules design considerations

Article • 09/08/2022 • 6 minutes to read • 4 contributors

Feedback

This article discusses the design considerations of the modularized Azure Landing Zones (ALZ) - Bicep solution you can use to deploy and manage the core platform capabilities of the Azure landing zone conceptual architecture as detailed in the Cloud Adoption Framework (CAF).

Bicep is a domain-specific language (DSL) that uses declarative syntax to deploy Azure resources. It has concise syntax, reliable type safety, and support for code reuse.

An implementation of this architecture is available on GitHub: Azure Landing Zones (ALZ) - Bicep Implementation. You can use it as a starting point and configure it as per your needs.

Azure Enablement Show
Introduction to Azure Landing Zones Bicep
Copy link
Cloud Adoption Framework
Introduction to Azure Landing Zones Bicep
HOSTED BY
Watch on YouTube
k Tracey, and Jan Faurskov

nes - Terraform module tions

tributors

Feedback

nsider when using the Azure landing zones Terraform module. The module oy and operate an Azure platform based on the Azure landing zone Cloud Adoption Framework (CAF).

Terraform is an open-source infrastructure as Code (IaC) tool, created by HashiCorp, that uses declarative syntax to deploy infrastructure resources. It is extensible, has cross-platform support and enables immutable infrastructure through state tracking.

Azure Enablement Show
Introduction to the Azure landing zones Terraform module
Copy link
Cloud Adoption Framework
Introduction to the Azure l zones Terraform module
HOSTED BY
Watch on YouTube
in Rowlandson and Matt White

ALZ Policy Updates

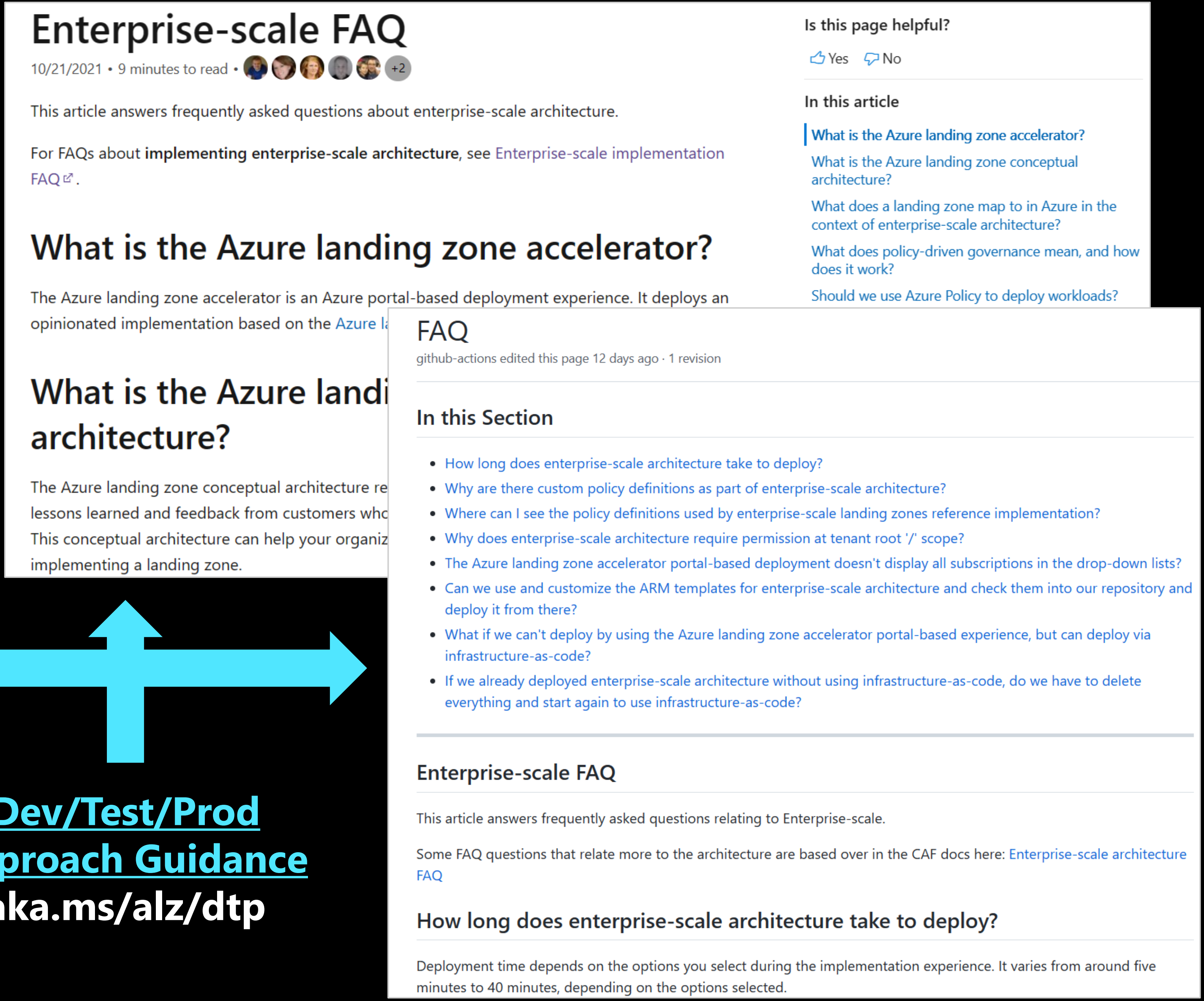
- We have updated a lot of policies over the last 6 months with fixes and enhancements
- We have finally split up policies.json into individual .json files
  - These are then compiled into policies.json via policies.bicep
  - Checkout aka.ms/alz/contribute
- In the middle of updating ALZ default policy assignments
  - Planning to complete by end of March (latest)
  - See aka.ms/alz/policies for current default assignments and this will get updated when we release
  - Adding default Sandbox & Decommissioned assignments (much asked for)

Updated & New FAQ pages

Enterprise-scale FAQ - Cloud Adoption Framework | Microsoft Docs – Architecture

FAQ · Azure/Enterprise-Scale Wiki (github.com) – Implementation

Dev/Test/Prod Approach Guidance
aka.ms/alz/dtp



Enterprise-scale FAQ

10/21/2021 • 9 minutes to read • +2

This article answers frequently asked questions about enterprise-scale architecture.

For FAQs about **implementing enterprise-scale architecture**, see Enterprise-scale implementation FAQ.

What is the Azure landing zone accelerator?

The Azure landing zone accelerator is an Azure portal-based deployment experience. It deploys an opinionated implementation based on the Azure la

What is the Azure landi architecture?

The Azure landing zone conceptual architecture re lessons learned and feedback from customers whc This conceptual architecture can help your organiz implementing a landing zone.

In this article

- What is the Azure landing zone accelerator?
- What is the Azure landing zone conceptual architecture?
- What does a landing zone map to in Azure in the context of enterprise-scale architecture?
- What does policy-driven governance mean, and how does it work?
- Should we use Azure Policy to deploy workloads?

FAQ

github-actions edited this page 12 days ago · 1 revision

In this Section

- How long does enterprise-scale architecture take to deploy?
- Why are there custom policy definitions as part of enterprise-scale architecture?
- Where can I see the policy definitions used by enterprise-scale landing zones reference implementation?
- Why does enterprise-scale architecture require permission at tenant root '/' scope?
- The Azure landing zone accelerator portal-based deployment doesn't display all subscriptions in the drop-down lists?
- Can we use and customize the ARM templates for enterprise-scale architecture and check them into our repository and deploy it from there?
- What if we can't deploy by using the Azure landing zone accelerator portal-based experience, but can deploy via infrastructure-as-code?
- If we already deployed enterprise-scale architecture without using infrastructure-as-code, do we have to delete everything and start again to use infrastructure-as-code?

Enterprise-scale FAQ

This article answers frequently asked questions relating to Enterprise-scale.

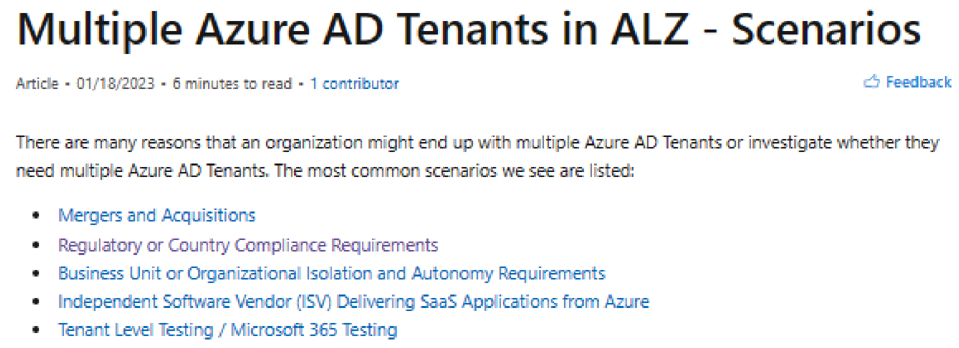
Some FAQ questions that relate more to the architecture are based over in the CAF docs here: Enterprise-scale architecture FAQ

How long does enterprise-scale architecture take to deploy?

Deployment time depends on the options you select during the implementation experience. It varies from around five minutes to 40 minutes, depending on the options selected.

ALZ Multi-Tenant Updates

New CAF docs on the way 😍



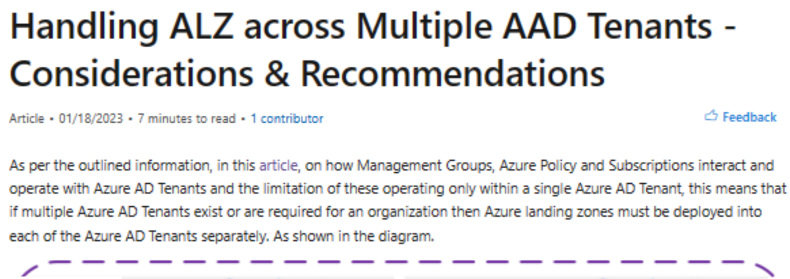
Multiple Azure AD Tenants in ALZ - Scenarios

Article • 01/18/2023 • 6 minutes to read • 1 contributor

Feedback

There are many reasons that an organization might end up with multiple Azure AD Tenants or investigate whether they need multiple Azure AD Tenants. The most common scenarios we see are listed:

- Mergers and Acquisitions
- Regulatory or Country Compliance Requirements
- Business Unit or Organizational Isolation and Autonomy Requirements
- Independent Software Vendor (ISV) Delivering SaaS Applications from Azure
- Tenant Level Testing / Microsoft 365 Testing

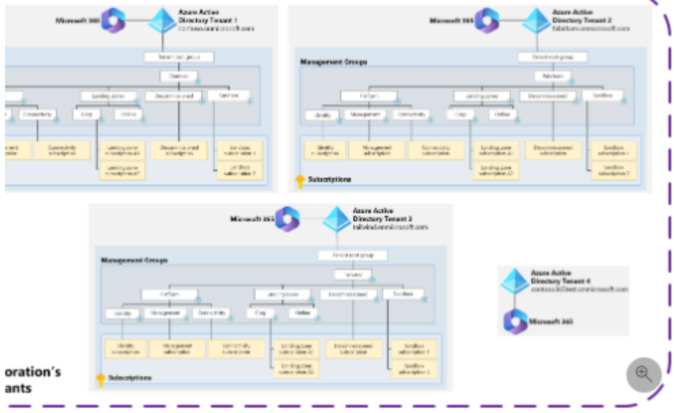


Handling ALZ across Multiple AAD Tenants - Considerations & Recommendations

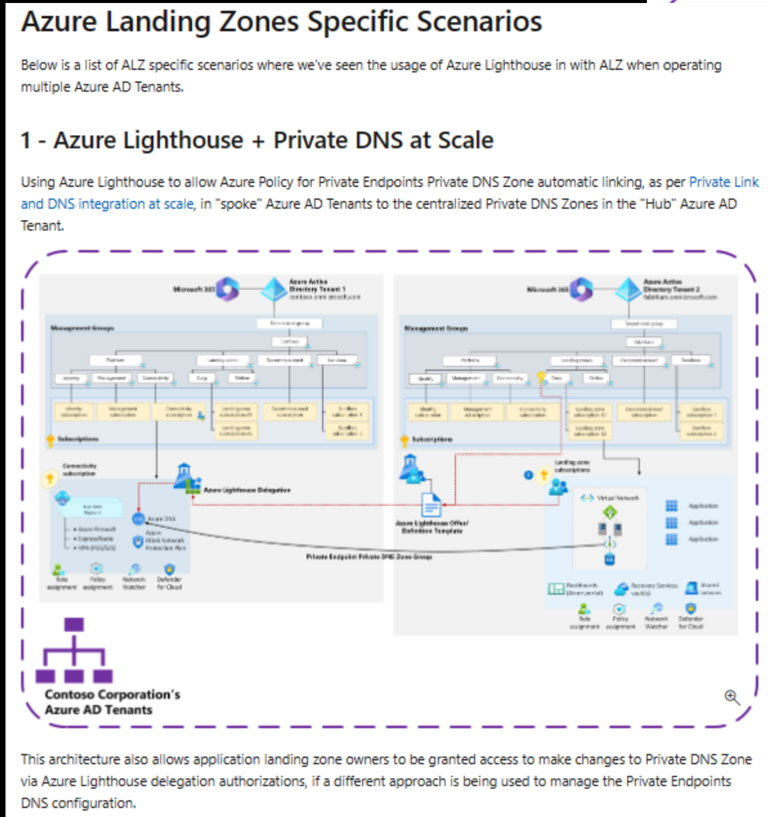
Article • 01/18/2023 • 7 minutes to read • 1 contributor

Feedback

As per the outlined information, in this article, on how Management Groups, Azure Policy and Subscriptions interact and operate with Azure AD Tenants and the limitation of these operating only within a single Azure AD Tenant, this means that if multiple Azure AD Tenants exist or are required for an organization then Azure landing zones must be deployed into each of the Azure AD Tenants separately. As shown in the diagram.



