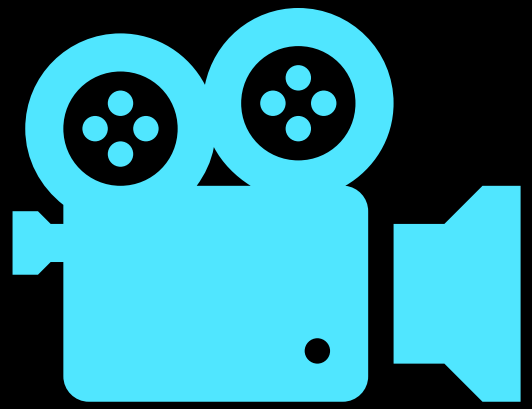
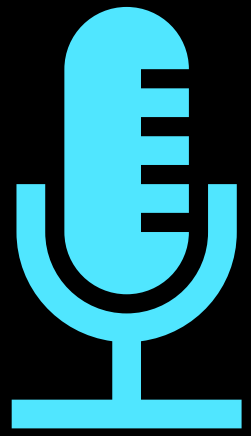
Microsoft

Azure Landing Zones

2nd May 2022 - Community Call

Microsoft





This meeting is being recorded

Agenda

- Welcome
- What's New?
- ALZ-Bicep Update
- ALZ Terraform Module Update
- Q & A

Before we get started...

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

(we have some of 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

Updates

Here's what's changed in Enterprise Scale:

April 2022

Docs

- New CAF document Plan for virtual machine remote access
- New CAF document Use Terraform to deploy Azure landing zones
  - Helps you to understand what Terraform approach and module to use to deploy, manage and operate ALZ
- New CAF document Tailor the Azure landing zone architecture to meet requirements
  - Guidance to help you understand how to tailor the ALZ architecture to meet your additional requirements
- New CAF document Independent software vendor (ISV) considerations for Azure landing zones

Tooling

- Azure Landing Zones Terraform Module v2.0.0 released 🥳
  - Adds support for Virtual WAN plus much more
  - Checkout release notes for details on all the changes and fixes
  - Checkout upgrade guide for details on how to upgrade to the latest release
- Updated Private DNS Zones that are created for Private Link/Endpoints in Portal Experience as per documentation here: Azure Private Endpoint DNS configuration
  - Also fixes issue 944
- Added Telemetry to Portal Experience. More info here Telemetry Tracking Using Customer Usage Attribution (PID)
- Increase `preparingToLaunch` deployment delay in portal experience to improve scenario in issue 902
- Added warnings to use dedicated Subscriptions for platform services when selecting the dedicated model to help avoid deployment failures seen when selecting the same Subscription in the dedicated platform Subscription model for Management, Identity and Connectivity
  - Improving experience as suggested in issue 910
  - Customers wanting a single subscription for platform services should select the 'Single' option on the 'Azure Core Setup' blade

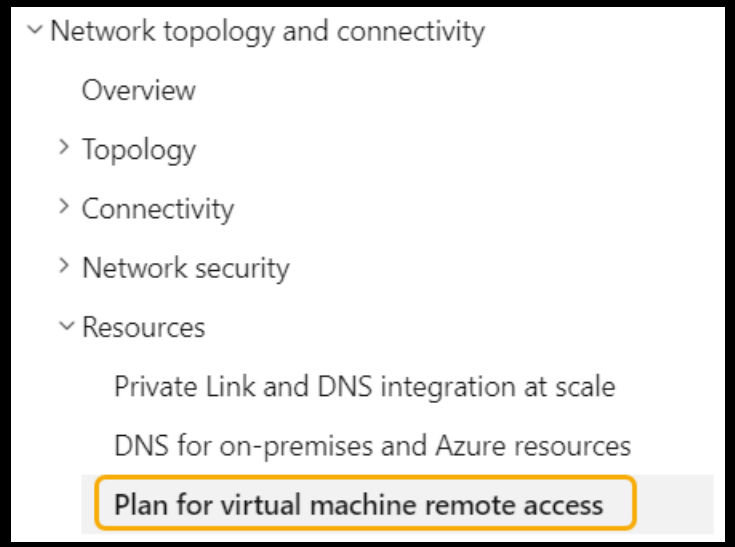
Policy

- Added new custom policy definition called `Deny vNet peering to non-approved vNets`
  - This is useful in scenarios where you only want to allow vNet peering to say a central hub vNet and not allow other vNet peerings between landing zones to be enabled.

Other

New CAF doc

Plan for VM Remote Access



https://aka.ms/ALZ/WhatsNew

Plan for virtual machine remote access

Article • 04/04/2022 • 3 minutes to read • 4 contributors

This article describes the recommended guidance for providing remote access to virtual machines (VMs) deployed within an Azure landing zones architecture.

Azure offers different technologies for providing remote access to VMs:

- Azure Bastion, a platform as a service (PaaS) solution, for accessing VMs through a browser or currently in preview through the native SSH/RDP client on Windows workstations
- Just in time (JIT) access provided through Microsoft Defender for Cloud
- Hybrid connectivity options, such as Azure ExpressRoute and VPNs
- Public IP attached directly to the VM or through a NAT rule via an Azure public load balancer

The choice of which remote access solution is most appropriate depends on factors like scale, topology, and security requirements.

