This month's presenters:

Microsoft

# Azure Landing Zones

11th March 2024 - External Community Call

**Registration:**
[https://aka.ms/ALZ/CommunityCallRegister](https://aka.ms/ALZ/CommunityCallRegister)

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

Microsoft

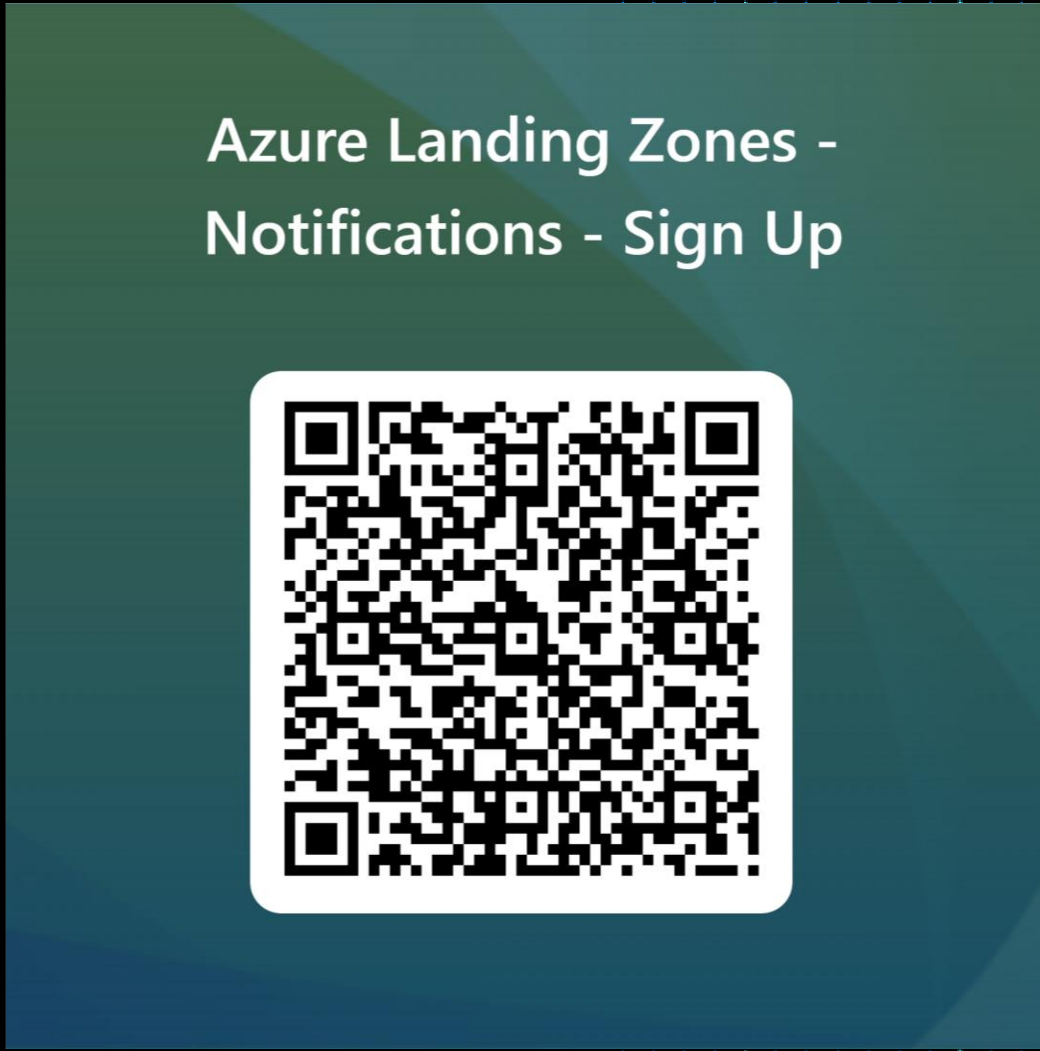
# This meeting is being recorded

Microsoft

# Want to hear about the latest Azure Landing Zone events, news, surveys etc.?

If so, sign up to our mailing list:

aka.ms/alz/notifications/signup



Azure Landing Zones - Notifications - Sign Up

You can also opt out, if registered, by heading to:
aka.ms/alz/notifications/optout

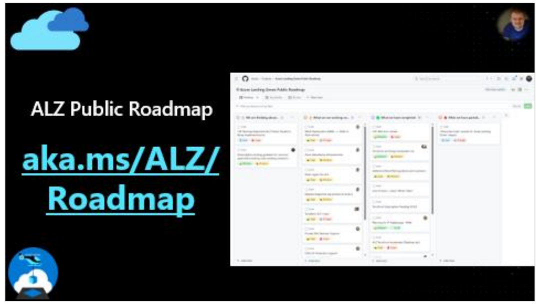
# Before we get started...

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

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

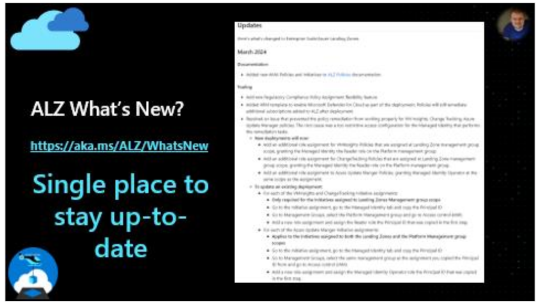
Also we may stop and discuss your question/point at that time, we want this to be an open discussion with all of you 🙂

Implementation Options & Accelerators



ALZ Public Roadmap

aka.ms/ALZ/Roadmap



ALZ What's New?

https://aka.ms/ALZ/WhatsNew

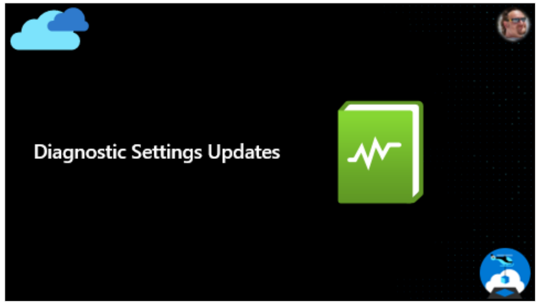
Single place to stay up-to-date

Updates

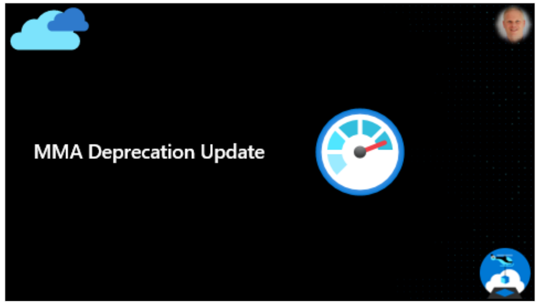
March 2024

Documentation

Policy Refresh Updates



Diagnostic Settings Updates



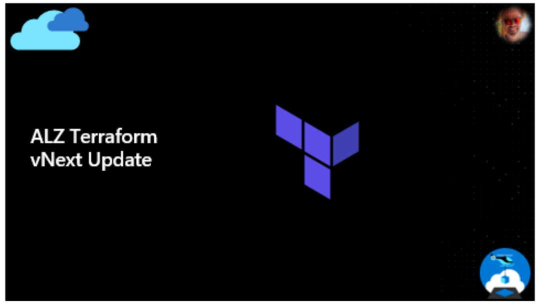
MMA Deprecation Update

AMBA Updates

Zone Redundancy Updates

Multi-Region Updates

ALZ Bicep Updates



ALZ Terraform vNext Update

Microsoft

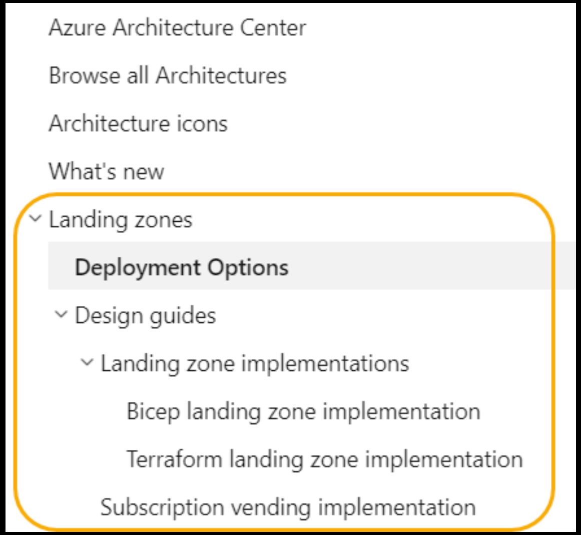
Q & A

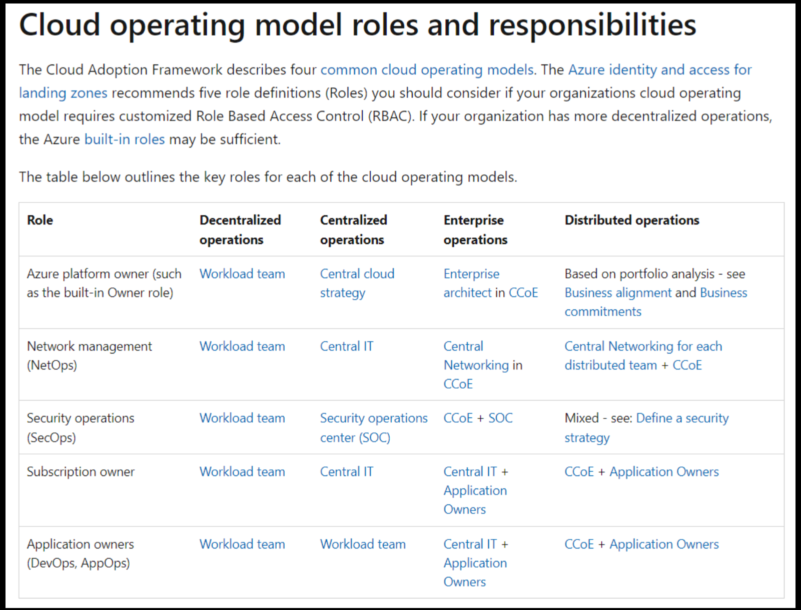
# Agenda

- What’s New in ALZ?
- Policy Refresh Updates
- Diagnostic Settings Policy Updates
- MMA Deprecation Updates
- AMBA Updates
- Zone Redundancy & Multi-Region Updates
- ALZ Bicep Updates
- ALZ TF Updates
- Wrap up