Microsoft 365
Azure Active Directory Tenant 1
Azure Active Directory Tenant 2
Azure Active Directory Tenant 3
Azure Active Directory Tenant 4
Management Groups
Tenant root group
Subscriptions
oration's
ants



Azure Landing Zones Specific Scenarios

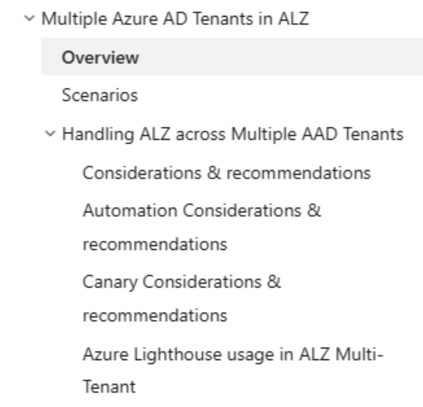
Below is a list of ALZ specific scenarios where we've seen the usage of Azure Lighthouse in with ALZ when operating multiple Azure AD Tenants.

1 - Azure Lighthouse + Private DNS at Scale

Using Azure Lighthouse to allow Azure Policy for Private Endpoints Private DNS Zone automatic linking, as per Private Link and DNS integration at scale, in "spoke" Azure AD Tenants to the centralized Private DNS Zones in the "Hub" Azure AD Tenant.

Microsoft 365
Azure Active Directory Tenant 1
Azure Active Directory Tenant 2
Management Groups
Subscriptions
Azure Lighthouse Delegation
Azure Lighthouse Offer/ Definition Template
Private Endpoint Private DNS Zone Group
Contoso Corporation's Azure AD Tenants

This architecture also allows application landing zone owners to be granted access to make changes to Private DNS Zone via Azure Lighthouse delegation authorizations, if a different approach is being used to manage the Private Endpoints DNS configuration.



Multiple Azure AD Tenants in ALZ
Overview
Scenarios
Handling ALZ across Multiple AAD Tenants
Considerations & recommendations
Automation Considerations & recommendations
Canary Considerations & recommendations
Azure Lighthouse usage in ALZ Multi-Tenant

m shows an example of
e corporation has grown

mergers and

*.onmicrosoft.com

Usag

ft.com

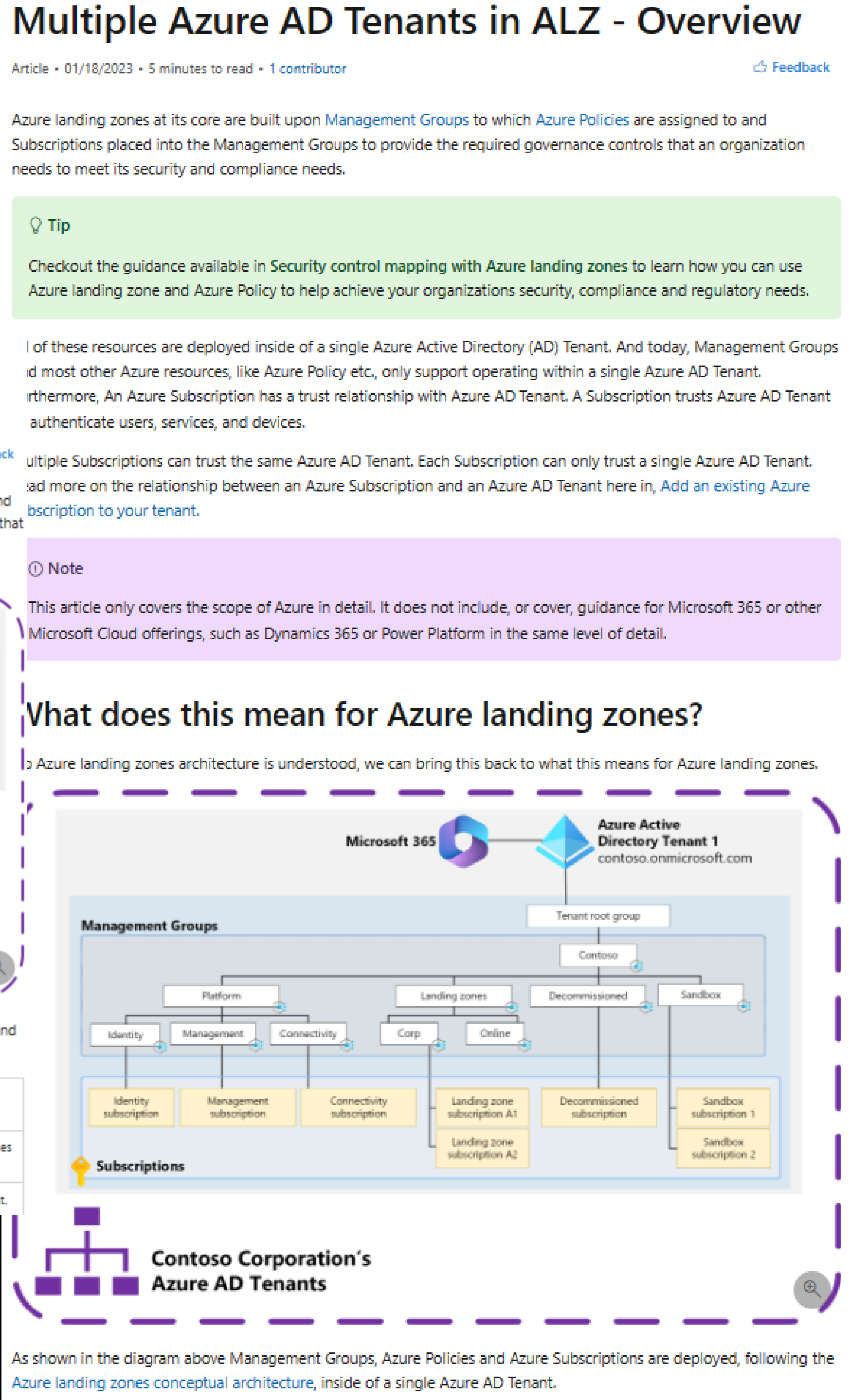
Prim
are u

ft 365 services

oft.com

Prim

n this Tenant.



Multiple Azure AD Tenants in ALZ - Overview

Article • 01/18/2023 • 5 minutes to read • 1 contributor

Feedback

Azure landing zones at its core are built upon Management Groups to which Azure Policies are assigned to and Subscriptions placed into the Management Groups to provide the required governance controls that an organization needs to meet its security and compliance needs.

Tip

Checkout the guidance available in Security control mapping with Azure landing zones to learn how you can use Azure landing zone and Azure Policy to help achieve your organizations security, compliance and regulatory needs.

l of these resources are deployed inside of a single Azure Active Directory (AD) Tenant. And today, Management Groups ıd most other Azure resources, like Azure Policy etc., only support operating within a single Azure AD Tenant. ırthermore, An Azure Subscription has a trust relationship with Azure AD Tenant. A Subscription trusts Azure AD Tenant authenticate users, services, and devices.

ultiple Subscriptions can trust the same Azure AD Tenant. Each Subscription can only trust a single Azure AD Tenant. ead more on the relationship between an Azure Subscription and an Azure AD Tenant here in, Add an existing Azure ıbscription to your tenant.

Note

This article only covers the scope of Azure in detail. It does not include, or cover, guidance for Microsoft 365 or other Microsoft Cloud offerings, such as Dynamics 365 or Power Platform in the same level of detail.

Vhat does this mean for Azure landing zones?

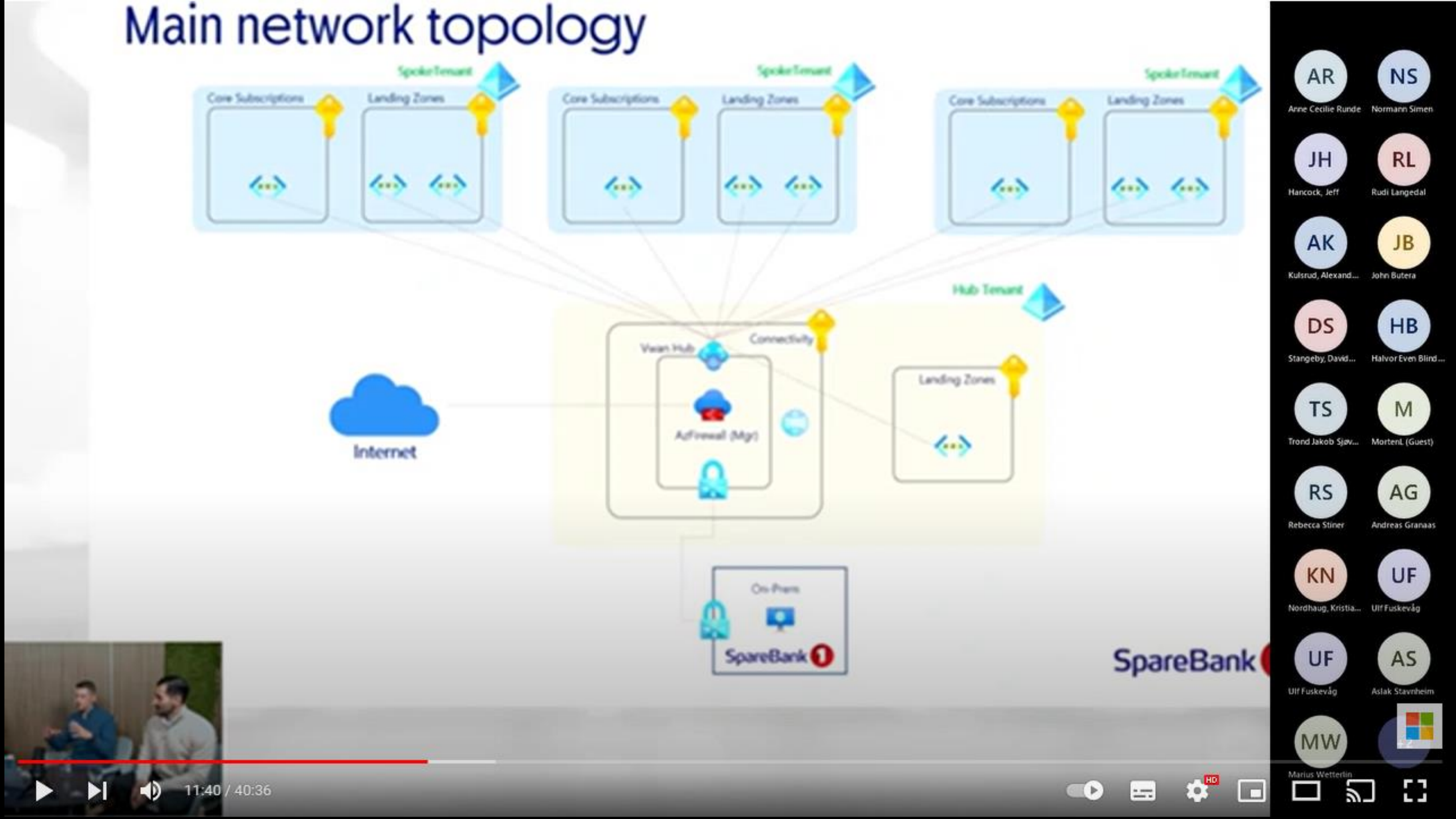
ɔ Azure landing zones architecture is understood, we can bring this back to what this means for Azure landing zones.

As shown in the diagram above Management Groups, Azure Policies and Azure Subscriptions are deployed, following the Azure landing zones conceptual architecture, inside of a single Azure AD Tenant.