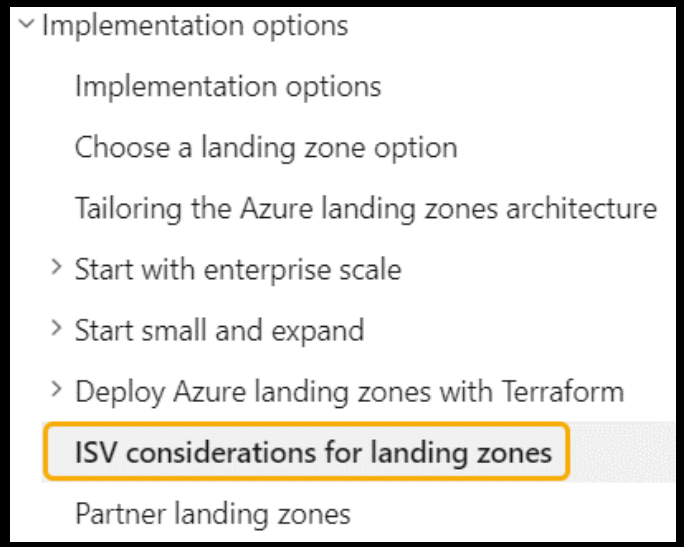
Design considerations

- When available, you can use existing hybrid connectivity to Azure virtual networks via ExpressRoute or S2S/P2S VPN connections to provide remote access from on-premises to Windows and Linux Azure VMs.
- NSGs can be used to secure SSH/RDP connections to Azure VMs.
- JIT allows remote SSH/RDP access over the internet without having to deploy any other infrastructure.
- There are some availability limitations with JIT access.
  - JIT access can't be used for VMs protected by Azure firewalls controlled by Azure Firewall Manager.
- Azure Bastion provides an extra layer of control. It enables secure and seamless RDP/SSH connectivity to your VMs directly from the Azure portal or native client in preview over a secure TLS channel. Azure Bastion also negates the need for hybrid connectivity.
- Consider the appropriate Azure Bastion SKU to use based on your requirements as described in About Azure Bastion configuration settings.
- Review the Azure Bastion FAQ for answers to common questions you might have about the service.
- Azure Bastion can be used in Azure Virtual WAN topology. Known limitations include:
  - Azure Bastion can't be deployed in a Virtual WAN virtual hub.

In this article
Design considerations
Design recommendations

New CAF doc

Independent software vendor (ISV) considerations for Azure landing zones



https://aka.ms/ALZ/WhatsNew

Independent software vendor (ISV) considerations for Azure landing zones

Article • 22/04/2022 • 17 minutes to read • 4 contributors

For many organizations, the Azure landing zones conceptual architecture represents the destination of their cloud adoption journey. The landing zones describe how to build an Azure environment with multiple subscriptions. Each landing zone accounts for scale, security, governance, networking, and identity, and is based on feedback and lessons learned from many customers.

> **Tip**
>
> It can be helpful to think of Azure landing zones as being like city plans. The architectures of workloads deployed into a landing zone are like plans for buildings in a city.
>
> A city's water, gas, electricity, and transport systems all must be in place before buildings can be constructed. Similarly, an Azure landing zone's components, including management groups, policies, subscriptions, and role-based access control (RBAC), all must be in place before any production workloads can be deployed.

As an independent software vendor (ISV) building and operating your solution on Azure, you should refer to the following resources as you build your Azure environment:

- Azure landing zones: Provides guidance for your overall Azure environment.
- Azure Well-Architected Framework: Provides architectural guidance applicable to all workloads.
- Architecting multitenant solutions on Azure: Provides specific architectural guidance for **multitenant** solutions on Azure.

The Azure landing zones help you choose a direction for your overall Azure environment. But as an ISV, SaaS provider, or startup, your specific implementation needs might differ from more standard customer scenarios. The following are just a few different implementation scenario examples:

- You build software that customers deploy into their own subscriptions.
- You have your own *control plane* and use automation scripts or software to deploy and configure Azure resources for your SaaS solutions.

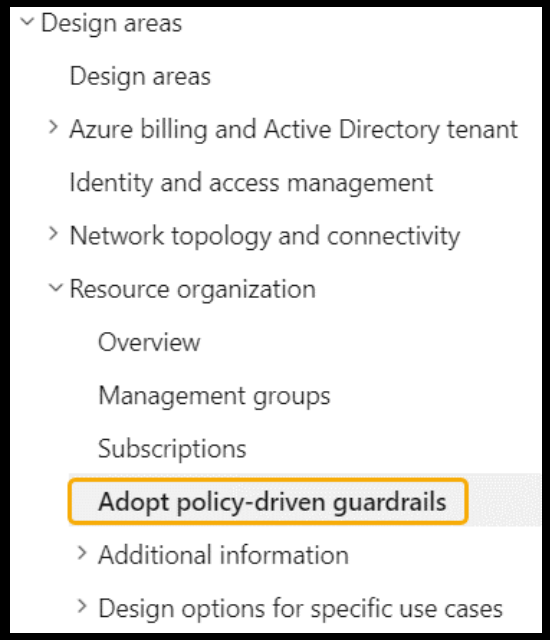
In this article

ISV deployment models
Azure landing zone design principles and implementations
Azure AD tenants
Management groups
Next steps

Show less

Adopt policy-driven guardrails

New CAF doc



https://aka.ms/ALZ/WhatsNew

Adopt policy-driven guardrails

Article • 22/04/2022 • 11 minutes to read • 8 contributors

Before you use policies, you need to understand where they're used within the Azure landing zone reference implementations and why. This article will help you understand whether you want to prevent DeployIfNotExists (DINE) or Modify policies from making changes within your Azure environment.

Why use DINE and Modify policies?

DINE and Modify policies are part of the Azure landing zone reference implementations. They help you and your organization ensure your landing zones, which are also known as subscriptions, and the resources within them are compliant. These policies also remove the operational burden for platform and landing zone teams as your Azure environment scales.