# Implementation Options & Accelerators 🏗️ 🏎️

# Accelerators


Azure Architecture Center
Browse all Architectures
Architecture icons
What's new
Landing zones
Deployment Options
Design guides
Landing zone implementations
Bicep landing zone implementation
Terraform landing zone implementation
Subscription vending implementation

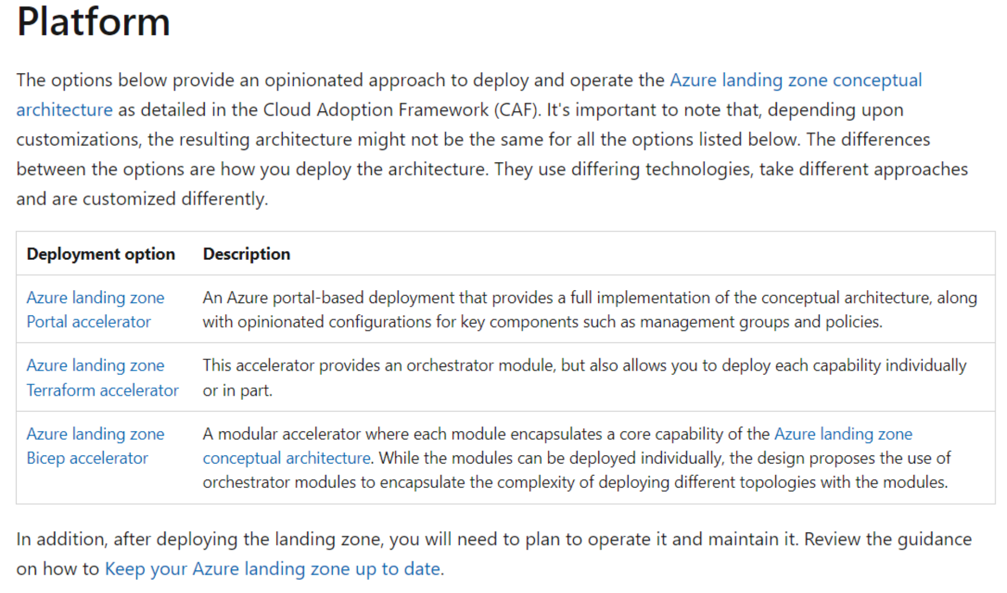


## Cloud operating model roles and responsibilities

The Cloud Adoption Framework describes four common cloud operating models. The Azure identity and access for landing zones recommends five role definitions (Roles) you should consider if your organizations cloud operating model requires customized Role Based Access Control (RBAC). If your organization has more decentralized operations, the Azure built-in roles may be sufficient.

The table below outlines the key roles for each of the cloud operating models.

| Role | Decentralized operations | Centralized operations | Enterprise operations | Distributed operations |
|---|---|---|---|---|
| Azure platform owner (such as the built-in Owner role) | Workload team | Central cloud strategy | Enterprise architect in CCoE | Based on portfolio analysis - see Business alignment and Business commitments |
| Network management (NetOps) | Workload team | Central IT | Central Networking in CCoE | Central Networking for each distributed team + CCoE |
| Security operations (SecOps) | Workload team | Security operations center (SOC) | CCoE + SOC | Mixed - see: Define a security strategy |
| Subscription owner | Workload team | Central IT | Central IT + Application Owners | CCoE + Application Owners |
| Application owners (DevOps, AppOps) | Workload team | Workload team | Central IT + Application Owners | CCoE + Application Owners |

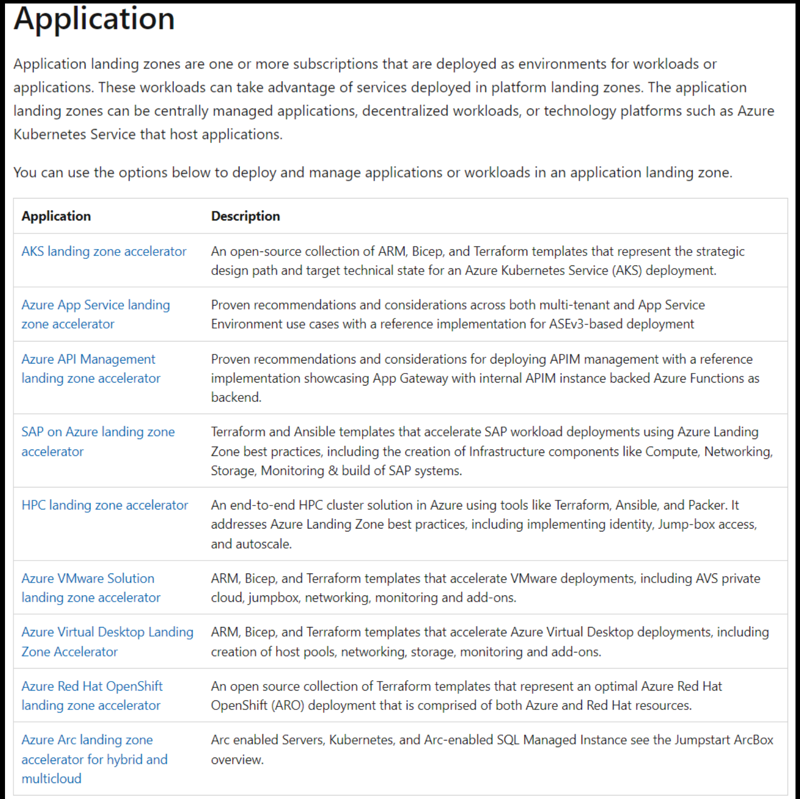


## Platform

The options below provide an opinionated approach to deploy and operate the Azure landing zone conceptual architecture as detailed in the Cloud Adoption Framework (CAF). It's important to note that, depending upon customizations, the resulting architecture might not be the same for all the options listed below. The differences between the options are how you deploy the architecture. They use differing technologies, take different approaches and are customized differently.

| Deployment option | Description |
|---|---|
| Azure landing zone Portal accelerator | An Azure portal-based deployment that provides a full implementation of the conceptual architecture, along with opinionated configurations for key components such as management groups and policies. |
| Azure landing zone Terraform accelerator | This accelerator provides an orchestrator module, but also allows you to deploy each capability individually or in part. |
| Azure landing zone Bicep accelerator | A modular accelerator where each module encapsulates a core capability of the Azure landing zone conceptual architecture. While the modules can be deployed individually, the design proposes the use of orchestrator modules to encapsulate the complexity of deploying different topologies with the modules. |

In addition, after deploying the landing zone, you will need to plan to operate it and maintain it. Review the guidance on how to Keep your Azure landing zone up to date.

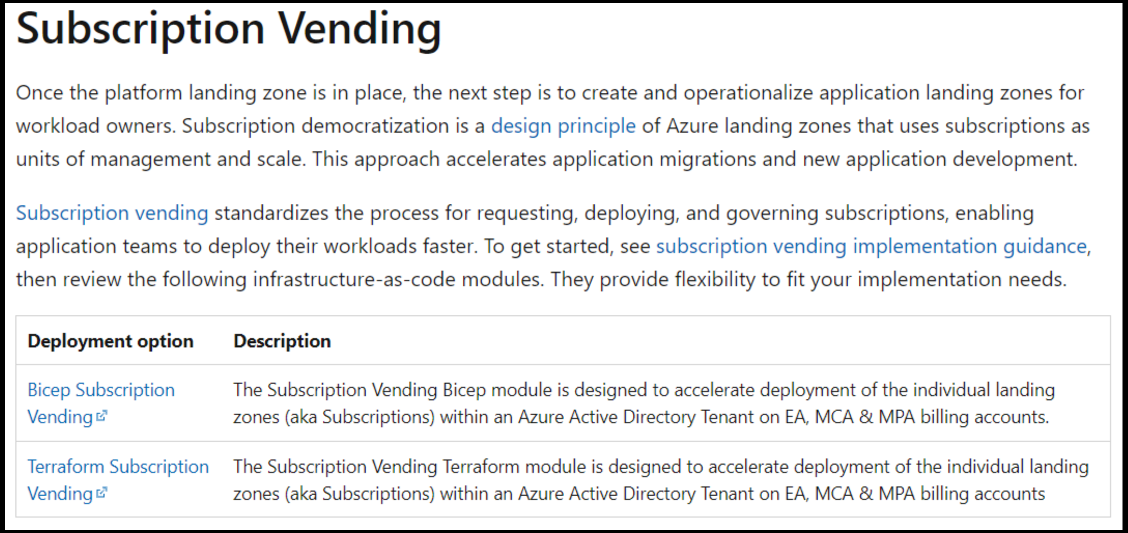


## Application

Application landing zones are one or more subscriptions that are deployed as environments for workloads or applications. These workloads can take advantage of services deployed in platform landing zones. The application landing zones can be centrally managed applications, decentralized workloads, or technology platforms such as Azure Kubernetes Service that host applications.