Ignite 2022 Session

Spotlight on Norway | CLC08

Worth a watch 👀



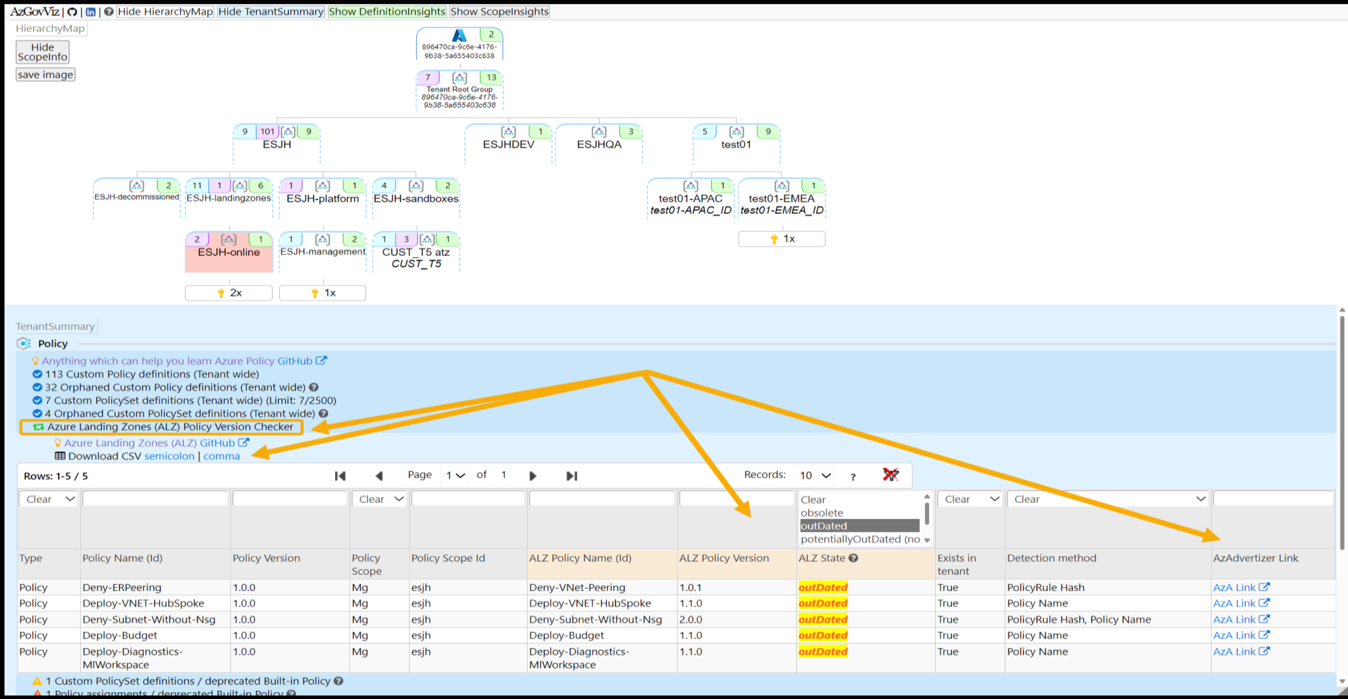
Updating ALZ (aka Evergreen) Updates

Updating ALZ ‘Evergreen’ Problem Statement

- Maintaining ALZ has various levels of complexity
- Customers have to manually subscribe to the ESLZ repo to follow changes (can be bombarded with notifications)
- We have a ‘What’s New’ section (https://aka.ms/alz/whatsnew) we keep up to date – this is manual customer effort to review
- Cost of change is greater than cost of staying the same
    - Customers aren’t aware of why they need to update e.g. bug fixes, security enhancements etc

Our investment

- Policy tooling
- Policy guidance
  - Moving from custom to built-in
  - Updating ALZ custom policies
- IaC guidance
- Backward compatibility
- Policy consolidation



Policy

- Anything which can help you learn Azure Policy GitHub
- 113 Custom Policy definitions (Tenant wide)
- 32 Orphaned Custom Policy definitions (Tenant wide)
- 7 Custom PolicySet definitions (Tenant wide) (Limit: 7/2500)
- 4 Orphaned Custom PolicySet definitions (Tenant wide)
- Azure Landing Zones (ALZ) Policy Version Checker
  - Azure Landing Zones (ALZ) GitHub
  - Download CSV semicolon | comma

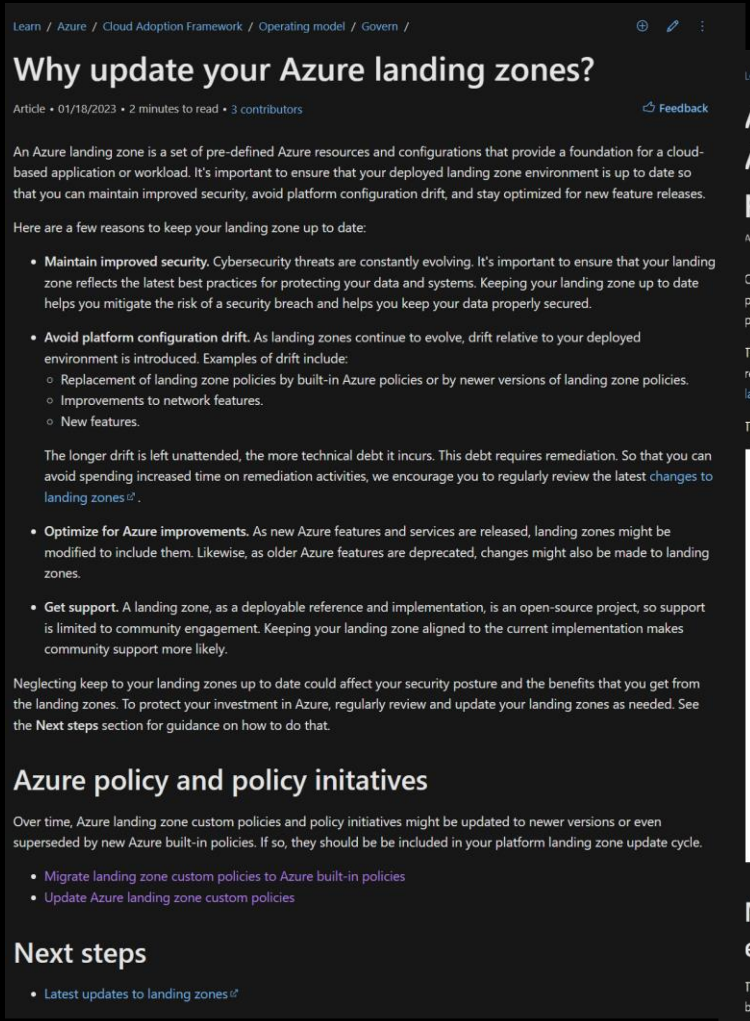
Rows: 1-5 / 5 Page 1 of 1 Records: 10 ?

Type	Policy Name (Id)	Policy Version	Policy Scope	Policy Scope Id	ALZ Policy Name (Id)	ALZ Policy Version	ALZ State	Exists in tenant	Detection method	AzAdvertizer Link
Clear			Clear				Clear obsolete outDated potentiallyOutDated (no	Clear	Clear	
Policy	Deny-ERPeering	1.0.0	Mg	esjh	Deny-VNet-Peering	1.0.1	outDated	True	PolicyRule Hash	AzA Link
Policy	Deploy-VNET-HubSpoke	1.0.0	Mg	esjh	Deploy-VNET-HubSpoke	1.1.0	outDated	True	Policy Name	AzA Link
Policy	Deny-Subnet-Without-Nsg	1.0.0	Mg	esjh	Deny-Subnet-Without-Nsg	2.0.0	outDated	True	PolicyRule Hash, Policy Name	AzA Link
Policy	Deploy-Budget	1.0.0	Mg	esjh	Deploy-Budget	1.1.0	outDated	True	Policy Name	AzA Link
Policy	Deploy-Diagnostics-MlWorkspace	1.0.0	Mg	esjh	Deploy-Diagnostics-MlWorkspace	1.1.0	outDated	True	Policy Name	AzA Link

- 1 Custom PolicySet definitions / deprecated Built-in Policy
- 1 Policy assignments / deprecated Built-in Policy

aka.ms/AzGovViz

New Guidance Released



Learn / Azure / Cloud Adoption Framework / Operating model / Govern /

Why update your Azure landing zones?

Article • 01/18/2023 • 2 minutes to read • 3 contributors

Feedback

An Azure landing zone is a set of pre-defined Azure resources and configurations that provide a foundation for a cloud-based application or workload. It's important to ensure that your deployed landing zone environment is up to date so that you can maintain improved security, avoid platform configuration drift, and stay optimized for new feature releases.

Here are a few reasons to keep your landing zone up to date:

- **Maintain improved security.** Cybersecurity threats are constantly evolving. It's important to ensure that your landing zone reflects the latest best practices for protecting your data and systems. Keeping your landing zone up to date helps you mitigate the risk of a security breach and helps you keep your data properly secured.
- **Avoid platform configuration drift.** As landing zones continue to evolve, drift relative to your deployed environment is introduced. Examples of drift include:
  - Replacement of landing zone policies by built-in Azure policies or by newer versions of landing zone policies.
  - Improvements to network features.
  - New features.

  The longer drift is left unattended, the more technical debt it incurs. This debt requires remediation. So that you can avoid spending increased time on remediation activities, we encourage you to regularly review the latest changes to landing zones.
- **Optimize for Azure improvements.** As new Azure features and services are released, landing zones might be modified to include them. Likewise, as older Azure features are deprecated, changes might also be made to landing zones.
- **Get support.** A landing zone, as a deployable reference and implementation, is an open-source project, so support is limited to community engagement. Keeping your landing zone aligned to the current implementation makes community support more likely.

Neglecting keep to your landing zones up to date could affect your security posture and the benefits that you get from the landing zones. To protect your investment in Azure, regularly review and update your landing zones as needed. See the **Next steps** section for guidance on how to do that.

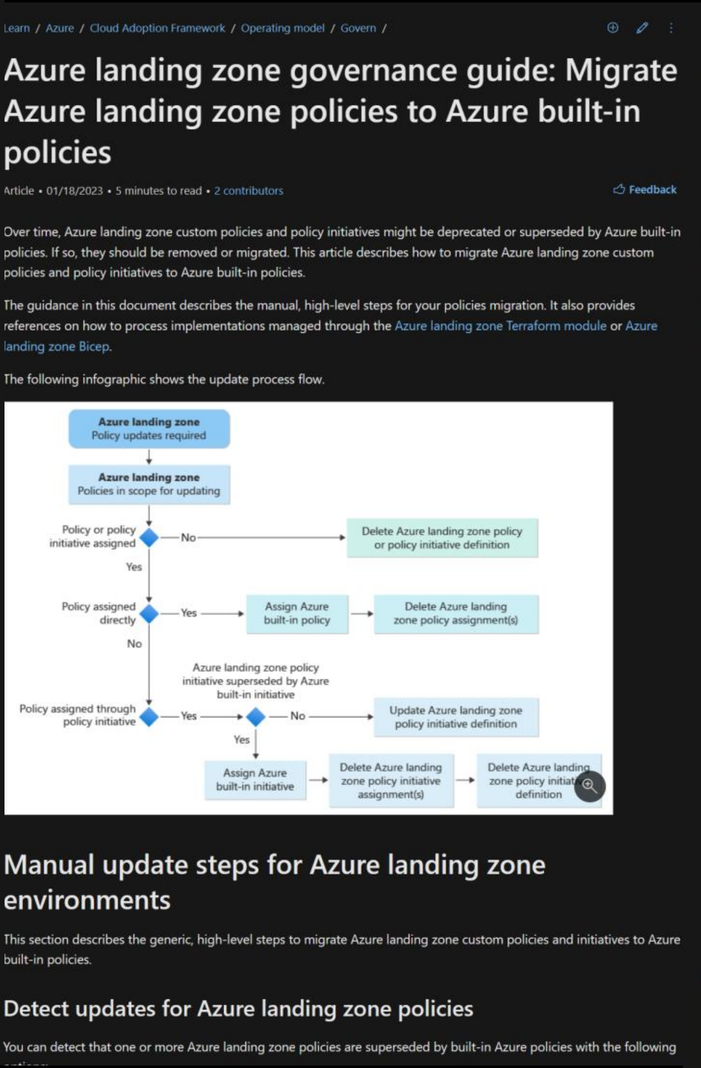
Azure policy and policy initatives

Over time, Azure landing zone custom policies and policy initiatives might be updated to newer versions or even superseded by new Azure built-in policies. If so, they should be be included in your platform landing zone update cycle.

- Migrate landing zone custom policies to Azure built-in policies
- Update Azure landing zone custom policies

Next steps

- Latest updates to landing zones



Learn / Azure / Cloud Adoption Framework / Operating model / Govern /

Azure landing zone governance guide: Migrate Azure landing zone policies to Azure built-in policies

Article • 01/18/2023 • 5 minutes to read • 2 contributors

Feedback

Over time, Azure landing zone custom policies and policy initiatives might be deprecated or superseded by Azure built-in policies. If so, they should be removed or migrated. This article describes how to migrate Azure landing zone custom policies and policy initiatives to Azure built-in policies.

The guidance in this document describes the manual, high-level steps for your policies migration. It also provides references on how to process implementations managed through the Azure landing zone Terraform module or Azure landing zone Bicep.

The following infographic shows the update process flow.