For example, consider a scenario where a new landing zone subscription is provisioned and placed in the "corp" management group. DINE and Modify policies then take the following actions for the landing zone subscription:

- Enable Microsoft Defender for Cloud. Configure Defender for Cloud exports to the central Log Analytics workspace in the management subscription.
- Enable Defender for Cloud for the different supported offerings based on the policy parameters configured on the policy assignment.
- Configure the Azure Activity logs to be sent to the central Log Analytics workspace in the management subscription.
- Configure the diagnostic settings for all resources to be sent to the central Log Analytics workspace in the management subscription.
- Deploy the required Azure Monitor agents for virtual machines and Azure Virtual Machine Scale Sets, including Azure Arc connected servers. Connect them to the central Log Analytics workspace in the management subscription.

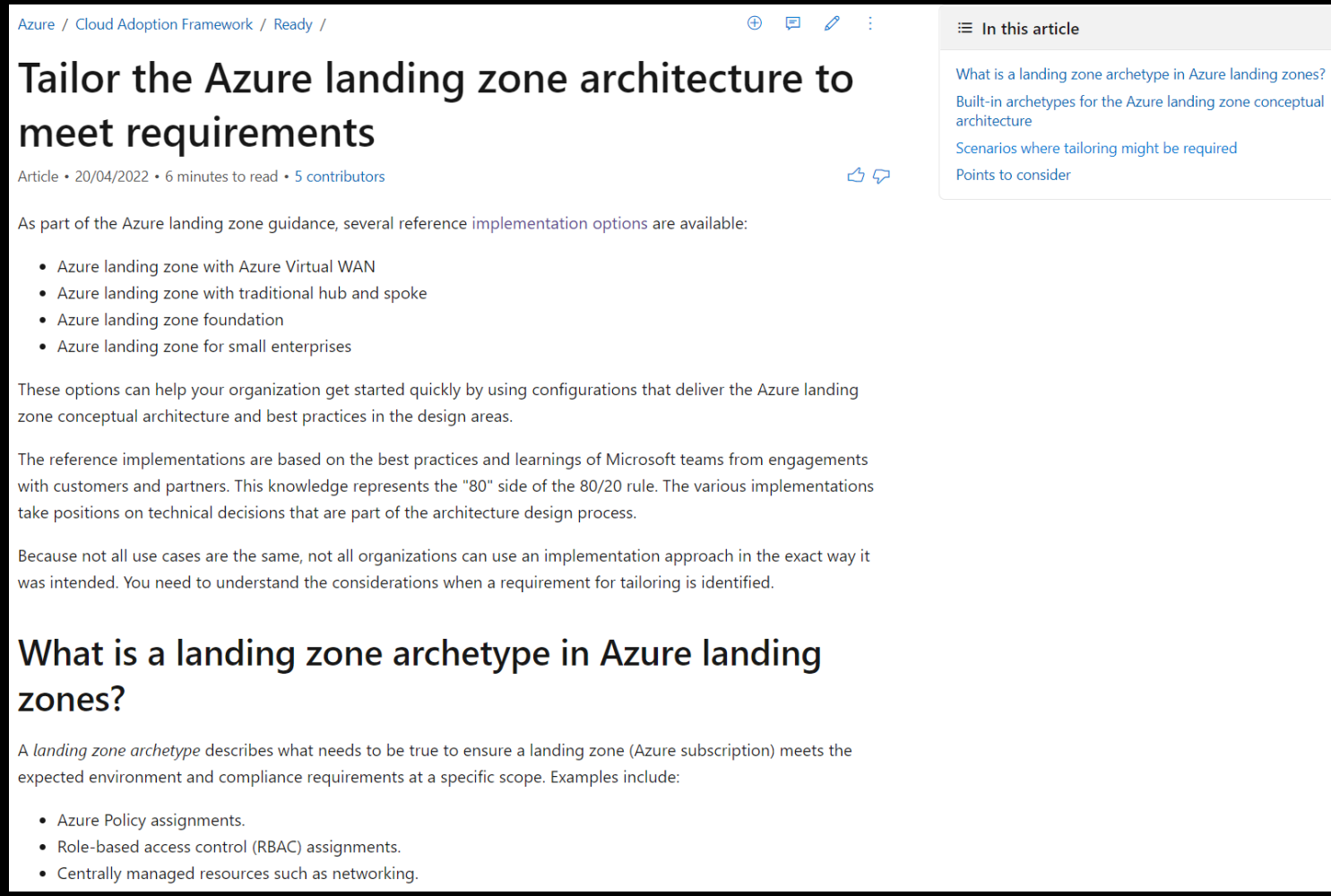
> **Note**
>
> You can disable the preceding options at any time or during deployment of the Azure landing zone reference implementations.
>
> The preceding list shows a subset of all the policies that are assigned as part of the Azure landing zone accelerator. For a full list of policies that can be assigned by the Azure landing zone reference implementation, see **Policies included in enterprise-scale landing zones reference implementations**.

New CAF doc

Tailor the Azure landing zone architecture

- Implementation options
  - Implementation options
  - Choose a landing zone option
  - **Tailoring the Azure landing zones architecture**
  - Start with enterprise scale
  - Start small and expand
  - Deploy Azure landing zones with Terraform
  - ISV considerations for landing zones
  - Partner landing zones

https://aka.ms/ALZ/WhatsNew



Azure / Cloud Adoption Framework / Ready /

Tailor the Azure landing zone architecture to meet requirements

Article • 20/04/2022 • 6 minutes to read • 5 contributors

In this article

- What is a landing zone archetype in Azure landing zones?
- Built-in archetypes for the Azure landing zone conceptual architecture
- Scenarios where tailoring might be required
- Points to consider

As part of the Azure landing zone guidance, several reference implementation options are available:

- Azure landing zone with Azure Virtual WAN
- Azure landing zone with traditional hub and spoke
- Azure landing zone foundation
- Azure landing zone for small enterprises

These options can help your organization get started quickly by using configurations that deliver the Azure landing zone conceptual architecture and best practices in the design areas.