You can use the options below to deploy and manage applications or workloads in an application landing zone.

| Application | Description |
|---|---|
| AKS landing zone accelerator | An open-source collection of ARM, Bicep, and Terraform templates that represent the strategic design path and target technical state for an Azure Kubernetes Service (AKS) deployment. |
| Azure App Service landing zone accelerator | Proven recommendations and considerations across both multi-tenant and App Service Environment use cases with a reference implementation for ASEv3-based deployment |
| Azure API Management landing zone accelerator | Proven recommendations and considerations for deploying APIM management with a reference implementation showcasing App Gateway with internal APIM instance backed Azure Functions as backend. |
| SAP on Azure landing zone accelerator | Terraform and Ansible templates that accelerate SAP workload deployments using Azure Landing Zone best practices, including the creation of Infrastructure components like Compute, Networking, Storage, Monitoring & build of SAP systems. |
| HPC landing zone accelerator | An end-to-end HPC cluster solution in Azure using tools like Terraform, Ansible, and Packer. It addresses Azure Landing Zone best practices, including implementing identity, Jump-box access, and autoscale. |
| Azure VMware Solution landing zone accelerator | ARM, Bicep, and Terraform templates that accelerate VMware deployments, including AVS private cloud, jumpbox, networking, monitoring and add-ons. |
| Azure Virtual Desktop Landing Zone Accelerator | ARM, Bicep, and Terraform templates that accelerate Azure Virtual Desktop deployments, including creation of host pools, networking, storage, monitoring and add-ons. |
| Azure Red Hat OpenShift landing zone accelerator | An open source collection of Terraform templates that represent an optimal Azure Red Hat OpenShift (ARO) deployment that is comprised of both Azure and Red Hat resources. |
| Azure Arc landing zone accelerator for hybrid and multicloud | Arc enabled Servers, Kubernetes, and Arc-enabled SQL Managed Instance see the Jumpstart ArcBox overview. |



## Subscription Vending

Once the platform landing zone is in place, the next step is to create and operationalize application landing zones for workload owners. Subscription democratization is a design principle of Azure landing zones that uses subscriptions as units of management and scale. This approach accelerates application migrations and new application development.

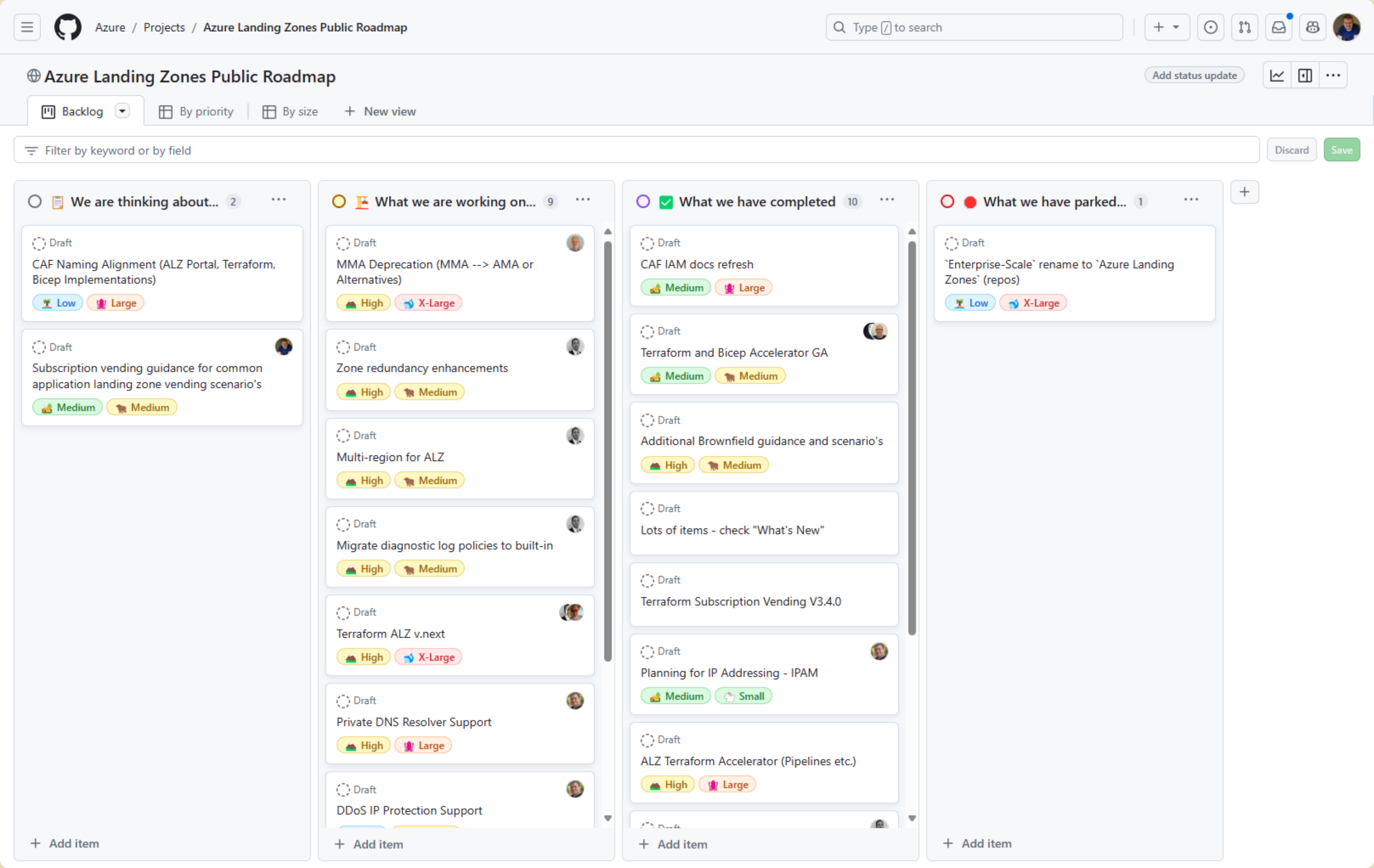
Subscription vending standardizes the process for requesting, deploying, and governing subscriptions, enabling application teams to deploy their workloads faster. To get started, see subscription vending implementation guidance, then review the following infrastructure-as-code modules. They provide flexibility to fit your implementation needs.

| Deployment option | Description |
|---|---|
| Bicep Subscription Vending | The Subscription Vending Bicep module is designed to accelerate deployment of the individual landing zones (aka Subscriptions) within an Azure Active Directory Tenant on EA, MCA & MPA billing accounts. |
| Terraform Subscription Vending | The Subscription Vending Terraform module is designed to accelerate deployment of the individual landing zones (aka Subscriptions) within an Azure Active Directory Tenant on EA, MCA & MPA billing accounts |

aka.ms/ALZ/AAC

# ALZ Public Roadmap

## aka.ms/ALZ/Roadmap


Azure / Projects / Azure Landing Zones Public Roadmap
Type / to search
Add status update
Backlog
By priority
By size
New view
Filter by keyword or by field
Discard
Save

Azure Landing Zones Public Roadmap

**We are thinking about... 2**

- Draft — CAF Naming Alignment (ALZ Portal, Terraform, Bicep Implementations) — Low, Large
- Draft — Subscription vending guidance for common application landing zone vending scenario's — Medium, Medium

**What we are working on... 9**

- Draft — MMA Deprecation (MMA --> AMA or Alternatives) — High, X-Large
- Draft — Zone redundancy enhancements — High, Medium
- Draft — Multi-region for ALZ — High, Medium
- Draft — Migrate diagnostic log policies to built-in — High, Medium
- Draft — Terraform ALZ v.next — High, X-Large
- Draft — Private DNS Resolver Support — High, Large
- Draft — DDoS IP Protection Support

**What we have completed 10**

- Draft — CAF IAM docs refresh — Medium, Large
- Draft — Terraform and Bicep Accelerator GA — Medium, Medium
- Draft — Additional Brownfield guidance and scenario's — High, Medium
- Draft — Lots of items - check "What's New"
- Draft — Terraform Subscription Vending V3.4.0
- Draft — Planning for IP Addressing - IPAM — Medium, Small
- Draft — ALZ Terraform Accelerator (Pipelines etc.) — High, Large

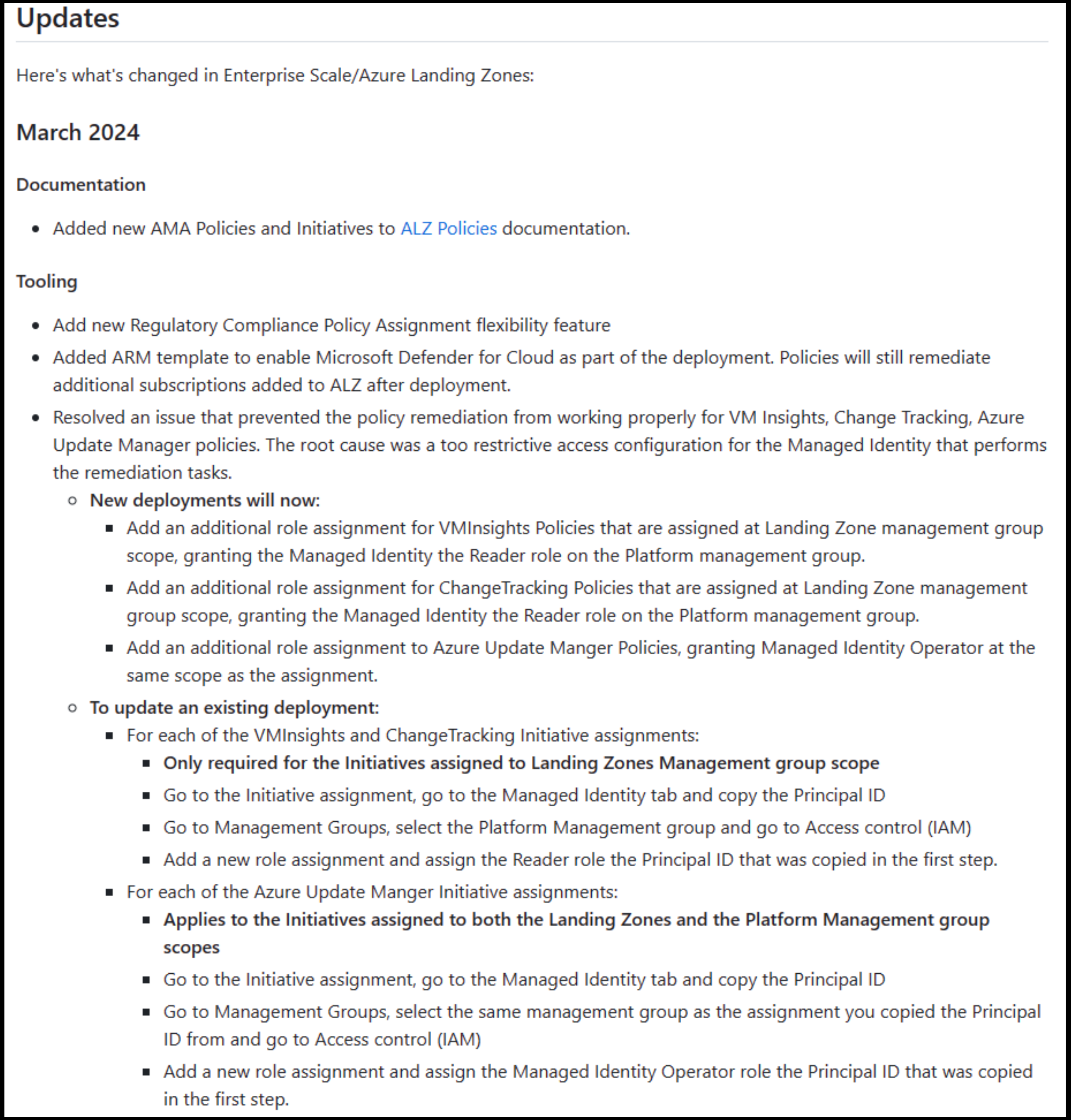
**What we have parked... 1**

- Draft — `Enterprise-Scale` rename to `Azure Landing Zones` (repos) — Low, X-Large