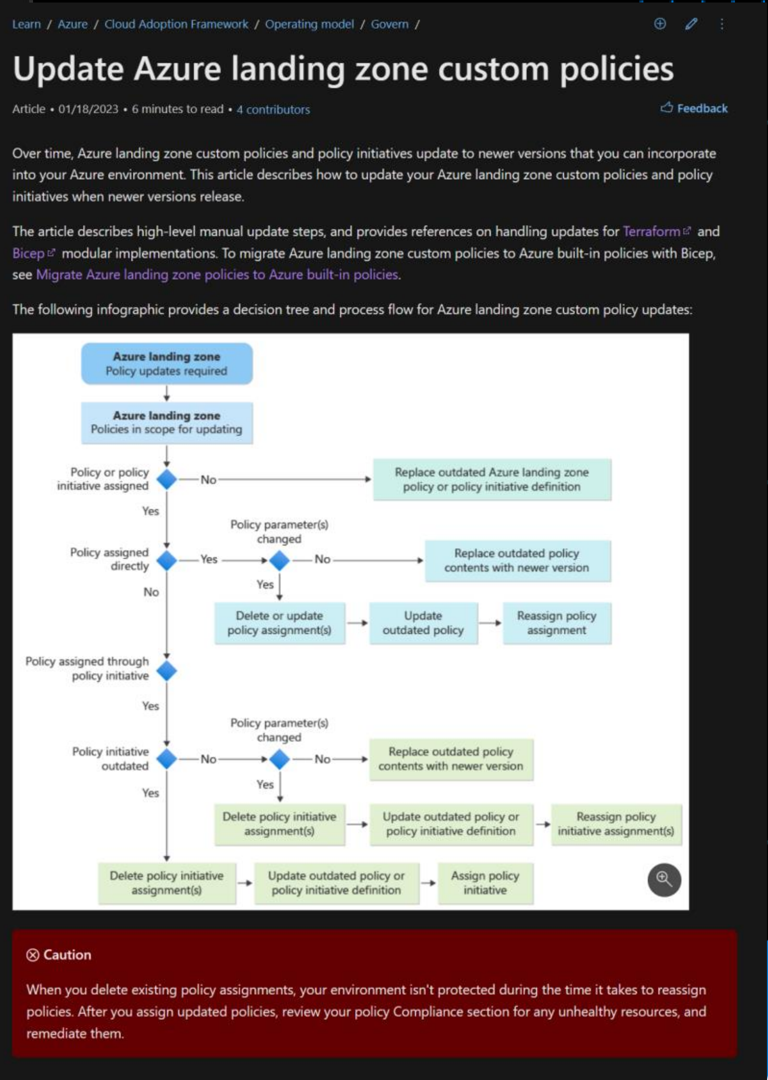
Azure landing zone
Policy updates required
Azure landing zone
Policies in scope for updating
Policy or policy initiative assigned
No
Delete Azure landing zone policy or policy initiative definition
Yes
Policy assigned directly
Yes
Assign Azure built-in policy
Delete Azure landing zone policy assignment(s)
No
Azure landing zone policy initiative superseded by Azure built-in initiative
Policy assigned through policy initiative
Yes
No
Update Azure landing zone policy initiative definition
Yes
Assign Azure built-in initiative
Delete Azure landing zone policy initiative assignment(s)
Delete Azure landing zone policy initiat definition

Manual update steps for Azure landing zone environments

This section describes the generic, high-level steps to migrate Azure landing zone custom policies and initiatives to Azure built-in policies.

Detect updates for Azure landing zone policies

You can detect that one or more Azure landing zone policies are superseded by built-in Azure policies with the following



Learn / Azure / Cloud Adoption Framework / Operating model / Govern /

Update Azure landing zone custom policies

Article • 01/18/2023 • 6 minutes to read • 4 contributors

Feedback

Over time, Azure landing zone custom policies and policy initiatives update to newer versions that you can incorporate into your Azure environment. This article describes how to update your Azure landing zone custom policies and policy initiatives when newer versions release.

The article describes high-level manual update steps, and provides references on handling updates for Terraform and Bicep modular implementations. To migrate Azure landing zone custom policies to Azure built-in policies with Bicep, see Migrate Azure landing zone policies to Azure built-in policies.

The following infographic provides a decision tree and process flow for Azure landing zone custom policy updates:

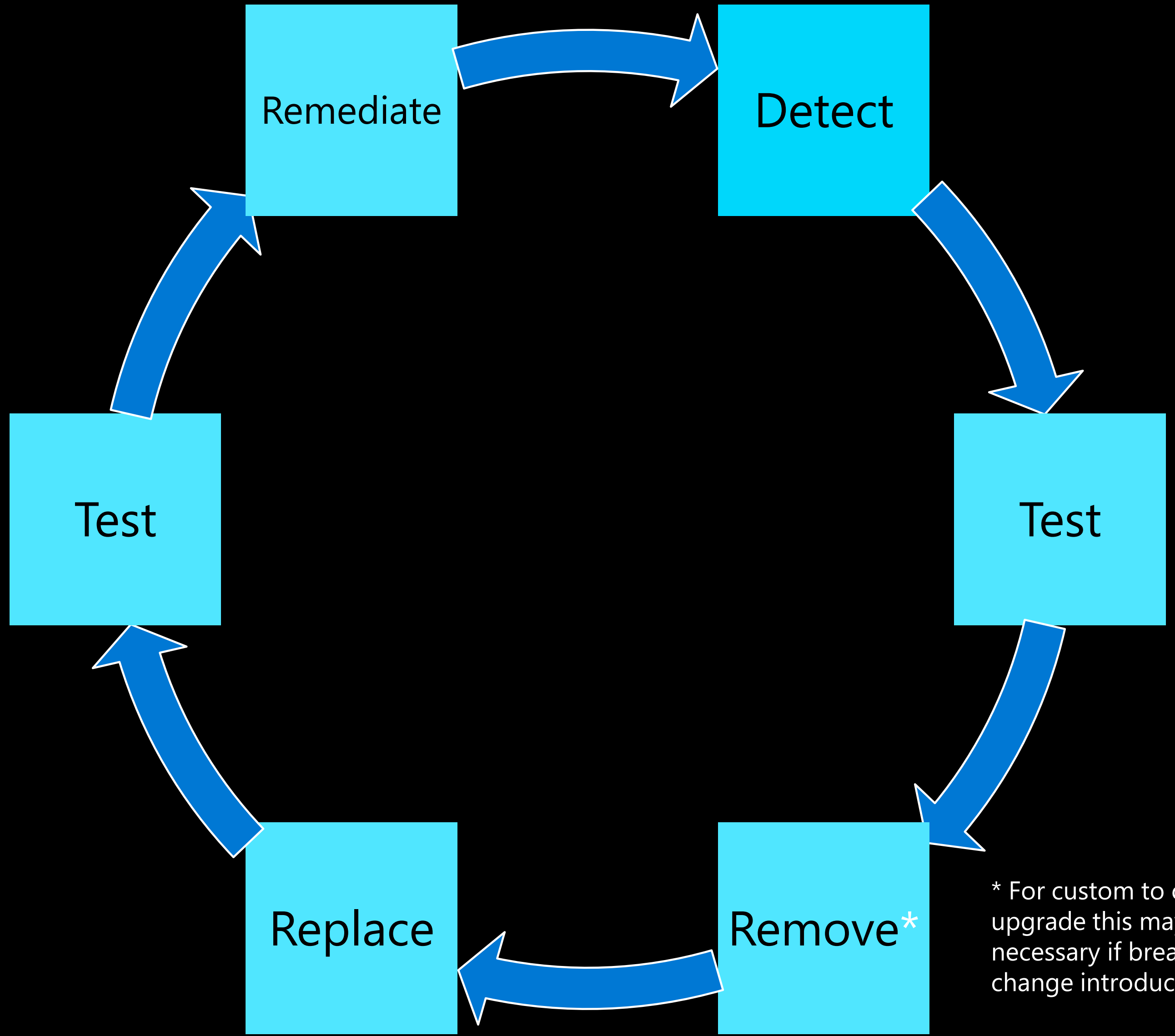
Azure landing zone
Policy updates required
Azure landing zone
Policies in scope for updating
Policy or policy initiative assigned
No
Replace outdated Azure landing zone policy or policy initiative definition
Yes
Policy parameter(s) changed
Policy assigned directly
Yes
No
Replace outdated policy contents with newer version
Yes
No
Delete or update policy assignment(s)
Update outdated policy
Reassign policy assignment
Policy assigned through policy initiative
Yes
Policy parameter(s) changed
Policy initiative outdated
No
No
Replace outdated policy contents with newer version
Yes
Yes
Delete policy initiative assignment(s)
Update outdated policy or policy initiative definition
Reassign policy initiative assignment(s)
Delete policy initiative assignment(s)
Update outdated policy or policy initiative definition
Assign policy initiative

ⓧ Caution

When you delete existing policy assignments, your environment isn't protected during the time it takes to reassign policies. After you assign updated policies, review your policy Compliance section for any unhealthy resources, and remediate them.

aka.ms/alz/update

ALZ Custom Policy and Initiatives Lifecycle



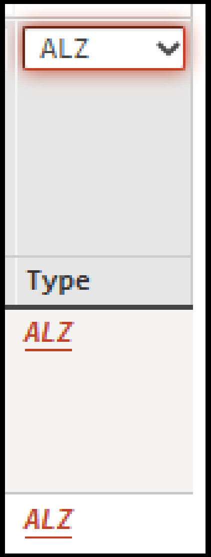
* For custom to custom upgrade this may be necessary if breaking change introduced

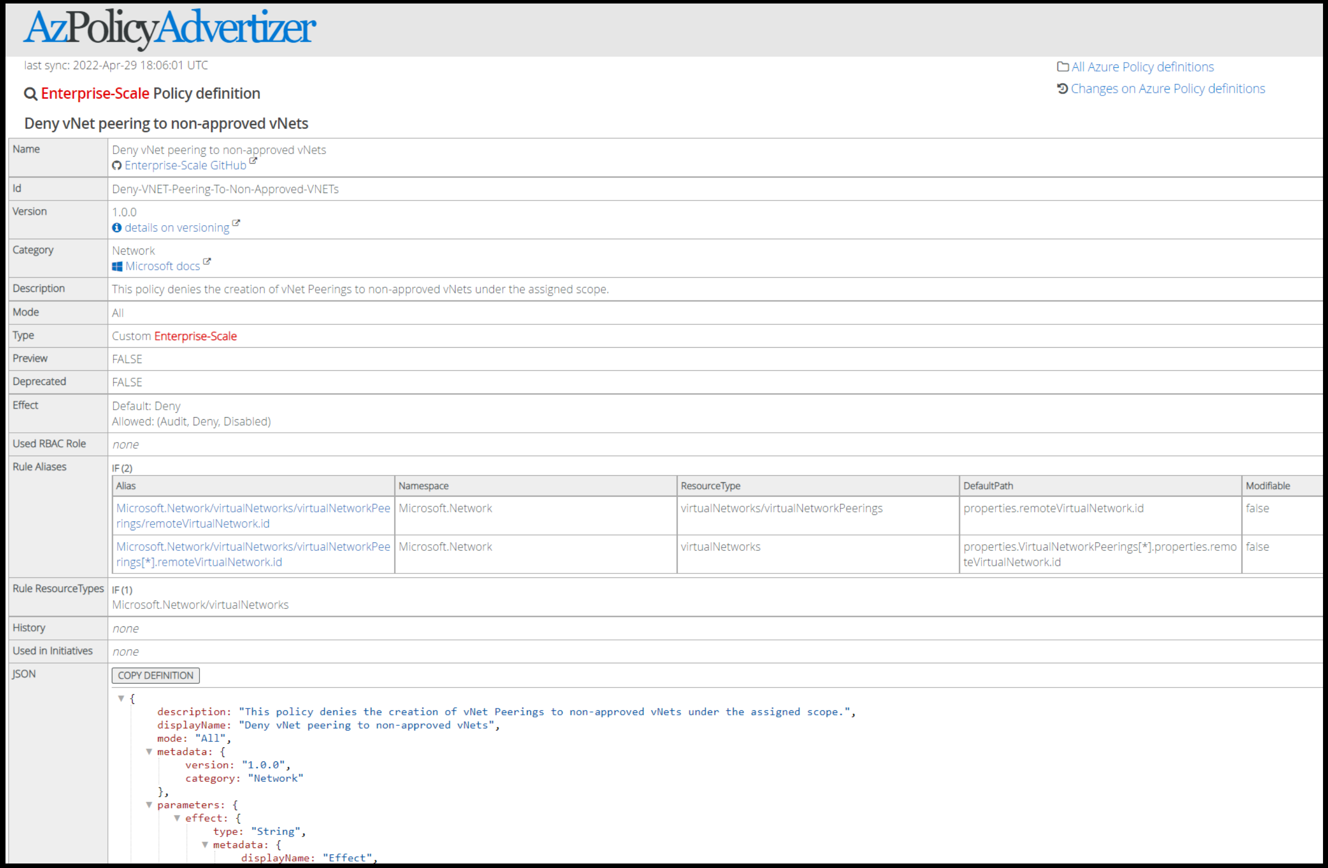
NOTE: Make sure all policies have been tested before applying – see ALZ testing guidance

AzGovViz & AzAdvertizer Updates

ALZ Policy – AzAdvertizer Integration

- Started integration with AzAdvertizer
- Covering ALZ Policy Definitions & Initiatives
- Use type column filtering to 'ALZ'




AzPolicyAdvertizer
All Azure Policy definitions
Changes on Azure Policy definitions

last sync: 2022-Apr-29 18:06:01 UTC

Enterprise-Scale Policy definition

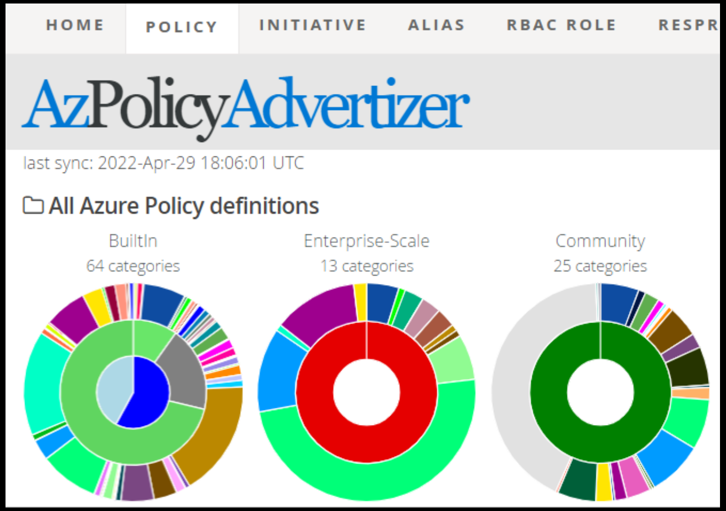
Deny vNet peering to non-approved vNets

Name	Deny vNet peering to non-approved vNets Enterprise-Scale GitHub
Id	Deny-VNET-Peering-To-Non-Approved-VNETs
Version	1.0.0 details on versioning
Category	Network Microsoft docs
Description	This policy denies the creation of vNet Peerings to non-approved vNets under the assigned scope.
Mode	All
Type	Custom Enterprise-Scale
Preview	FALSE
Deprecated	FALSE
Effect	Default: Deny Allowed: (Audit, Deny, Disabled)
Used RBAC Role	*none*
Rule Aliases	IF (2)