The reference implementations are based on the best practices and learnings of Microsoft teams from engagements with customers and partners. This knowledge represents the "80" side of the 80/20 rule. The various implementations take positions on technical decisions that are part of the architecture design process.

Because not all use cases are the same, not all organizations can use an implementation approach in the exact way it was intended. You need to understand the considerations when a requirement for tailoring is identified.

What is a landing zone archetype in Azure landing zones?

A *landing zone archetype* describes what needs to be true to ensure a landing zone (Azure subscription) meets the expected environment and compliance requirements at a specific scope. Examples include:

- Azure Policy assignments.
- Role-based access control (RBAC) assignments.
- Centrally managed resources such as networking.

Deploy Azure landing zones by using Terraform

- Implementation options
  - Implementation options
  - Choose a landing zone option
  - Tailoring the Azure landing zones architecture
  - Start with enterprise scale
  - Start small and expand
  - Deploy Azure landing zones with Terraform
    - Overview
    - Azure landing zones Terraform module
    - CAF Terraform landing zones
  - ISV considerations for landing zones
  - Partner landing zones

https://aka.ms/ALZ/WhatsNew

New CAF doc

Deploy Azure landing zones by using Terraform

Article • 28/04/2022 • 2 minutes to read • 5 contributors

Azure provides native services for building your Azure landing zones. Other tools can also help with this effort. One tool that customers and partners often use to deploy landing zones is Terraform by HashiCorp.

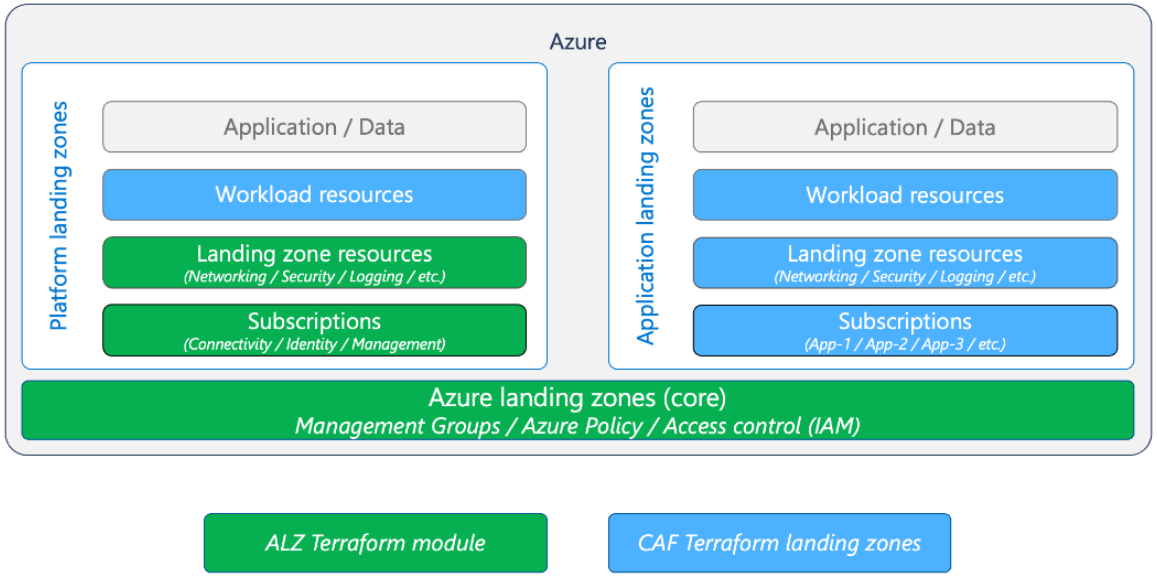
The Terraform module for Azure landing zones is the official Terraform module for deploying the platform resources from the conceptual architecture for Azure landing zones. The module is designed to simplify the deployment of the management group hierarchy, policies, and resources in the connectivity and management subscriptions.

Deployment of resources to application landing zones is outside the scope of the module. Decisions on the deployment method and tooling are for the team that's responsible for the application.

Cloud Adoption Framework Terraform landing zones provide an abstracted, opinionated implementation of Terraform to provide deployment automation in Azure. The set of tools in this approach allows customers to deploy resources into application landing zones by using Terraform, along with providing a mechanism to deploy subscriptions.

The Cloud Adoption Framework approach can also deploy the conceptual architecture for Azure landing zones. It does so by implementing the Terraform module for Azure landing zones.

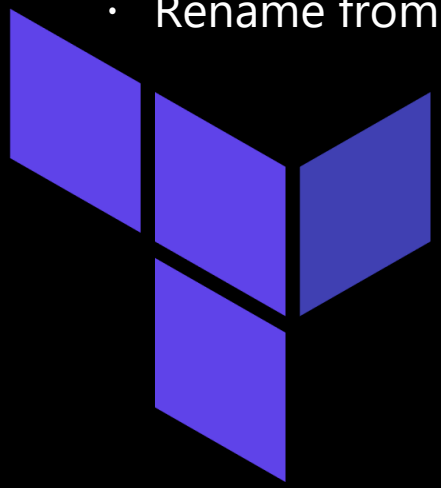
The following diagram illustrates the coverage of the two approaches.