# 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/Azure Landing Zones:

### March 2024

**Documentation**

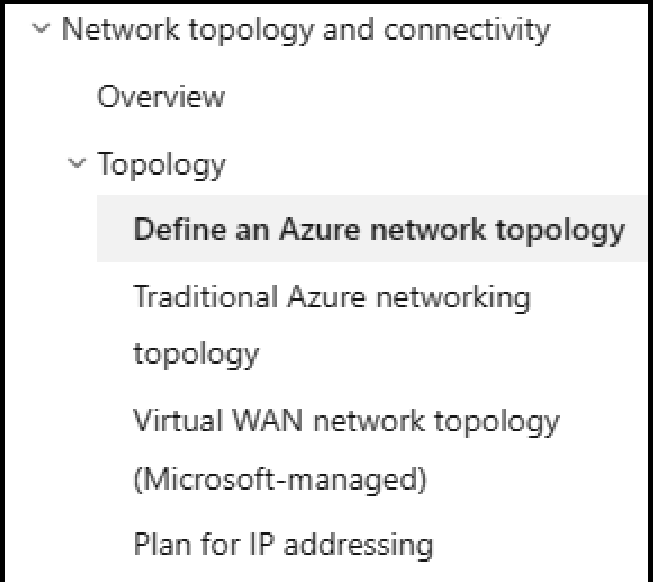
- Added new AMA Policies and Initiatives to ALZ Policies documentation.

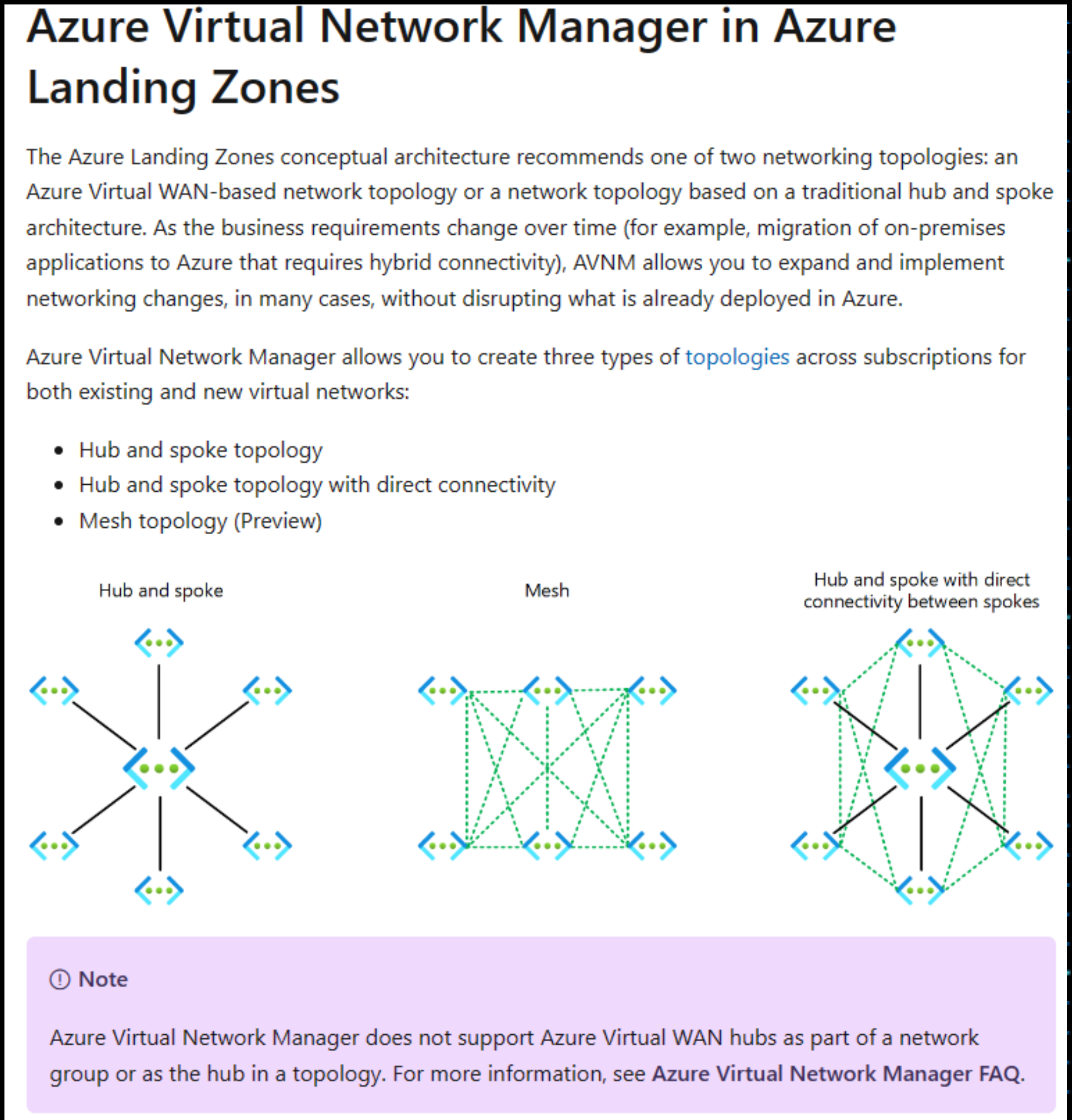
**Tooling**

- Add new Regulatory Compliance Policy Assignment flexibility feature
- Added ARM template to enable Microsoft Defender for Cloud as part of the deployment. Policies will still remediate additional subscriptions added to ALZ after deployment.
- Resolved an issue that prevented the policy remediation from working properly for VM Insights, Change Tracking, Azure Update Manager policies. The root cause was a too restrictive access configuration for the Managed Identity that performs the remediation tasks.
  - **New deployments will now:**
    - Add an additional role assignment for VMInsights Policies that are assigned at Landing Zone management group scope, granting the Managed Identity the Reader role on the Platform management group.
    - Add an additional role assignment for ChangeTracking Policies that are assigned at Landing Zone management group scope, granting the Managed Identity the Reader role on the Platform management group.
    - Add an additional role assignment to Azure Update Manger Policies, granting Managed Identity Operator at the same scope as the assignment.
  - **To update an existing deployment:**
    - For each of the VMInsights and ChangeTracking Initiative assignments:
      - **Only required for the Initiatives assigned to Landing Zones Management group scope**
      - Go to the Initiative assignment, go to the Managed Identity tab and copy the Principal ID
      - Go to Management Groups, select the Platform Management group and go to Access control (IAM)
      - Add a new role assignment and assign the Reader role the Principal ID that was copied in the first step.
    - For each of the Azure Update Manger Initiative assignments:
      - **Applies to the Initiatives assigned to both the Landing Zones and the Platform Management group scopes**
      - Go to the Initiative assignment, go to the Managed Identity tab and copy the Principal ID
      - Go to Management Groups, select the same management group as the assignment you copied the Principal ID from and go to Access control (IAM)
      - Add a new role assignment and assign the Managed Identity Operator role the Principal ID that was copied in the first step.

# New Section in CAF + Updates

## Networking – AVNM


Network topology and connectivity
Overview
Topology
Define an Azure network topology
Traditional Azure networking topology
Virtual WAN network topology (Microsoft-managed)
Plan for IP addressing



## Azure Virtual Network Manager in Azure Landing Zones

The Azure Landing Zones conceptual architecture recommends one of two networking topologies: an Azure Virtual WAN-based network topology or a network topology based on a traditional hub and spoke architecture. As the business requirements change over time (for example, migration of on-premises applications to Azure that requires hybrid connectivity), AVNM allows you to expand and implement networking changes, in many cases, without disrupting what is already deployed in Azure.