Alias	Namespace	ResourceType	DefaultPath	Modifiable
Microsoft.Network/virtualNetworks/virtualNetworkPeerings/remoteVirtualNetwork.id	Microsoft.Network	virtualNetworks/virtualNetworkPeerings	properties.remoteVirtualNetwork.id	false
Microsoft.Network/virtualNetworks/virtualNetworkPeerings[*].remoteVirtualNetwork.id	Microsoft.Network	virtualNetworks	properties.VirtualNetworkPeerings[*].properties.remoteVirtualNetwork.id	false

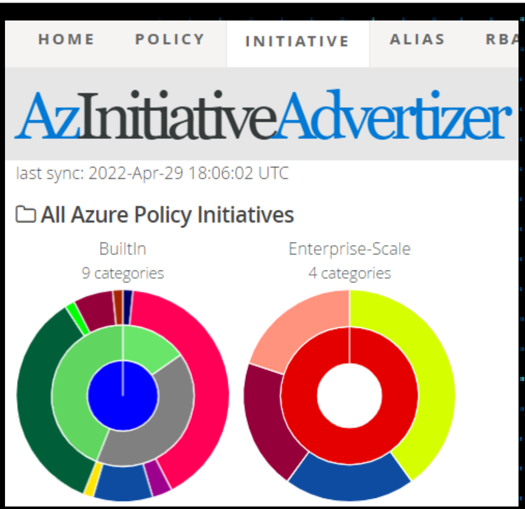
Rule ResourceTypes	IF (1) Microsoft.Network/virtualNetworks
History	*none*
Used in Initiatives	*none*
JSON	COPY DEFINITION

```
▼ {
      description: "This policy denies the creation of vNet Peerings to non-approved vNets under the assigned scope.",
      displayName: "Deny vNet peering to non-approved vNets",
      mode: "All",
    ▼ metadata: {
          version: "1.0.0",
          category: "Network"
      },
    ▼ parameters: {
        ▼ effect: {
              type: "String",
            ▼ metadata: {
                  displayName: "Effect",
```



last sync: 2022-Apr-29 18:06:01 UTC

All Azure Policy definitions



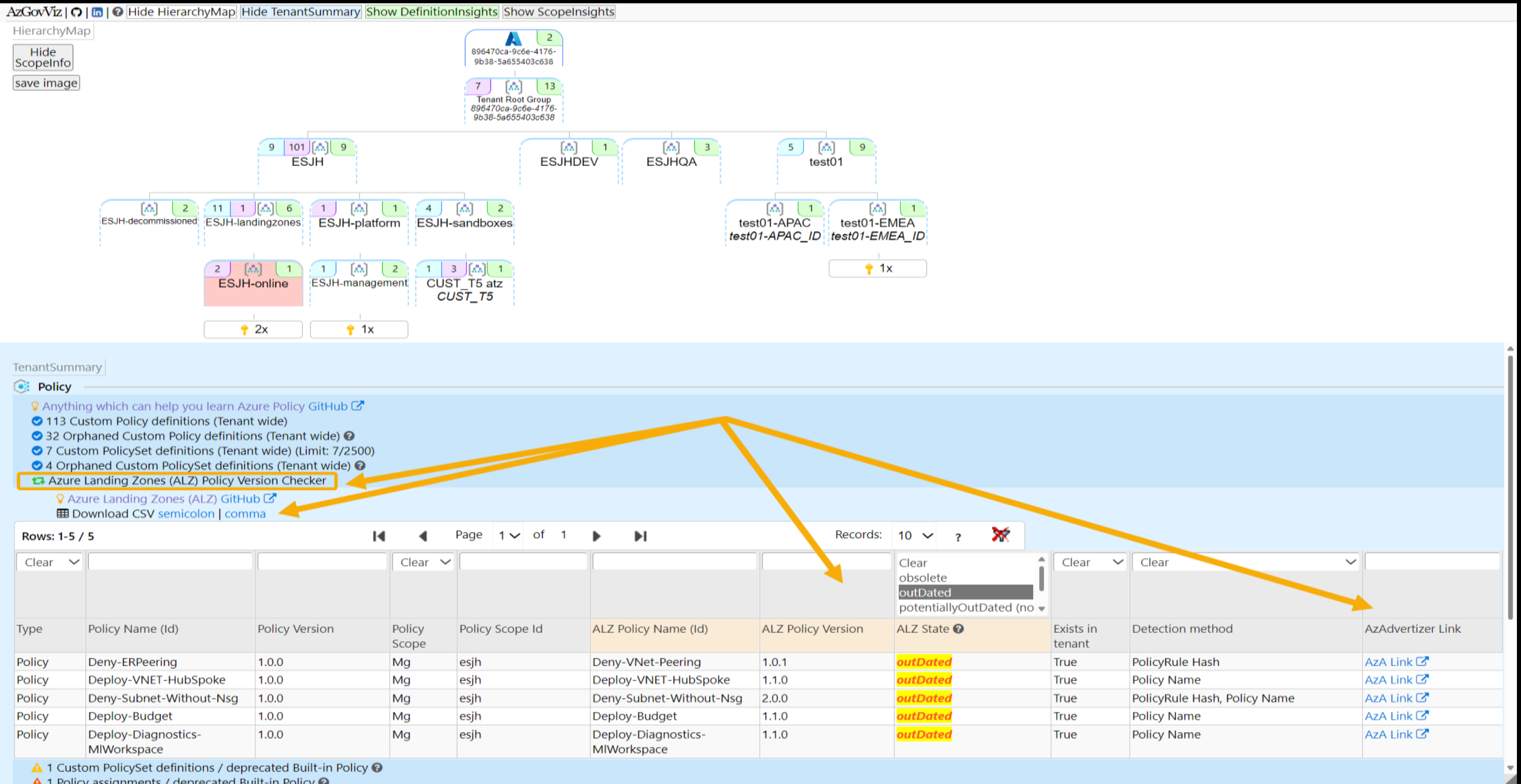
last sync: 2022-Apr-29 18:06:02 UTC

All Azure Policy Initiatives

aka.ms/AzAdvertizer

ALZ Policy – AzGovViz ‘Evergreen’ Feature

- Helping customers understand how “out of date” their ALZ custom policies are from when they initially deployed them
- Matching on several different pieces of logic
- Enabled by default in latest version of Azure Governance Visualizer (can be disabled by setting parameter ‘-NoALZPolicyVersionChecker’)



Anything which can help you learn Azure Policy GitHub
113 Custom Policy definitions (Tenant wide)
32 Orphaned Custom Policy definitions (Tenant wide)
7 Custom PolicySet definitions (Tenant wide) (Limit: 7/2500)
4 Orphaned Custom PolicySet definitions (Tenant wide)
Azure Landing Zones (ALZ) Policy Version Checker
Azure Landing Zones (ALZ) GitHub
Download CSV semicolon | comma

Rows: 1-5 / 5 Page 1 of 1 Records: 10 ?

Type	Policy Name (Id)	Policy Version	Policy Scope	Policy Scope Id	ALZ Policy Name (Id)	ALZ Policy Version	ALZ State	Exists in tenant	Detection method	AzAdvertizer Link
Clear			Clear				Clear obsolete outDated potentiallyOutDated (no	Clear	Clear	
Policy	Deny-ERPeering	1.0.0	Mg	esjh	Deny-VNet-Peering	1.0.1	outDated	True	PolicyRule Hash	AzA Link
Policy	Deploy-VNET-HubSpoke	1.0.0	Mg	esjh	Deploy-VNET-HubSpoke	1.1.0	outDated	True	Policy Name	AzA Link
Policy	Deny-Subnet-Without-Nsg	1.0.0	Mg	esjh	Deny-Subnet-Without-Nsg	2.0.0	outDated	True	PolicyRule Hash, Policy Name	AzA Link
Policy	Deploy-Budget	1.0.0	Mg	esjh	Deploy-Budget	1.1.0	outDated	True	Policy Name	AzA Link
Policy	Deploy-Diagnostics-MlWorkspace	1.0.0	Mg	esjh	Deploy-Diagnostics-MlWorkspace	1.1.0	outDated	True	Policy Name	AzA Link

⚠ 1 Custom PolicySet definitions / deprecated Built-in Policy
⚠ 1 Policy assignments / deprecated Built-in Policy

aka.ms/AzGovViz

Azure Governance Visualizer aka AzGovViz
&
AzAdvertizer

Updates - Demo

AzGovViz Demo

Subscription Vending Updates

Subscription Vending Modules

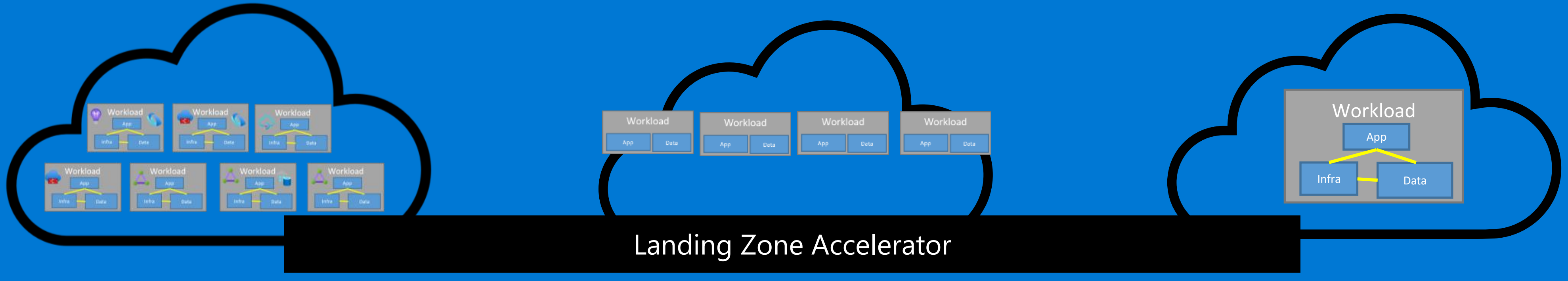
Available Now!
aka.ms/lz-vending/bicep

Available Now!
aka.ms/lz-vending/tf

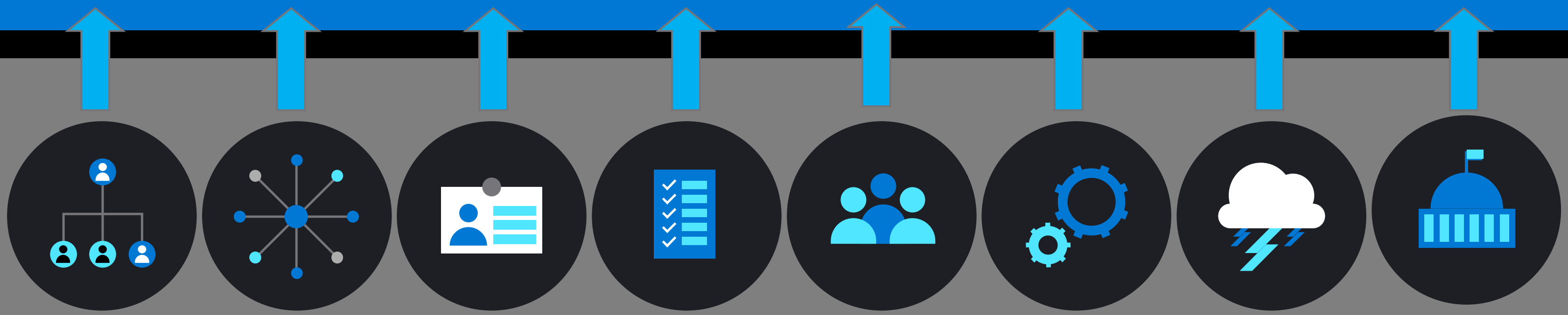
- Infrastructure as code modules to automate:
  - Subscription creation
  - Management Group placement
  - Virtual Networking
    - Virtual WAN Hub Connection
    - Virtual Network Peering
    - DDoS Plan Link
    - Custom DNS Servers
  - Role Assignments
  - Resource Locks
  - Tags

Azure landing zones

Each **landing zone** supports one or more applications in your cloud portfolio using the inherited controls



Centrally managed landing zone **Tech Platform landing zone** **Workload landing zone**