Azure Landing Zones Terraform Module – v2.0.0

Virtual WAN support is now available in v2.0.0 🥹🥹

- Also, a ton of bug fixes, improvements and enhancements 🏋️
  - 20 issues closed out with release ☑
- Check the release notes & Upgrade Guide for all the information you need
  - New features, upgrade notes, breaking changes, etc.
- Rename from ESLZ to ALZ starting also 👍



https://aka.ms/ALZ/TF

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](#)

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 l

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.

Is this page helpful?

Yes No

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.

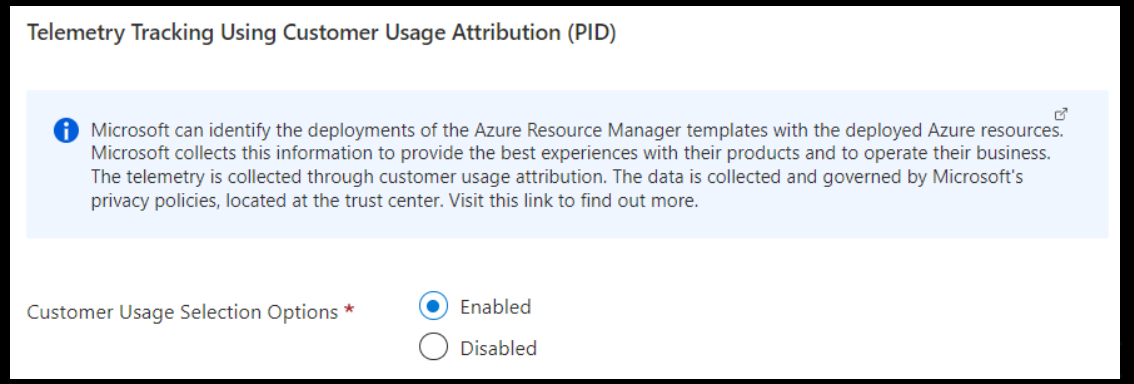
Some FAQ questions that relate more to the architecture are based over in the CAF docs here: Enterprise-scale architecture FAQ

How long does enterprise-scale architecture take to deploy?

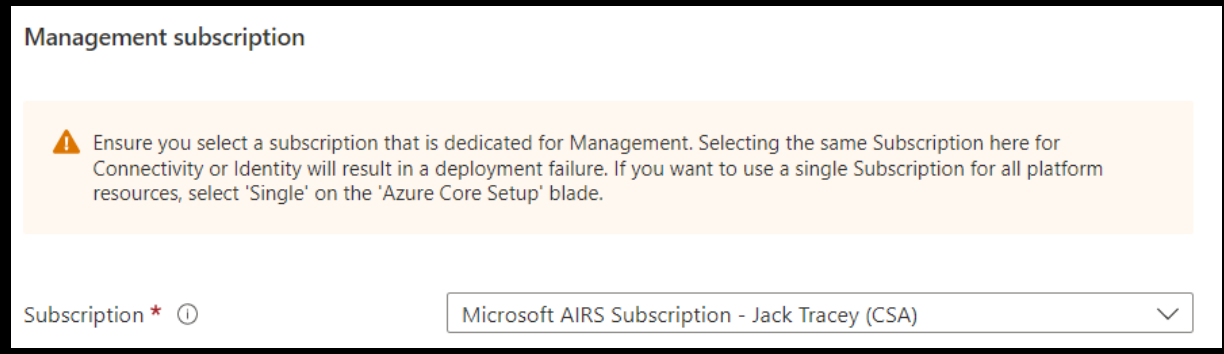
Deployment time depends on the options you select during the implementation experience. It varies from around five minutes to 40 minutes, depending on the options selected.

ALZ Accelerator Update (Portal Experience)

- Added telemetry to help us see usage patterns
  - Can be disabled, see docs



- Increased the "preparingToLaunch" artificial ARM delay to improve policy assignment success – helping issue #902
- Added warning messages to use different dedicated subscriptions for platform subscriptions



ALZ Accelerator Update (Portal Experience)

- Updated to deploy an Azure Firewall Policy Premium SKU instead of Standard when Premium is selected for the Azure Firewall in a Hub & Spoke VNet Connectivity model.

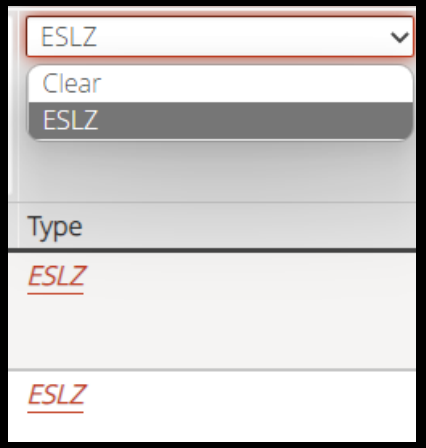
- Updated to deploy an Azure Firewall Policy for customers using the Virtual WAN connectivity model.