Azure Virtual Network Manager allows you to create three types of topologies across subscriptions for both existing and new virtual networks:

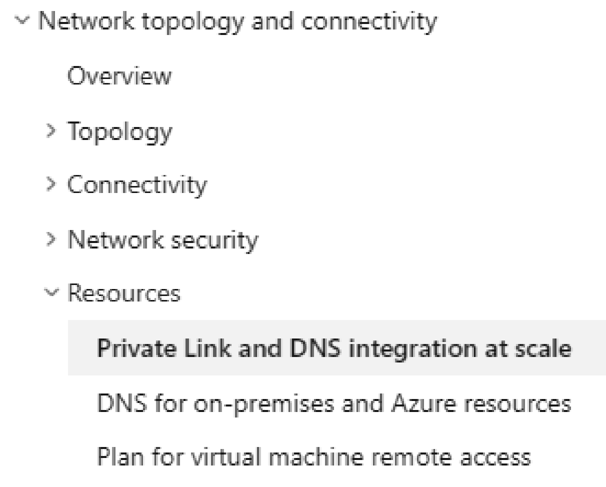
- Hub and spoke topology
- Hub and spoke topology with direct connectivity
- Mesh topology (Preview)

ⓘ Note

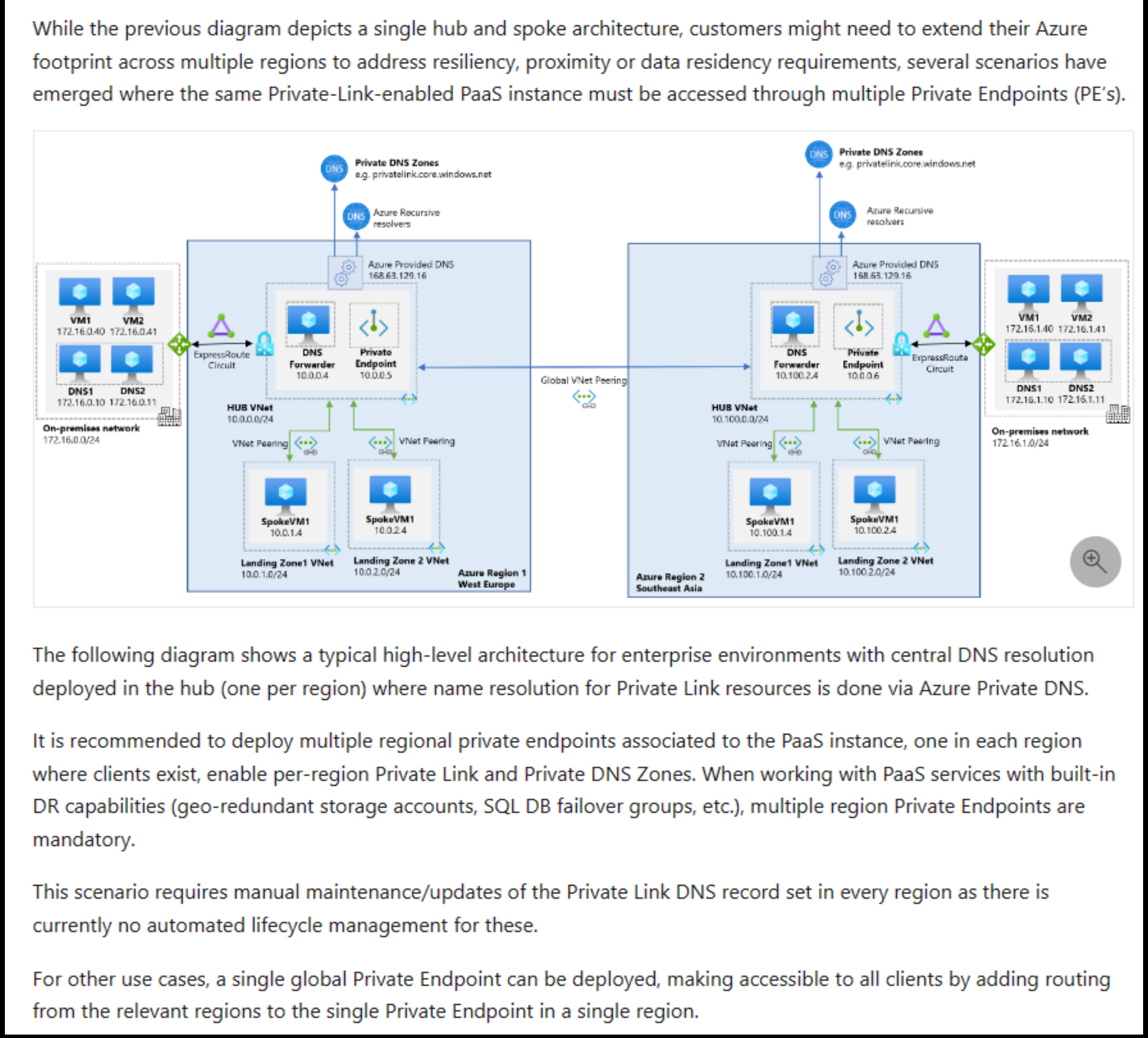
Azure Virtual Network Manager does not support Azure Virtual WAN hubs as part of a network group or as the hub in a topology. For more information, see **Azure Virtual Network Manager FAQ**.

# New Addition to CAF + Updates

## Networking – Multi-Region DNS



- Network topology and connectivity
  - Overview
  - Topology
  - Connectivity
  - Network security
  - Resources
    - **Private Link and DNS integration at scale**
    - DNS for on-premises and Azure resources
    - Plan for virtual machine remote access



While the previous diagram depicts a single hub and spoke architecture, customers might need to extend their Azure footprint across multiple regions to address resiliency, proximity or data residency requirements, several scenarios have emerged where the same Private-Link-enabled PaaS instance must be accessed through multiple Private Endpoints (PE's).

The following diagram shows a typical high-level architecture for enterprise environments with central DNS resolution deployed in the hub (one per region) where name resolution for Private Link resources is done via Azure Private DNS.

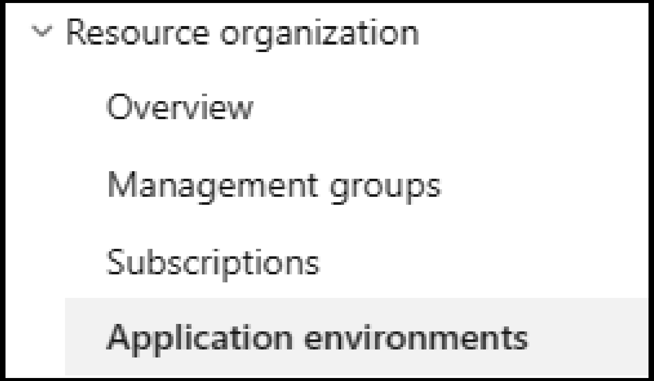
It is recommended to deploy multiple regional private endpoints associated to the PaaS instance, one in each region where clients exist, enable per-region Private Link and Private DNS Zones. When working with PaaS services with built-in DR capabilities (geo-redundant storage accounts, SQL DB failover groups, etc.), multiple region Private Endpoints are mandatory.

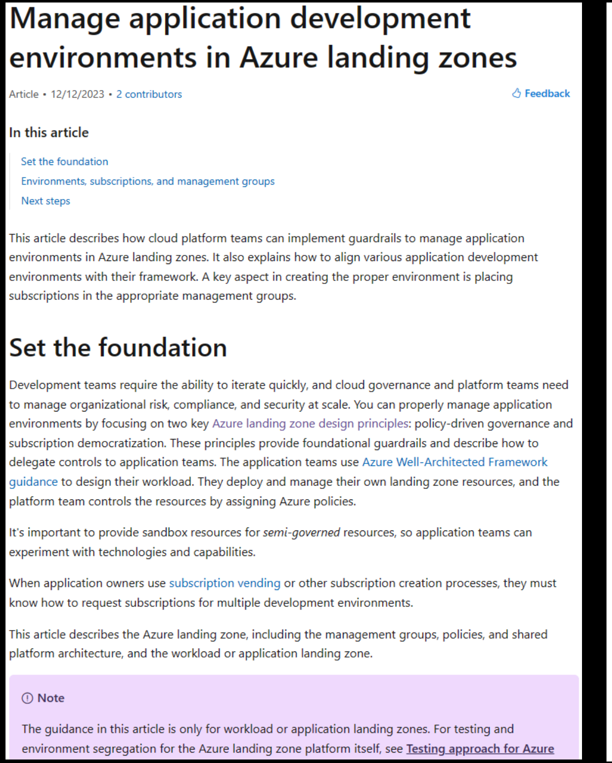
This scenario requires manual maintenance/updates of the Private Link DNS record set in every region as there is currently no automated lifecycle management for these.

For other use cases, a single global Private Endpoint can be deployed, making accessible to all clients by adding routing from the relevant regions to the single Private Endpoint in a single region.

# New CAF Doc

# Manage application development environments in Azure landing zones





## Manage application development environments in Azure landing zones

Article • 12/12/2023 • 2 contributors

**In this article**

- Set the foundation
- Environments, subscriptions, and management groups
- Next steps

This article describes how cloud platform teams can implement guardrails to manage application environments in Azure landing zones. It also explains how to align various application development environments with their framework. A key aspect in creating the proper environment is placing subscriptions in the appropriate management groups.

## Set the foundation

Development teams require the ability to iterate quickly, and cloud governance and platform teams need to manage organizational risk, compliance, and security at scale. You can properly manage application environments by focusing on two key Azure landing zone design principles: policy-driven governance and subscription democratization. These principles provide foundational guardrails and describe how to delegate controls to application teams. The application teams use Azure Well-Architected Framework guidance to design their workload. They deploy and manage their own landing zone resources, and the platform team controls the resources by assigning Azure policies.

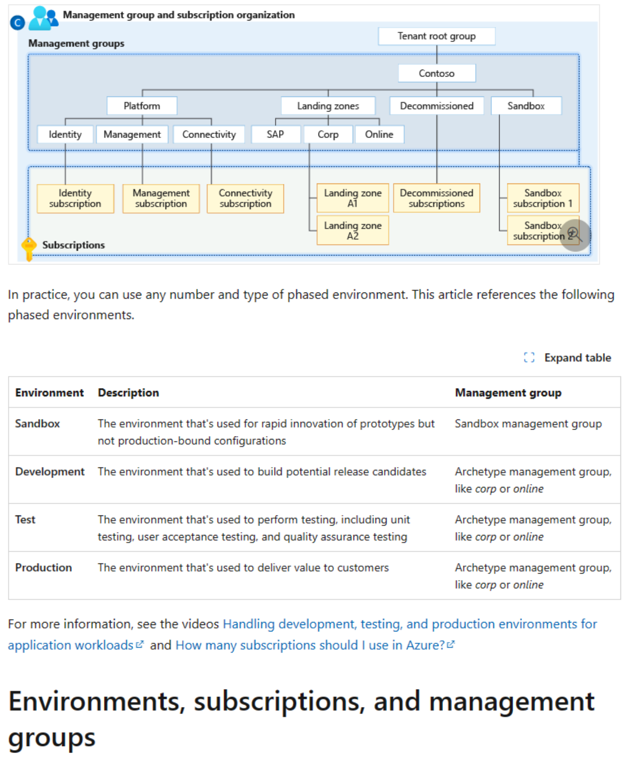
It's important to provide sandbox resources for *semi-governed* resources, so application teams can experiment with technologies and capabilities.