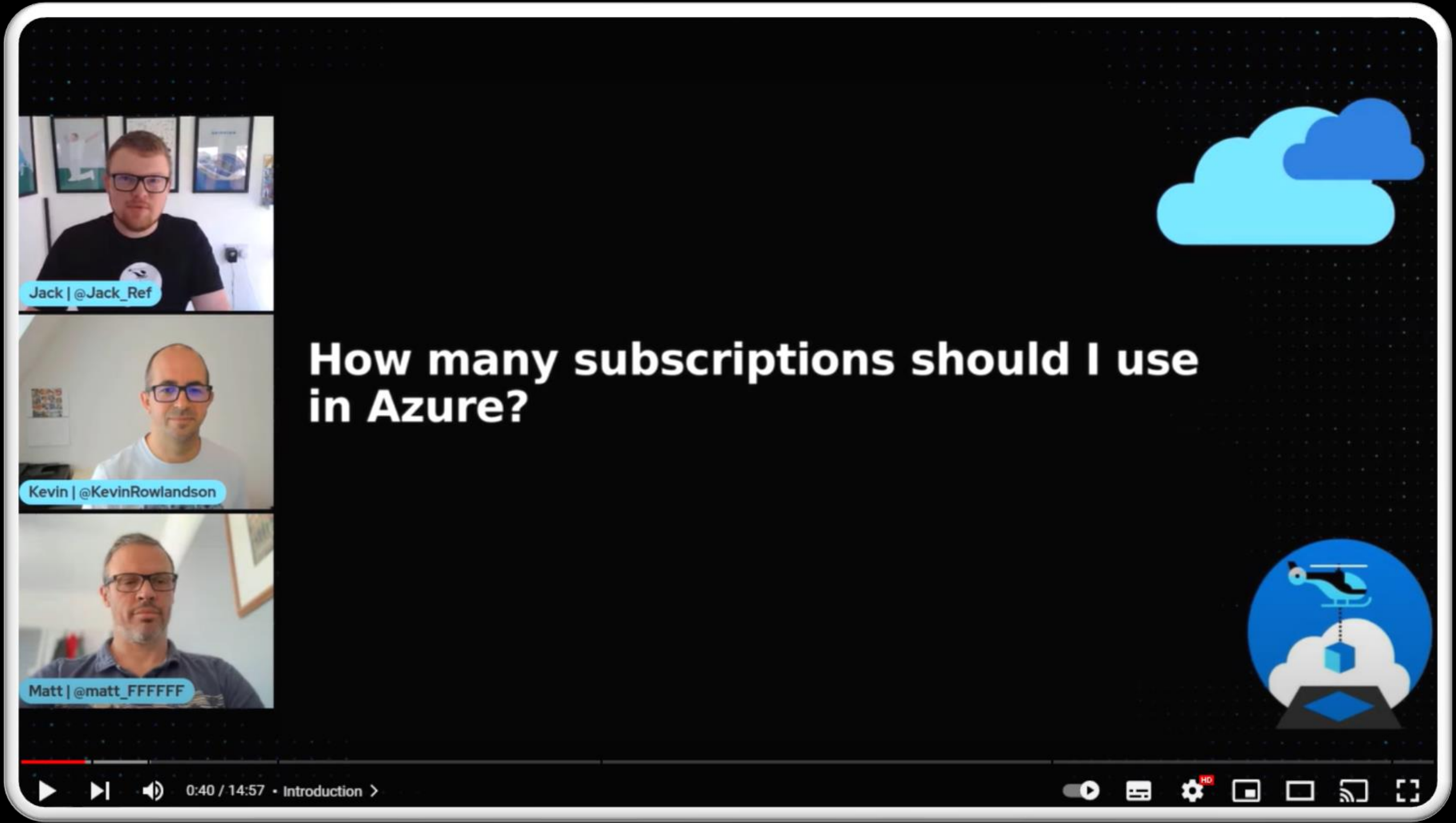
Azure landing zone implementations establish an enterprise control plane by defining environmental configuration & controls required for compliant operations management

Why?

- We have heard that we do a great job at helping accelerate:
  - Platform Landing Zones (aka Azure Landing Zones)
    - What is an Azure landing zone?
  - Workload/Application Accelerators (aka Cloud Adoption Scenarios)
    - Azure VMware Solution landing zone accelerator
    - Azure Virtual Desktop landing zone accelerator
    - More here…
- **But, there is a gap – how do we create the applicaiton landing zones?** (aka Subscriptions)
  - Types of Landing Zones – Platform vs Application

How many Subscriptions should I use in Azure?

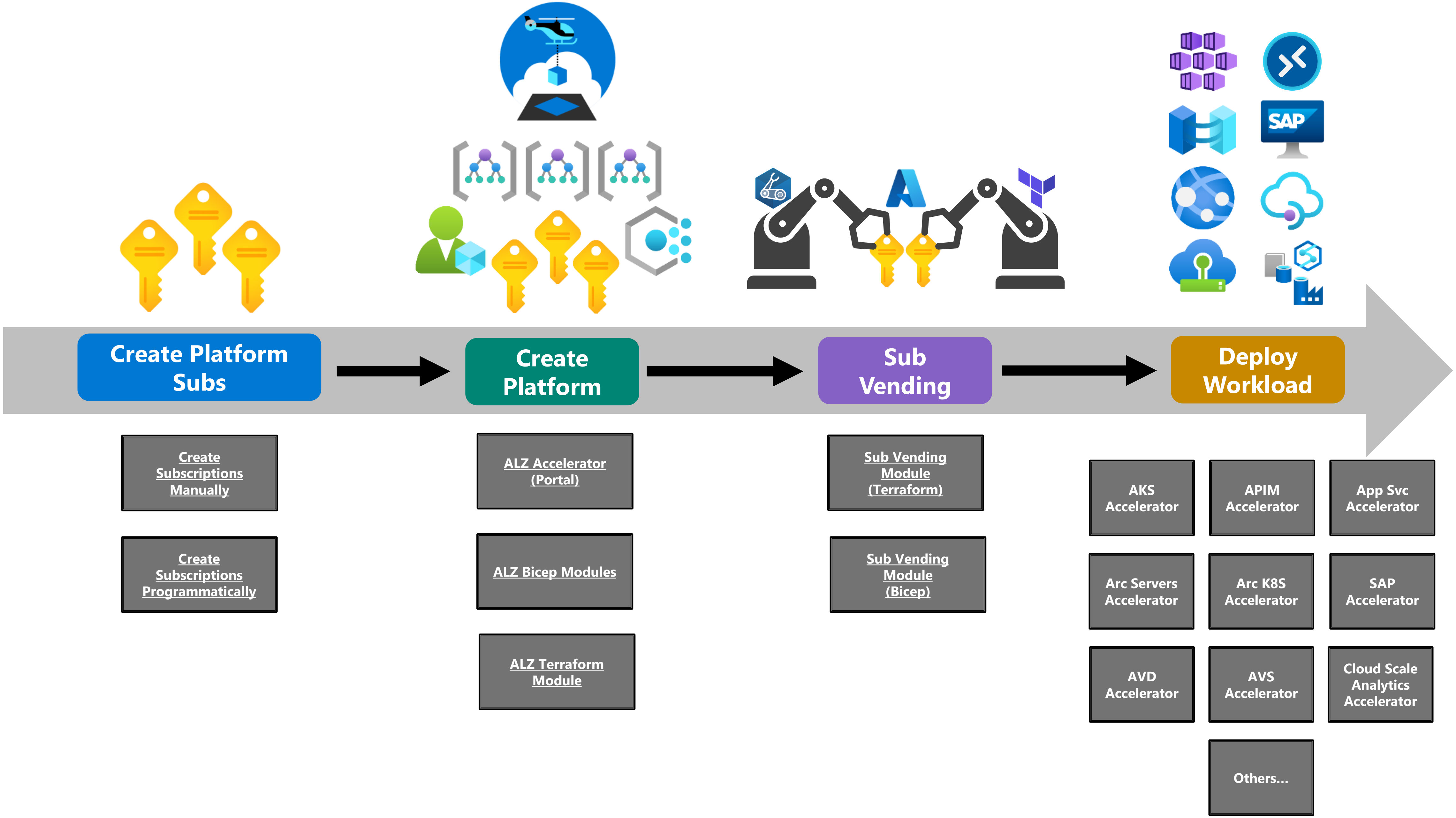
Subscription Democratization



How many subscriptions should I use in Azure?

More planned for aka.ms/CAEYouTube

Example ALZ Customer Journey



Create Platform Subs → **Create Platform** → **Sub Vending** → **Deploy Workload**

Create Platform Subs:

- Create Subscriptions Manually
- Create Subscriptions Programmatically

Create Platform:

- ALZ Accelerator (Portal)
- ALZ Bicep Modules
- ALZ Terraform Module

Sub Vending:

- Sub Vending Module (Terraform)
- Sub Vending Module (Bicep)

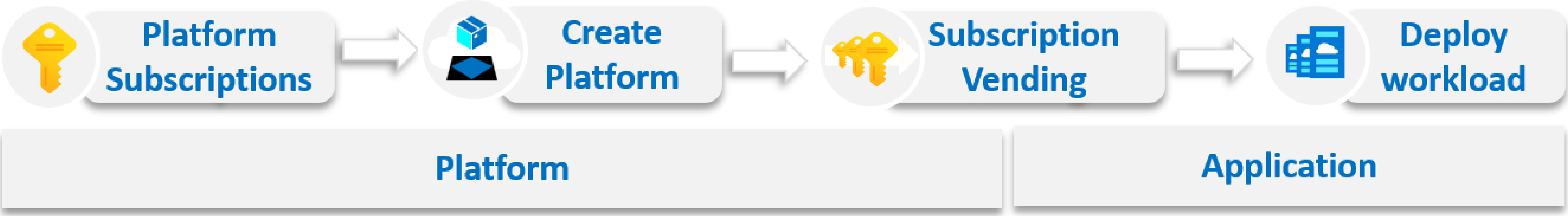
Deploy Workload:

- AKS Accelerator
- APIM Accelerator
- App Svc Accelerator
- Arc Servers Accelerator
- Arc K8S Accelerator
- SAP Accelerator
- AVD Accelerator
- AVS Accelerator
- Cloud Scale Analytics Accelerator
- Others...

aka.ms/lz-vending/bicep

aka.ms/lz-vending/tf

LZ Vending



Platform Subscriptions → Create Platform → Subscription Vending → Deploy workload

Platform

Application

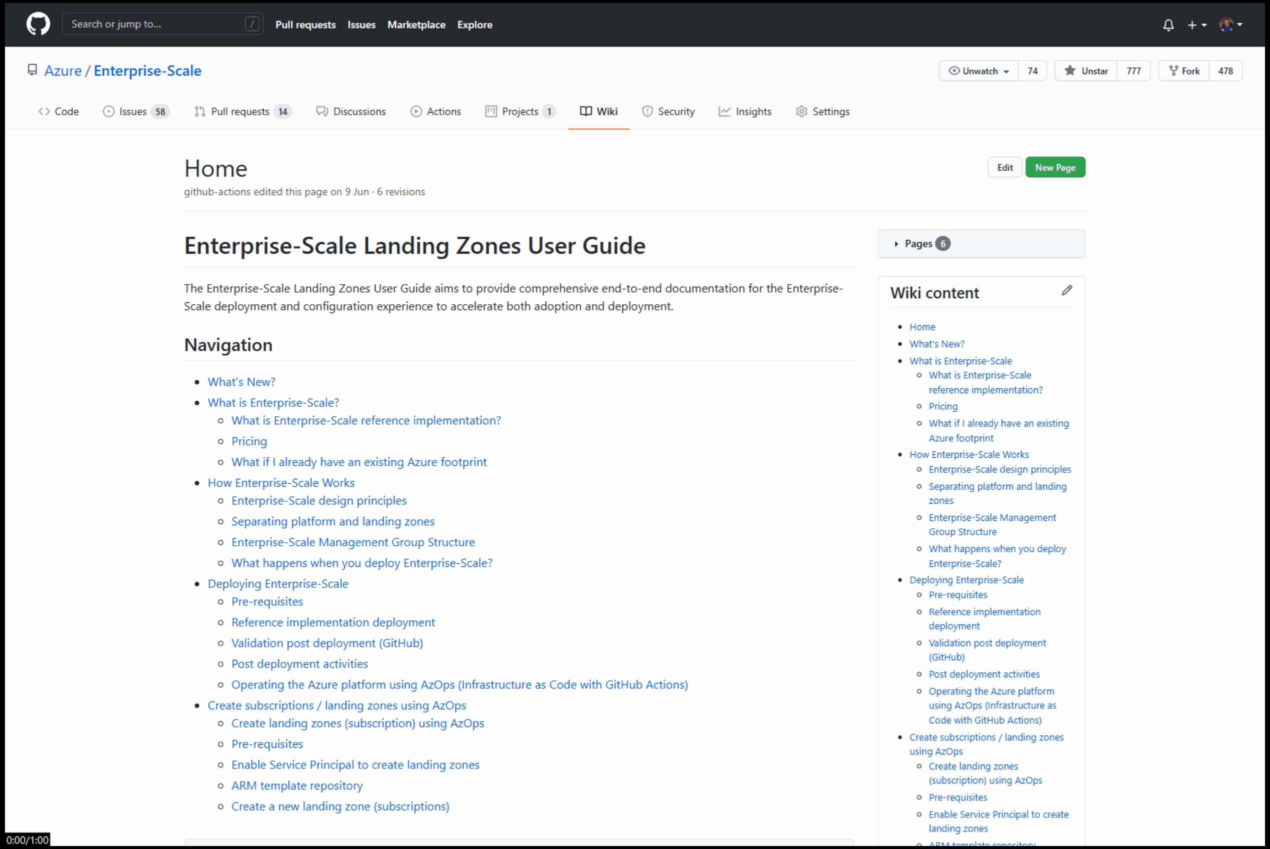
Contributing to ALZ Repo Updates

We Want You! https://aka.ms/ALZ/Repo

To contribute to ALZ

- Create issues, bugs and feature requests on any of our repos
- Tell us where we can improve existing guidance or provide new guidance

Update docs/wiki:



Home

github-actions edited this page on 9 Jun · 6 revisions

Enterprise-Scale Landing Zones User Guide

The Enterprise-Scale Landing Zones User Guide aims to provide comprehensive end-to-end documentation for the Enterprise-Scale deployment and configuration experience to accelerate both adoption and deployment.