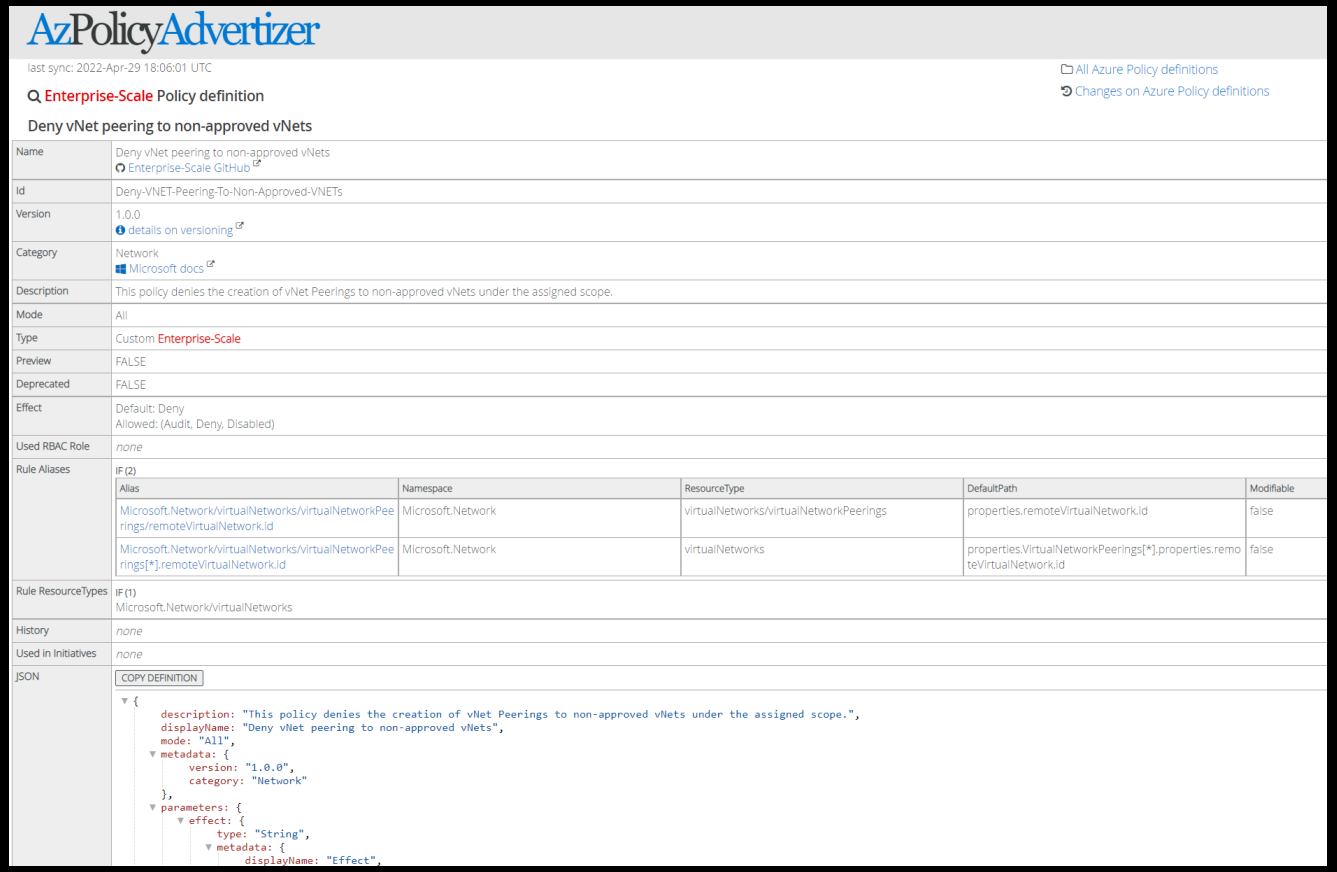
ALZ Policy Updates

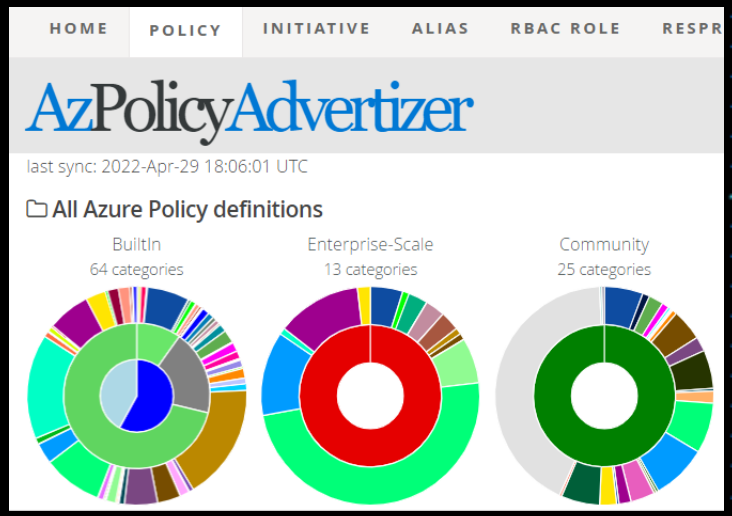
- Replaced ‘Deploy-Default-Udr’ policy with ‘Deploy-Custom-Route-Table’ that allows deploying custom route tables with an arbitrary set of UDRs (including a 0/0 default route if needed). See here for usage details
- Updated ‘Deploy-Budget’ policy, to v1.1.0, adding new parameter of ‘budgetName’ that defaults to: ‘budget-set-by-policy’
- Added ‘AuditEvent’ to ‘Deploy-Diagnostics-AA’
- Renamed ‘Deploy-ASCDF-Config’ to ‘Deploy-MDFC-Config’ and updated version to 3.0.0
  - Aligning to renaming changes in platform
- Updated ‘Deny-Subnet-Without-Nsg’ & ‘Deny-Subnet-Without-Udr’ to version 2.0.0
  - Covering all scenarios/ways that subnets can be created to ensure they are captured
- Added new custom policy definition called ‘Deny vNet peering to non-approved vNets’
  - Useful in scenarios where you only want to allow vNet peering to say a central hub vNet and not allow other vNet peerings between landing zones to be enabled.