When application owners use subscription vending or other subscription creation processes, they must know how to request subscriptions for multiple development environments.

This article describes the Azure landing zone, including the management groups, policies, and shared platform architecture, and the workload or application landing zone.

ⓘ Note

The guidance in this article is only for workload or application landing zones. For testing and environment segregation for the Azure landing zone platform itself, see Testing approach for Azure

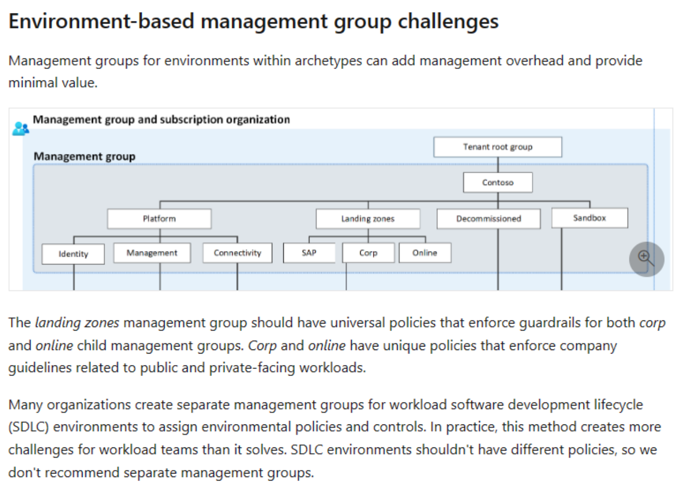


In practice, you can use any number and type of phased environment. This article references the following phased environments.

| Environment | Description | Management group |
|---|---|---|
| **Sandbox** | The environment that's used for rapid innovation of prototypes but not production-bound configurations | Sandbox management group |
| **Development** | The environment that's used to build potential release candidates | Archetype management group, like *corp* or *online* |
| **Test** | The environment that's used to perform testing, including unit testing, user acceptance testing, and quality assurance testing | Archetype management group, like *corp* or *online* |
| **Production** | The environment that's used to deliver value to customers | Archetype management group, like *corp* or *online* |

For more information, see the videos Handling development, testing, and production environments for application workloads and How many subscriptions should I use in Azure?

## Environments, subscriptions, and management groups



### Environment-based management group challenges

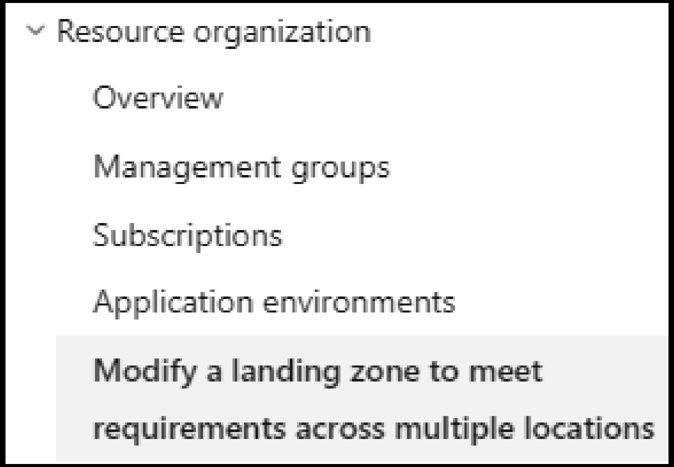
Management groups for environments within archetypes can add management overhead and provide minimal value.

The *landing zones* management group should have universal policies that enforce guardrails for both *corp* and *online* child management groups. *Corp* and *online* have unique policies that enforce company guidelines related to public and private-facing workloads.

Many organizations create separate management groups for workload software development lifecycle (SDLC) environments to assign environmental policies and controls. In practice, this method creates more challenges for workload teams than it solves. SDLC environments shouldn't have different policies, so we don't recommend separate management groups.

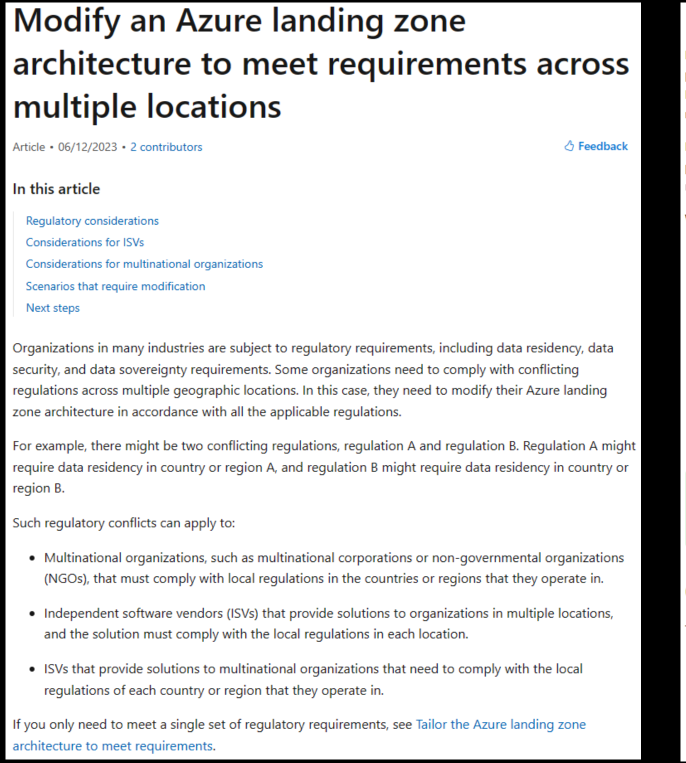
# New CAF Doc

# Modify an Azure landing zone architecture to meet requirements across multiple locations



Resource organization

- Overview
- Management groups
- Subscriptions
- Application environments
- Modify a landing zone to meet requirements across multiple locations



## Modify an Azure landing zone architecture to meet requirements across multiple locations

Article • 06/12/2023 • 2 contributors

### In this article

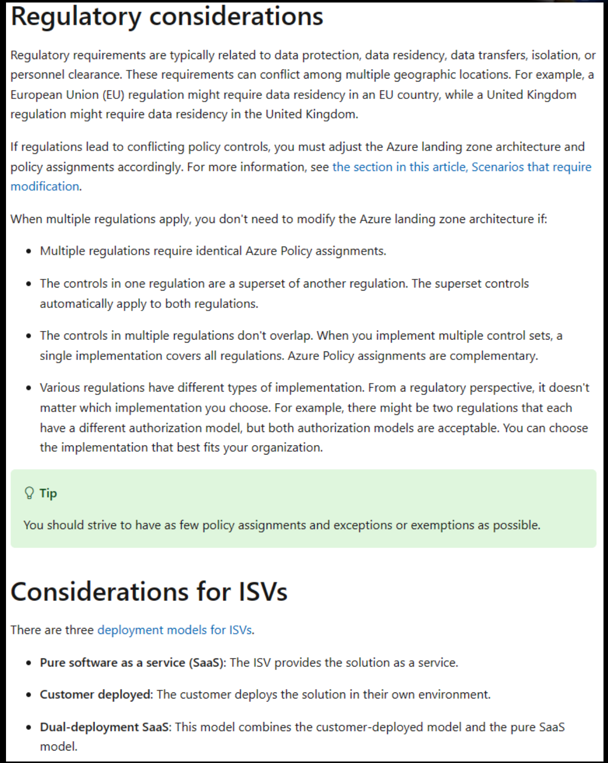
Organizations in many industries are subject to regulatory requirements, including data residency, data security, and data sovereignty requirements. Some organizations need to comply with conflicting regulations across multiple geographic locations. In this case, they need to modify their Azure landing zone architecture in accordance with all the applicable regulations.

For example, there might be two conflicting regulations, regulation A and regulation B. Regulation A might require data residency in country or region A, and regulation B might require data residency in country or region B.

Such regulatory conflicts can apply to:

- Multinational organizations, such as multinational corporations or non-governmental organizations (NGOs), that must comply with local regulations in the countries or regions that they operate in.
- Independent software vendors (ISVs) that provide solutions to organizations in multiple locations, and the solution must comply with the local regulations in each location.
- ISVs that provide solutions to multinational organizations that need to comply with the local regulations of each country or region that they operate in.

If you only need to meet a single set of regulatory requirements, see Tailor the Azure landing zone architecture to meet requirements.



## Regulatory considerations

Regulatory requirements are typically related to data protection, data residency, data transfers, isolation, or personnel clearance. These requirements can conflict among multiple geographic locations. For example, a European Union (EU) regulation might require data residency in an EU country, while a United Kingdom regulation might require data residency in the United Kingdom.

If regulations lead to conflicting policy controls, you must adjust the Azure landing zone architecture and policy assignments accordingly. For more information, see the section in this article, Scenarios that require modification.

When multiple regulations apply, you don't need to modify the Azure landing zone architecture if:

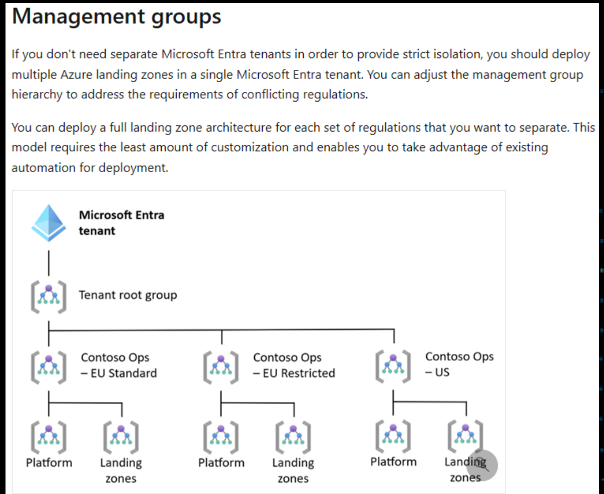
- Multiple regulations require identical Azure Policy assignments.
- The controls in one regulation are a superset of another regulation. The superset controls automatically apply to both regulations.
- The controls in multiple regulations don't overlap. When you implement multiple control sets, a single implementation covers all regulations. Azure Policy assignments are complementary.
- Various regulations have different types of implementation. From a regulatory perspective, it doesn't matter which implementation you choose. For example, there might be two regulations that each have a different authorization model, but both authorization models are acceptable. You can choose the implementation that best fits your organization.