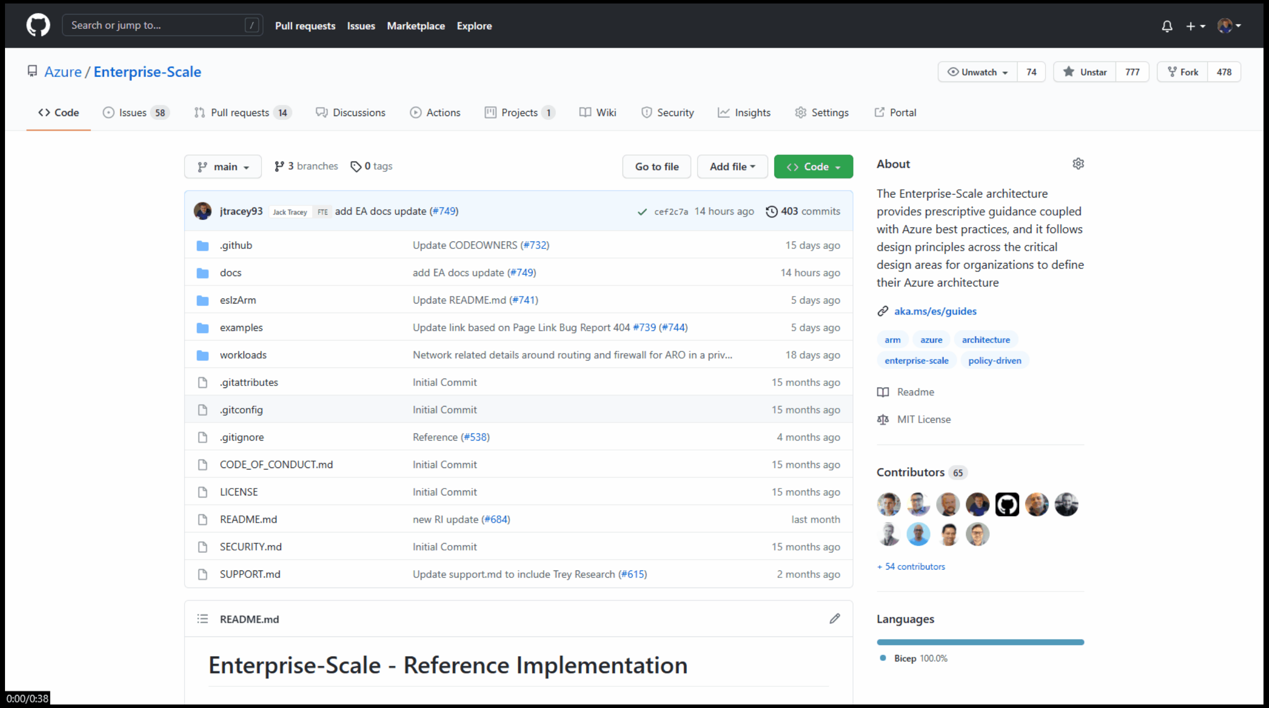
Navigation

- What's New?
- What is Enterprise-Scale?
  - What is Enterprise-Scale reference implementation?
  - Pricing
  - What if I already have an existing Azure footprint
- How Enterprise-Scale Works
  - Enterprise-Scale design principles
  - Separating platform and landing zones
  - Enterprise-Scale Management Group Structure
  - What happens when you deploy Enterprise-Scale?
- Deploying Enterprise-Scale
  - Pre-requisites
  - Reference implementation deployment
  - Validation post deployment (GitHub)
  - Post deployment activities
  - Operating the Azure platform using AzOps (Infrastructure as Code with GitHub Actions)
- Create subscriptions / landing zones using AzOps
  - Create landing zones (subscription) using AzOps
  - Pre-requisites
  - Enable Service Principal to create landing zones
  - ARM template repository
  - Create a new landing zone (subscriptions)

Wiki content

- Home
- What's New?
- What is Enterprise-Scale
  - What is Enterprise-Scale reference implementation?
  - Pricing
  - What if I already have an existing Azure footprint
- How Enterprise-Scale Works
  - Enterprise-Scale design principles
  - Separating platform and landing zones
  - Enterprise-Scale Management Group Structure
  - What happens when you deploy Enterprise-Scale?
- Deploying Enterprise-Scale
  - Pre-requisites
  - Reference implementation deployment
  - Validation post deployment (GitHub)
  - Post deployment activities
  - Operating the Azure platform using AzOps (Infrastructure as Code with GitHub Actions)
- Create subscriptions / landing zones using AzOps
  - Create landing zones (subscription) using AzOps
  - Pre-requisites
  - Enable Service Principal to create landing zones
  - ARM template repository

Create an issue/feature request:



jtracey93 Jack Tracey FTE add EA docs update (#749) ✓ cef2c7a 14 hours ago 403 commits

.github	Update CODEOWNERS (#732)	15 days ago
docs	add EA docs update (#749)	14 hours ago
eslzArm	Update README.md (#741)	5 days ago
examples	Update link based on Page Link Bug Report 404 #739 (#744)	5 days ago
workloads	Network related details around routing and firewall for ARO in a priv...	18 days ago
.gitattributes	Initial Commit	15 months ago
.gitconfig	Initial Commit	15 months ago
.gitignore	Reference (#538)	4 months ago
CODE_OF_CONDUCT.md	Initial Commit	15 months ago
LICENSE	Initial Commit	15 months ago
README.md	new RI update (#684)	last month
SECURITY.md	Initial Commit	15 months ago
SUPPORT.md	Update support.md to include Trey Research (#615)	2 months ago

README.md

Enterprise-Scale - Reference Implementation

About

The Enterprise-Scale architecture provides prescriptive guidance coupled with Azure best practices, and it follows design principles across the critical design areas for organizations to define their Azure architecture

aka.ms/es/guides

arm azure architecture enterprise-scale policy-driven

Readme

MIT License

Contributors 65

+ 54 contributors

Languages

Bicep 100.0%

Creating Issues, Feature Requests, Questions is also contributing 🥰

https://aka.ms/alz/bicep
https://aka.ms/alz/tf
https://aka.ms/alz/repo

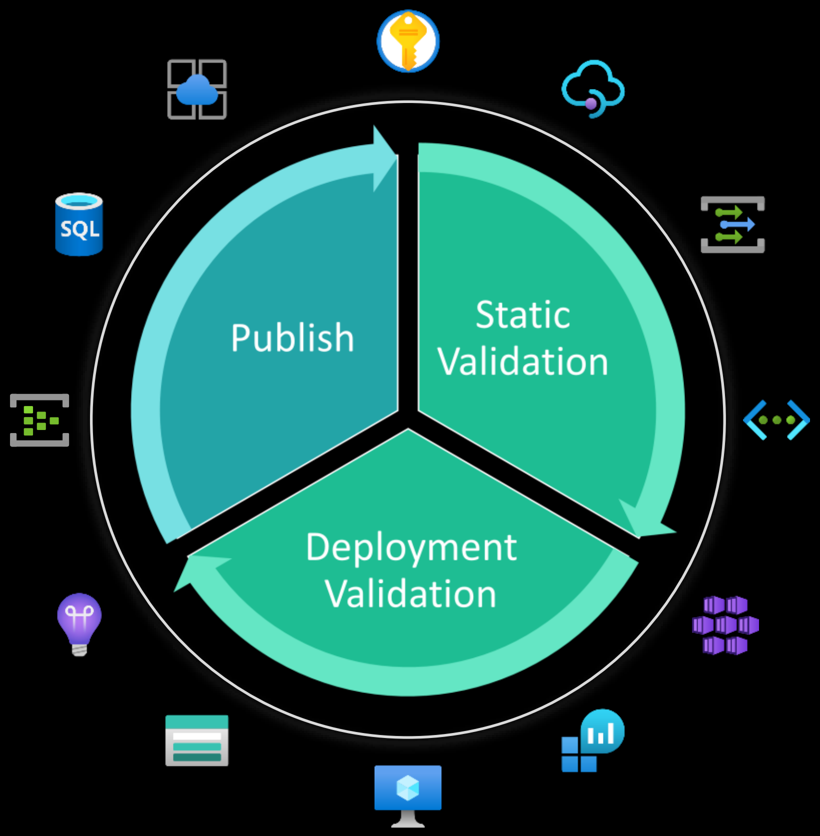
CARML

Common Azure Resource Modules Library

The Common Azure Resource Modules Library (CARML)

- A library of comprehensive, reusable, Bicep-based building blocks to deploy Azure resources

- A continuous integration (CI) framework including static code analysis and deployment validation before publishing known good modules
- Supports GitHub & Azure DevOps



Value proposition

- Enable consistent solution development and delivery.
- It accelerates solution development and delivery over time.

https://aka.ms/CARML

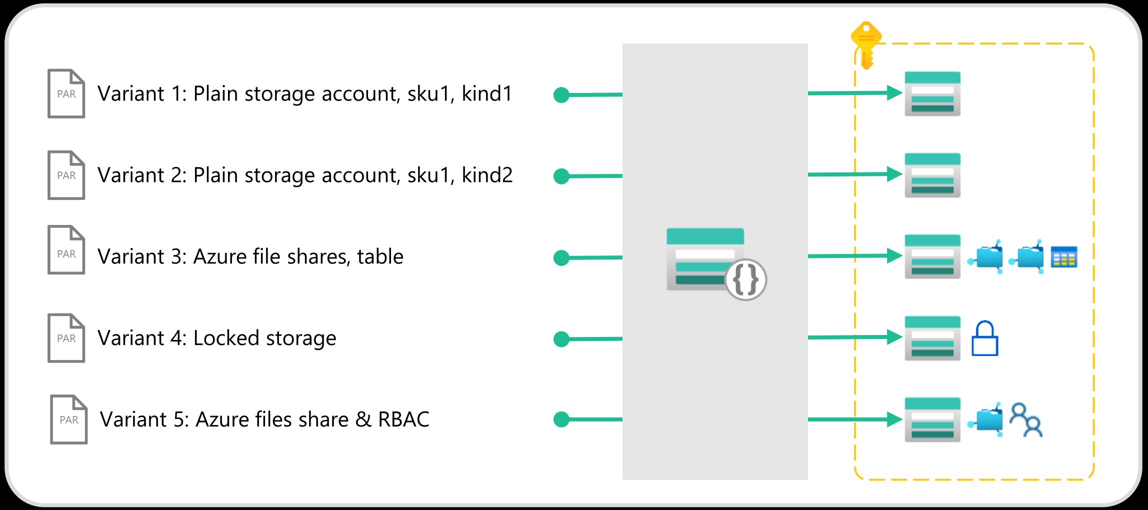
C@RML

Common Azure Resource Modules Library

A module in CARML

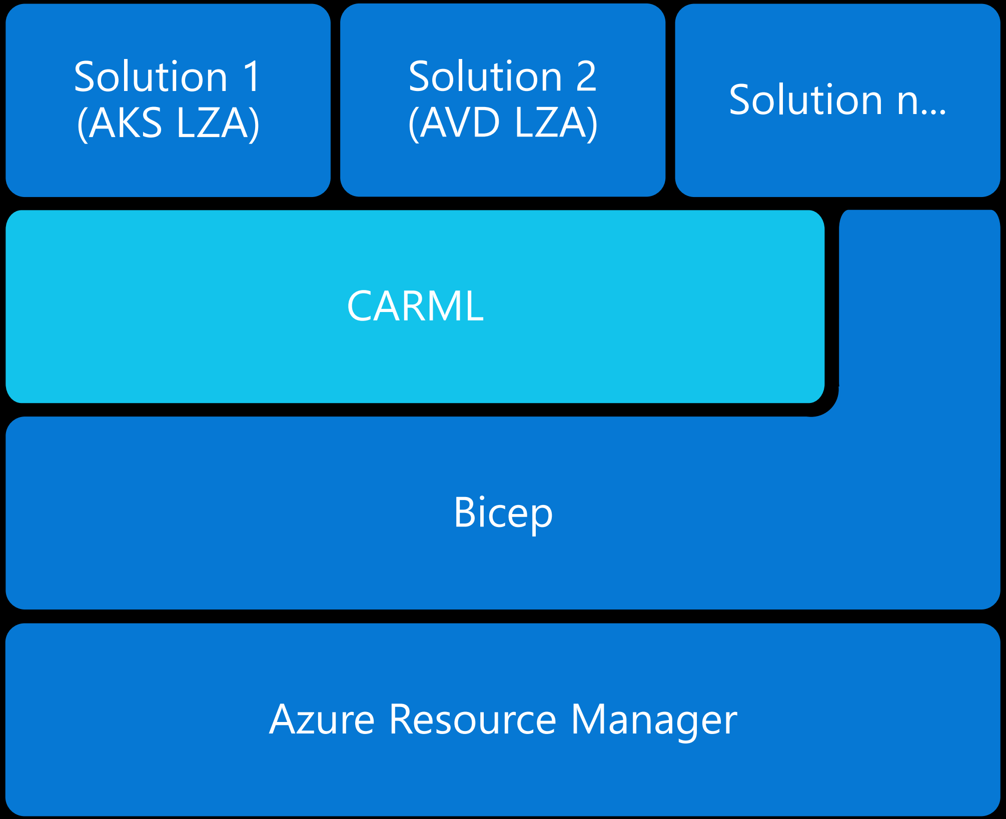
A ***reusable building block*** for *Infrastructure as Code* deployments

Flexible, generalized, **multi-purpose**
Integrates **child resources**
Integrates **extension resources**