ALZ Policy Updates – AzAdvertizer Integration

- Started integration with AzAdvertizer
- Covering Policy Definitions & Initiatives
- Use type column filtering to ‘ESLZ’ (working on rename to ALZ)







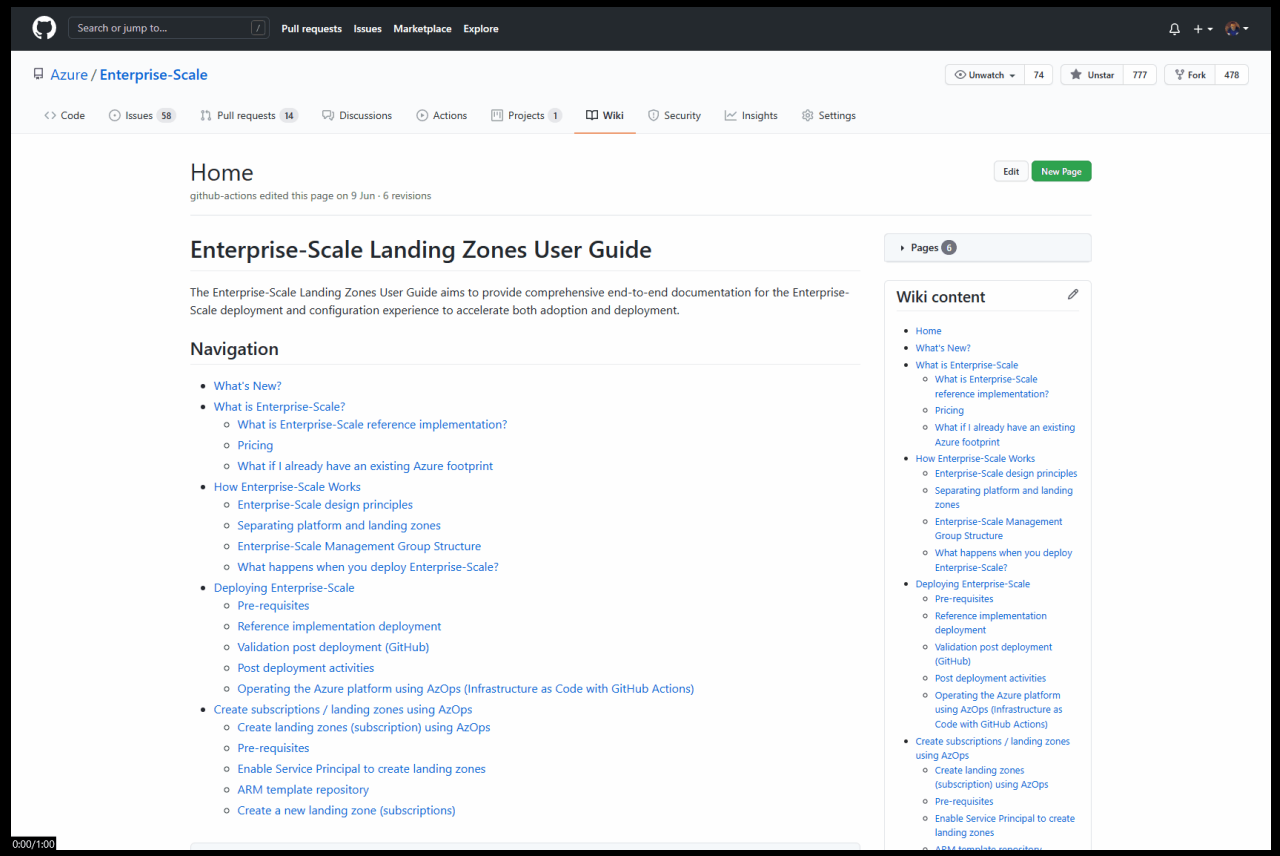
We Want You!