> Tip
>
> You should strive to have as few policy assignments and exceptions or exemptions as possible.

## Considerations for ISVs

There are three deployment models for ISVs.

- **Pure software as a service (SaaS)**: The ISV provides the solution as a service.
- **Customer deployed**: The customer deploys the solution in their own environment.
- **Dual-deployment SaaS**: This model combines the customer-deployed model and the pure SaaS model.

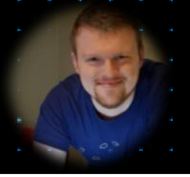


## Management groups

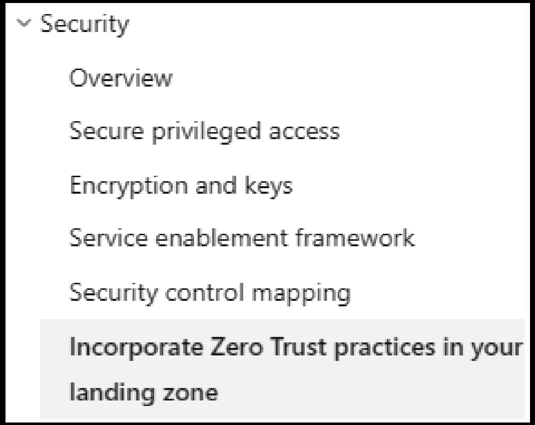
If you don't need separate Microsoft Entra tenants in order to provide strict isolation, you should deploy multiple Azure landing zones in a single Microsoft Entra tenant. You can adjust the management group hierarchy to address the requirements of conflicting regulations.

You can deploy a full landing zone architecture for each set of regulations that you want to separate. This model requires the least amount of customization and enables you to take advantage of existing automation for deployment.

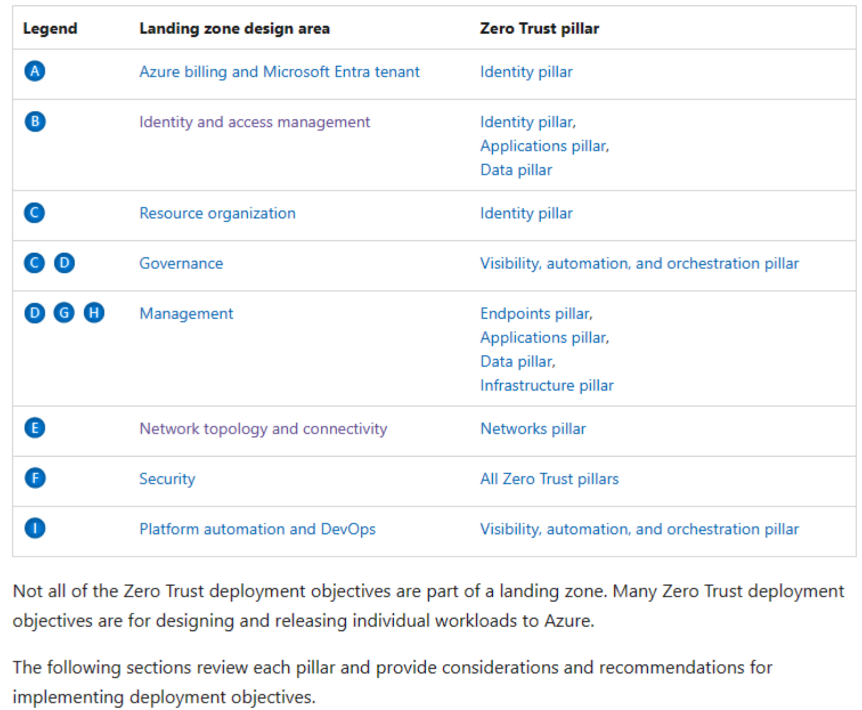
# New CAF Doc



# Incorporate Zero Trust practices in your landing zone



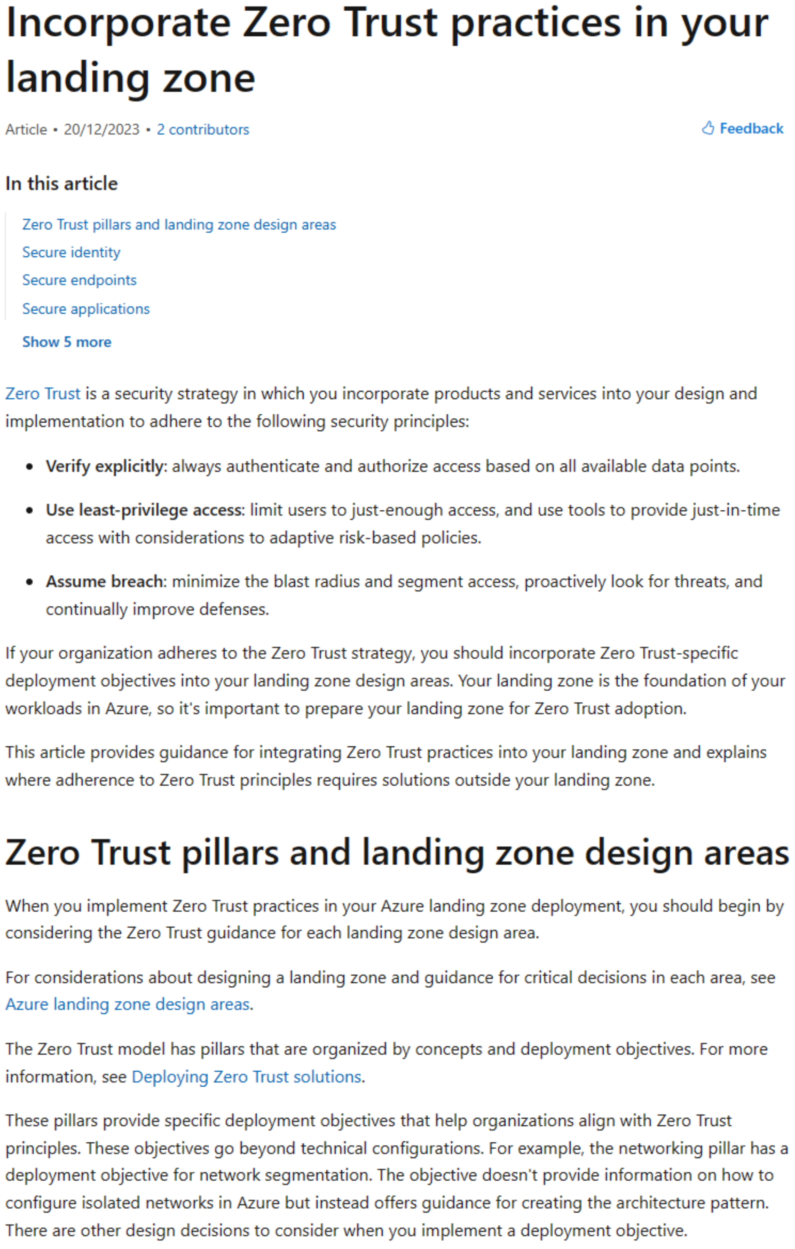
- Security
  - Overview
  - Secure privileged access
  - Encryption and keys
  - Service enablement framework
  - Security control mapping
  - Incorporate Zero Trust practices in your landing zone



| Legend | Landing zone design area | Zero Trust pillar |
|---|---|---|
| A | Azure billing and Microsoft Entra tenant | Identity pillar |
| B | Identity and access management | Identity pillar,<br>Applications pillar,<br>Data pillar |
| C | Resource organization | Identity pillar |
| C D | Governance | Visibility, automation, and orchestration pillar |
| D G H | Management | Endpoints pillar,<br>Applications pillar,<br>Data pillar,<br>Infrastructure pillar |
| E | Network topology and connectivity | Networks pillar |
| F | Security | All Zero Trust pillars |
| I | Platform automation and DevOps | Visibility, automation, and orchestration pillar |

Not all of the Zero Trust deployment objectives are part of a landing zone. Many Zero Trust deployment objectives are for designing and releasing individual workloads to Azure.

The following sections review each pillar and provide considerations and recommendations for implementing deployment objectives.



## Incorporate Zero Trust practices in your landing zone

Article • 20/12/2023 • 2 contributors

Feedback

**In this article**

- Zero Trust pillars and landing zone design areas
- Secure identity
- Secure endpoints
- Secure applications

Show 5 more

Zero Trust is a security strategy in which you incorporate products and services into your design and implementation to adhere to the following security principles:

- **Verify explicitly**: always authenticate and authorize access based on all available data points.
- **Use least-privilege access**: limit users to just-enough access, and use tools to provide just-in-time access with considerations to adaptive risk-based policies.
- **Assume breach**: minimize the blast radius and segment access, proactively look for threats, and continually improve defenses.

If your organization adheres to the Zero Trust strategy, you should incorporate Zero Trust-specific deployment objectives into your landing zone design areas. Your landing zone is the foundation of your workloads in Azure, so it's important to prepare your landing zone for Zero Trust adoption.

This article provides guidance for integrating Zero Trust practices into your landing zone and explains where adherence to Zero Trust principles requires solutions outside your landing zone.

## Zero Trust pillars and landing zone design areas

When you implement Zero Trust practices in your Azure landing zone deployment, you should begin by considering the Zero Trust guidance for each landing zone design area.