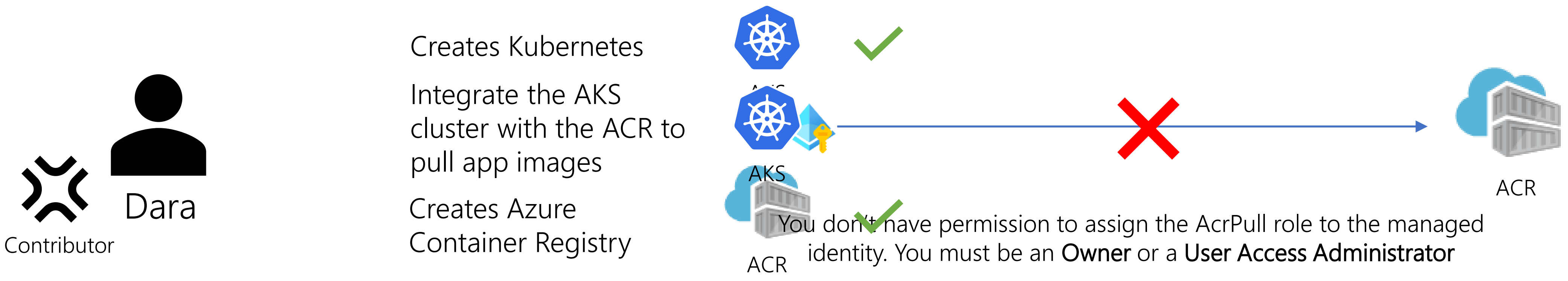
PAR
Variant 1: Plain storage account, sku1, kind1
PAR
Variant 2: Plain storage account, sku1, kind2
PAR
Variant 3: Azure file shares, table
PAR
Variant 4: Locked storage
PAR
Variant 5: Azure files share & RBAC

Deploys a single or strongly correlated services



RBAC Constrained Delegation

Authenticate with Azure Container Registry from Azure Kubernetes Service



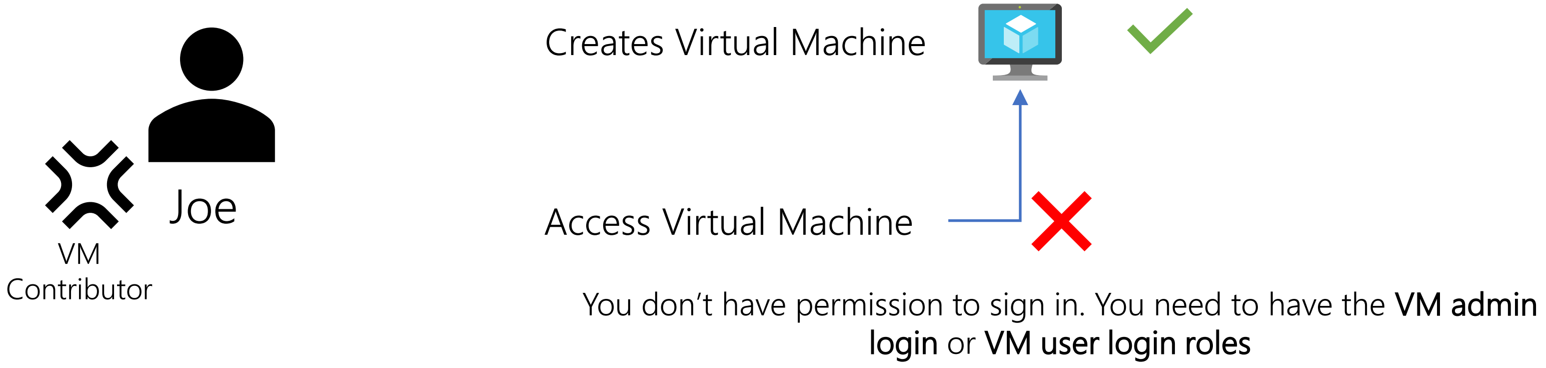
Creates Kubernetes ✓

Integrate the AKS cluster with the ACR to pull app images

Creates Azure Container Registry ✓

You don't have permission to assign the AcrPull role to the managed identity. You must be an **Owner** or a **User Access Administrator**

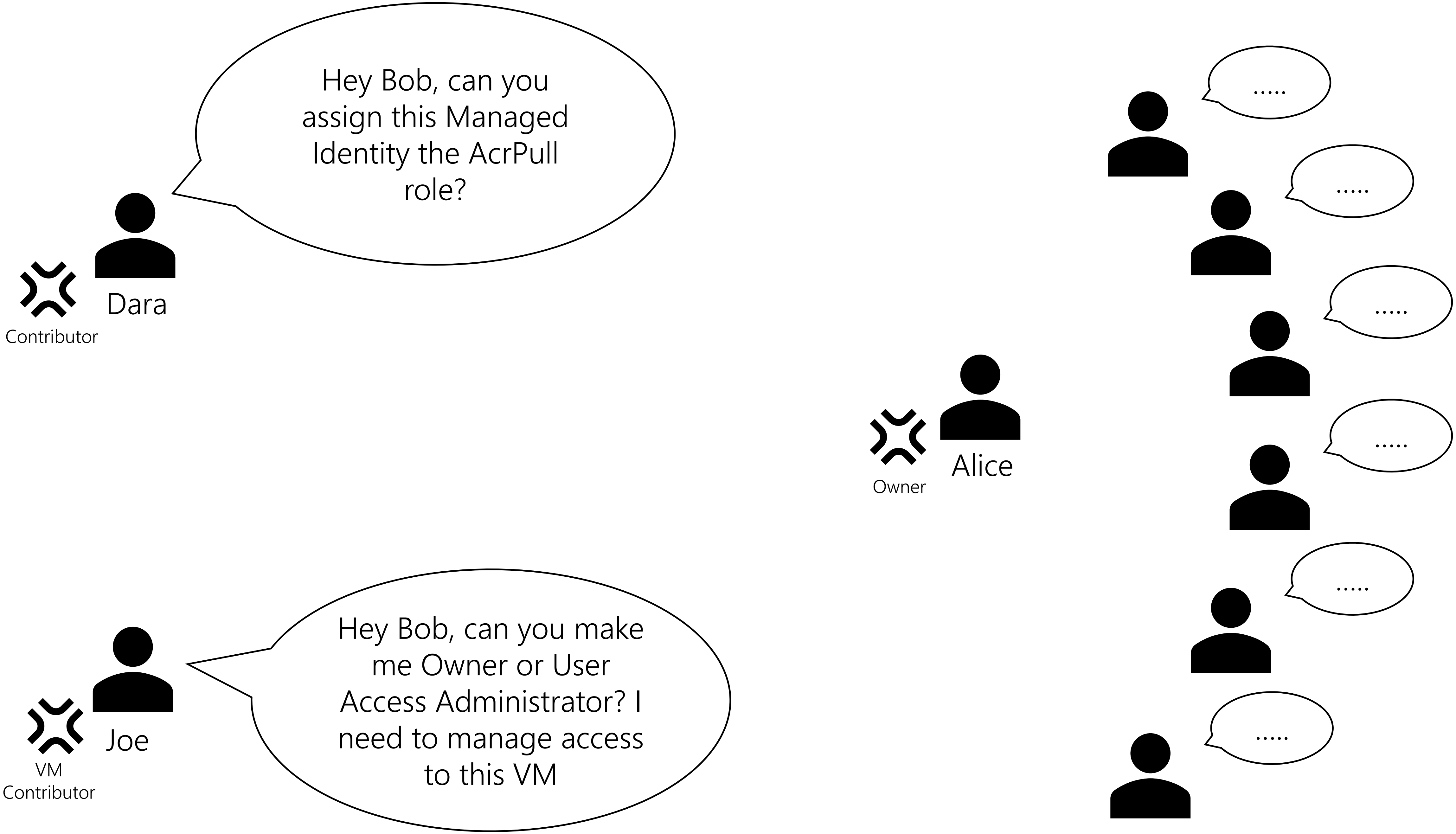
Create and access a Virtual Machine using Azure AD and Azure RBAC



Creates Virtual Machine ✓

Access Virtual Machine

You don't have permission to sign in. You need to have the **VM admin login** or **VM user login roles**


Hey Bob, can you assign this Managed Identity the AcrPull role?
Dara
Contributor
Hey Bob, can you make me Owner or User Access Administrator? I need to manage access to this VM
Joe
VM Contributor
Alice
Owner
.....
.....
.....
.....
.....
.....

Scenarios

- As a Subscription owner, I want to allow a security principal to assign a limited set of roles.
- As a DevOps, I need to access my resources and grant data plane access to my resource.

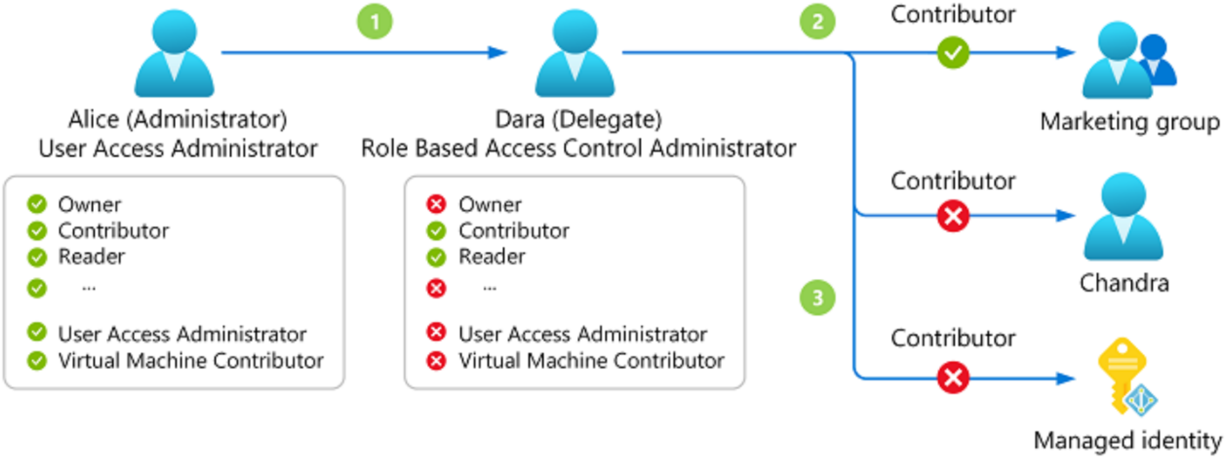
Private preview available now:

As a Subscription owner, I want to allow a security principal to assign a limited set of roles

Alice wants to delegate to Dara the task to assign Azure RBAC roles in the subscription A.

Alice doesn’t want Dara to be able to assign all Azure RBAC roles but just specific roles. For example: Contributor and reader roles

1. Alice assigns Dara the Role Based Access Administrator role
2. Alice uses a conditions to specify which roles Dara can assign.


1
2
3
Alice (Administrator)
User Access Administrator
✓ Owner
✓ Contributor
✓ Reader
✓ ...
✓ User Access Administrator
✓ Virtual Machine Contributor
Dara (Delegate)
Role Based Access Control Administrator
✗ Owner
✓ Contributor
✓ Reader
✗ ...
✗ User Access Administrator
✗ Virtual Machine Contributor
Contributor
Marketing group
Contributor
Chandra
Contributor
Managed identity

As a Subscription/Platform owner, I want to allow a security principal to assign a limited set of roles

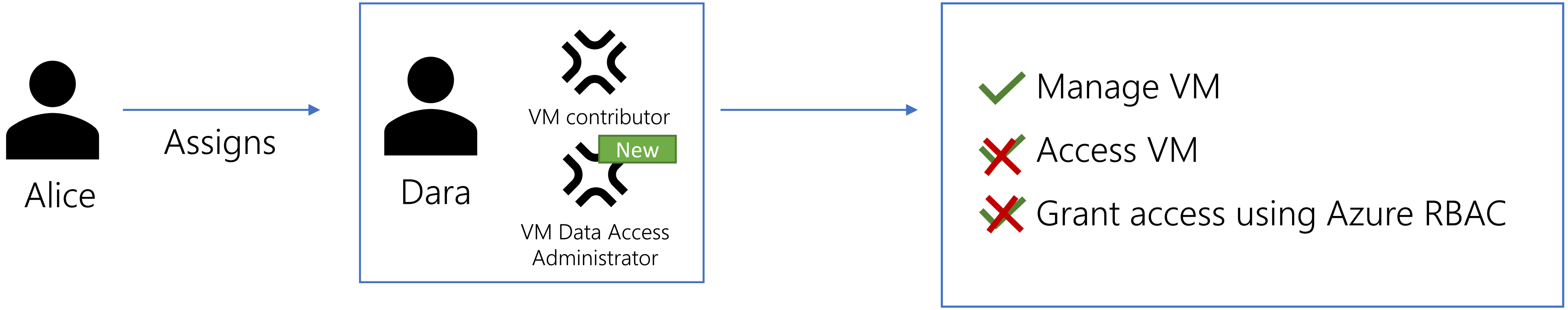
Demo

Delegate Azure role assignments with constraints

Preview coming out early next quarter:

As a DevOps, I need to access the resource I create and to grant data plane access

New role to grant data plane access



- Dara can create a virtual machine using VM contributor
- Data can grant access to the virtual machine using the VM Data Access Administrator role by assigning the VM Admin Login and VM User Login roles.

Microsoft

Q & A

Next Community Call will be in April 👍

Will likely be hosted in an ANZ/APAC friendlier time slot. We will alternate between this and a US friendly time slot.

Stay tuned to issue #1191 (ALZ/ESLZ Repo)

Recordings will be available at aka.ms/ALZ/Community

Microsoft

Thank You! 👋

Stay up-to-date:

https://aka.ms/ALZ/WhatsNew