https://aka.ms/ALZ/Repo

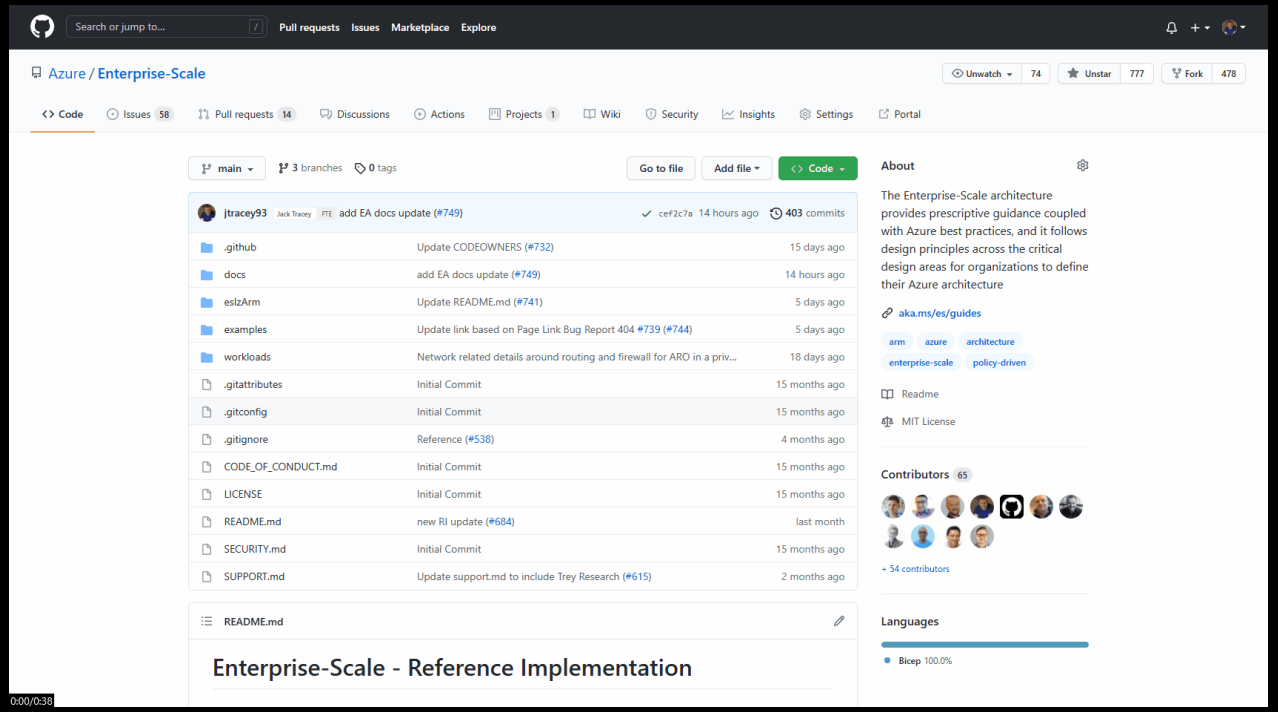
To contribute to ALZ

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

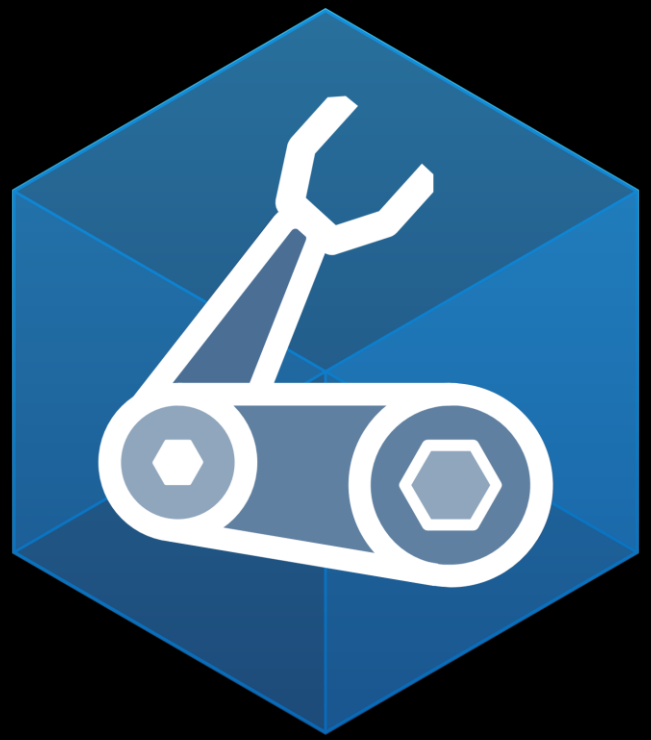
Update docs/wiki:



Create an issue/feature request:



ALZ Bicep Update



- Public Preview launched at start of February
- Lots of activity and usage seen across customers, partners and others
  - 214 stars
  - Good number of contributions from external contributors
- Complete coverage for the ALZ required resources
- Currently v0.6.1
  - Using GitHub releases to help everyone keep track of updates and changes etc.
  - Especially any breaking changes
- Modules are ready for usage in production, they are just normal supported Bicep templates/modules
- Added a Consumer Guide to help with usage patterns/scenarios
- Upcoming “Schooled in ALZ Bicep” episode with JohnnyChipz (MVP) – stay tuned here

ALZ Bicep Modules High Level

Modules

- Management Groups
- Subscription Placement
- Custom Policy Definitions
- Policy Assignments
- Logging & Automation
- Hub Network - Traditional
- Hub Network - VWAN
- Custom Role Definitions
- RBAC Role Assignments

Orchestration Templates

- Hub & Spoke (Adventure Works)
- **GA Goal**
- VWAN (Contoso)
- **GA Goal**
- No Hybrid Connectivity (Wingtip)

OR

OR

Users can choose an orchestration template

https://github.com/Azure/bicep/issues/5371

Now fixed which enables this for us.

We are testing currently

Simplest Path

ALZ Bicep Modules High Level

Modules

- Management Groups
- Subscription Placement
- Custom Policy Definitions
- Policy Assignments
- Logging & Automation
- Hub Network - Traditional
- Hub Network - VWAN
- Custom Role Definitions
- RBAC Role Assignments

Flexibility Option 1

Or users can choose to use individual modules (with sequencing guidance)

ALZ Bicep Modules High Level

Flexibility Option 2

Modules

- Management Groups
- Subscription Placement
- Custom Policy Definitions
- Policy Assignments
- Logging & Automation
- Hub Network - Traditional
- Hub Network - VWAN
- Custom Role Definitions
- RBAC Role Assignments

OR

AND

Or users can choose to build their own orchestration module/s using individual modules (with sequencing guidance)

ALZ Bicep Modules High Level

Flexibility Option 3

Modules

- Management Groups
- Subscription Placement
- Custom Policy Definitions
- Policy Assignments
- Logging & Automation
- Hub Network - Traditional
- Hub Network - VWAN
- Custom Role Definitions
- RBAC Role Assignments

OR

Or users can choose to build their own orchestration module/s using individual modules (with sequencing guidance)

What does “evergreen” mean to you?

Let us know in the feedback survey – Question 2

https://aka.ms/ALZCommunitySurvey

Microsoft

Q & A

Microsoft

Thank You!

https://aka.ms/ALZCommunitySurvey

Stay up-to-date:
https://aka.ms/ALZ/WhatsNew