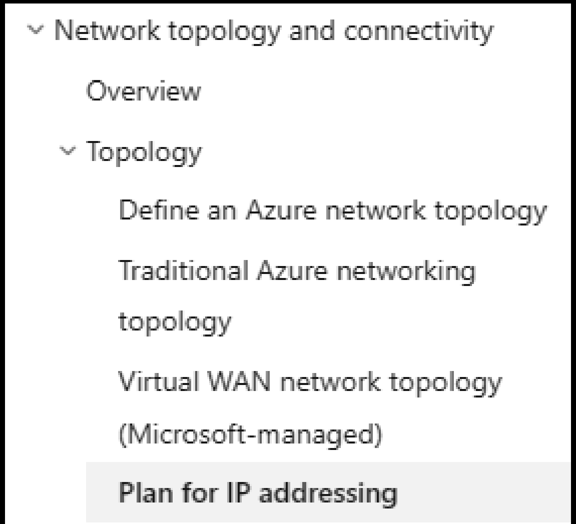
For considerations about designing a landing zone and guidance for critical decisions in each area, see Azure landing zone design areas.

The Zero Trust model has pillars that are organized by concepts and deployment objectives. For more information, see Deploying Zero Trust solutions.

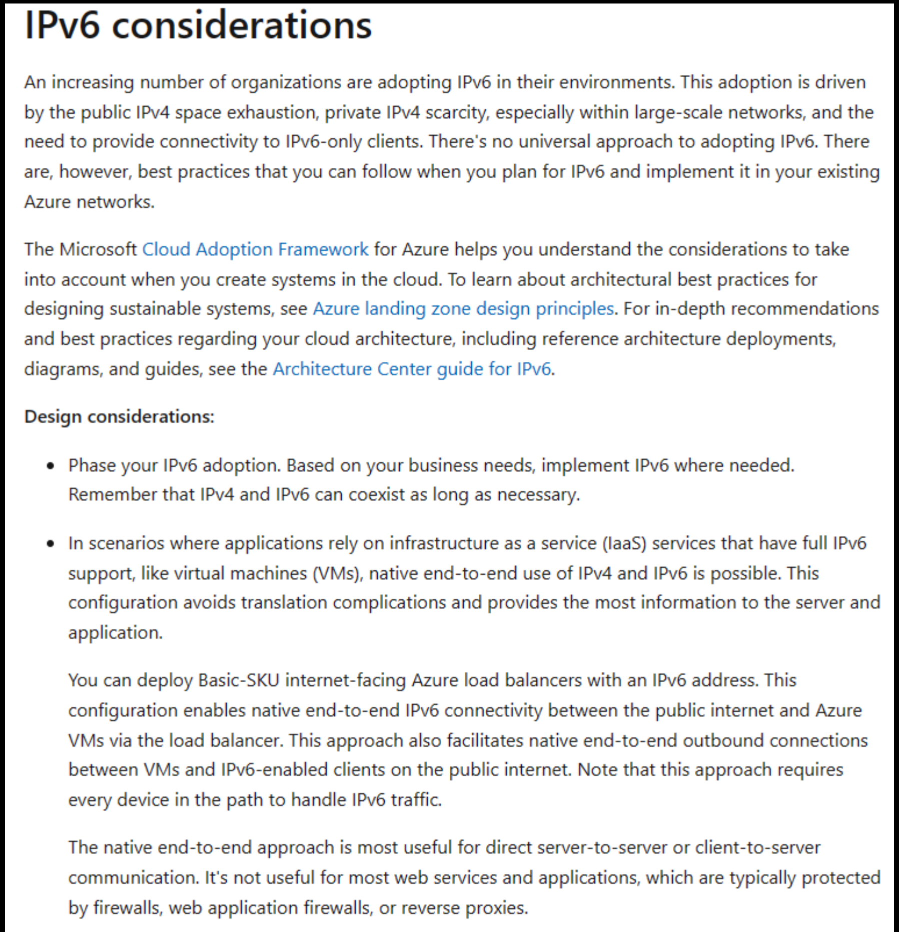
These pillars provide specific deployment objectives that help organizations align with Zero Trust principles. These objectives go beyond technical configurations. For example, the networking pillar has a deployment objective for network segmentation. The objective doesn't provide information on how to configure isolated networks in Azure but instead offers guidance for creating the architecture pattern. There are other design decisions to consider when you implement a deployment objective.

# Update of CAF Doc

## Plan for IP Addressing



- Network topology and connectivity
  - Overview
  - Topology
    - Define an Azure network topology
    - Traditional Azure networking topology
    - Virtual WAN network topology (Microsoft-managed)
    - **Plan for IP addressing**



### IPv6 considerations

An increasing number of organizations are adopting IPv6 in their environments. This adoption is driven by the public IPv4 space exhaustion, private IPv4 scarcity, especially within large-scale networks, and the need to provide connectivity to IPv6-only clients. There's no universal approach to adopting IPv6. There are, however, best practices that you can follow when you plan for IPv6 and implement it in your existing Azure networks.

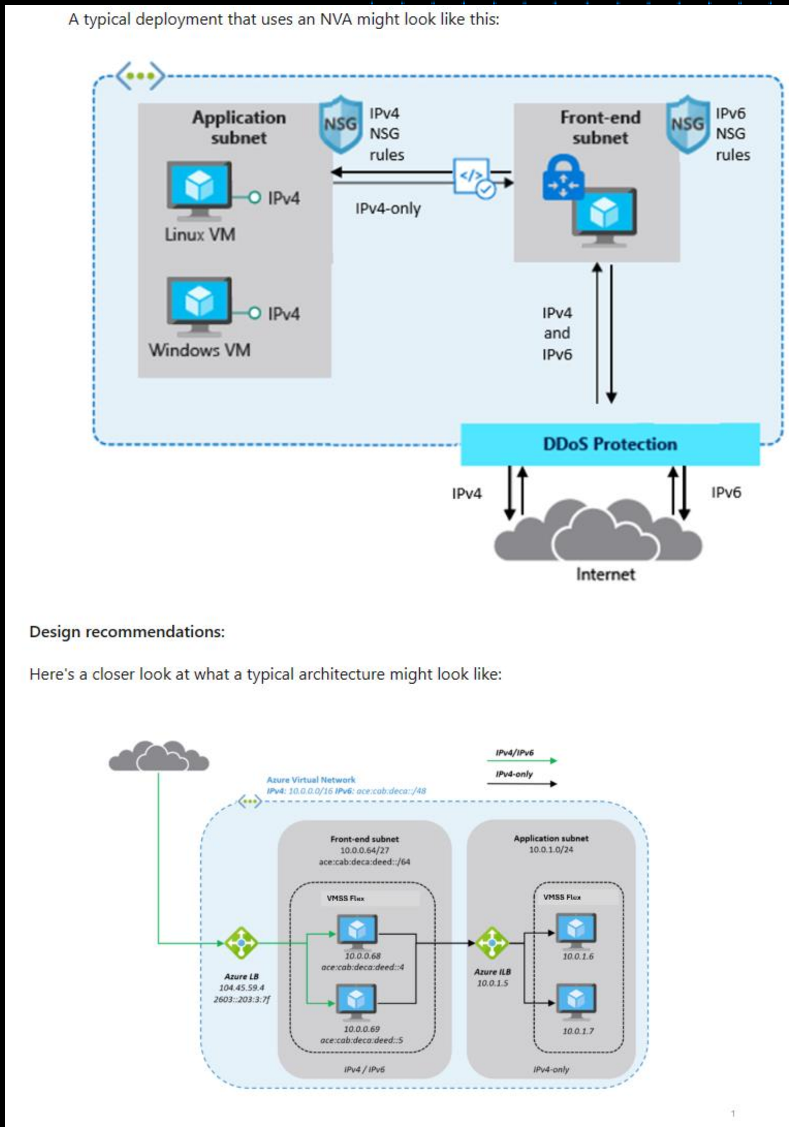
The Microsoft Cloud Adoption Framework for Azure helps you understand the considerations to take into account when you create systems in the cloud. To learn about architectural best practices for designing sustainable systems, see Azure landing zone design principles. For in-depth recommendations and best practices regarding your cloud architecture, including reference architecture deployments, diagrams, and guides, see the Architecture Center guide for IPv6.

**Design considerations:**

- Phase your IPv6 adoption. Based on your business needs, implement IPv6 where needed. Remember that IPv4 and IPv6 can coexist as long as necessary.
- In scenarios where applications rely on infrastructure as a service (IaaS) services that have full IPv6 support, like virtual machines (VMs), native end-to-end use of IPv4 and IPv6 is possible. This configuration avoids translation complications and provides the most information to the server and application.

  You can deploy Basic-SKU internet-facing Azure load balancers with an IPv6 address. This configuration enables native end-to-end IPv6 connectivity between the public internet and Azure VMs via the load balancer. This approach also facilitates native end-to-end outbound connections between VMs and IPv6-enabled clients on the public internet. Note that this approach requires every device in the path to handle IPv6 traffic.

  The native end-to-end approach is most useful for direct server-to-server or client-to-server communication. It's not useful for most web services and applications, which are typically protected by firewalls, web application firewalls, or reverse proxies.



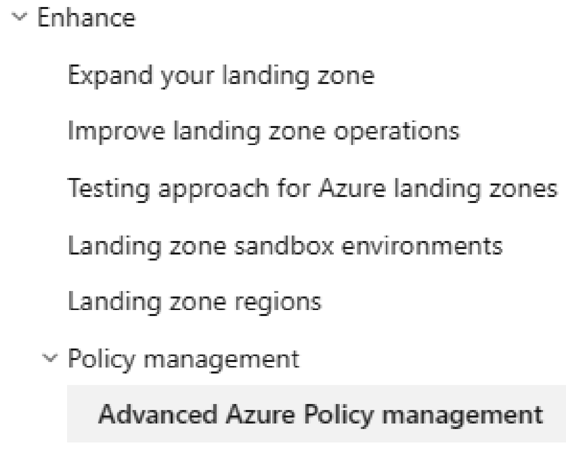
A typical deployment that uses an NVA might look like this:

**Design recommendations:**

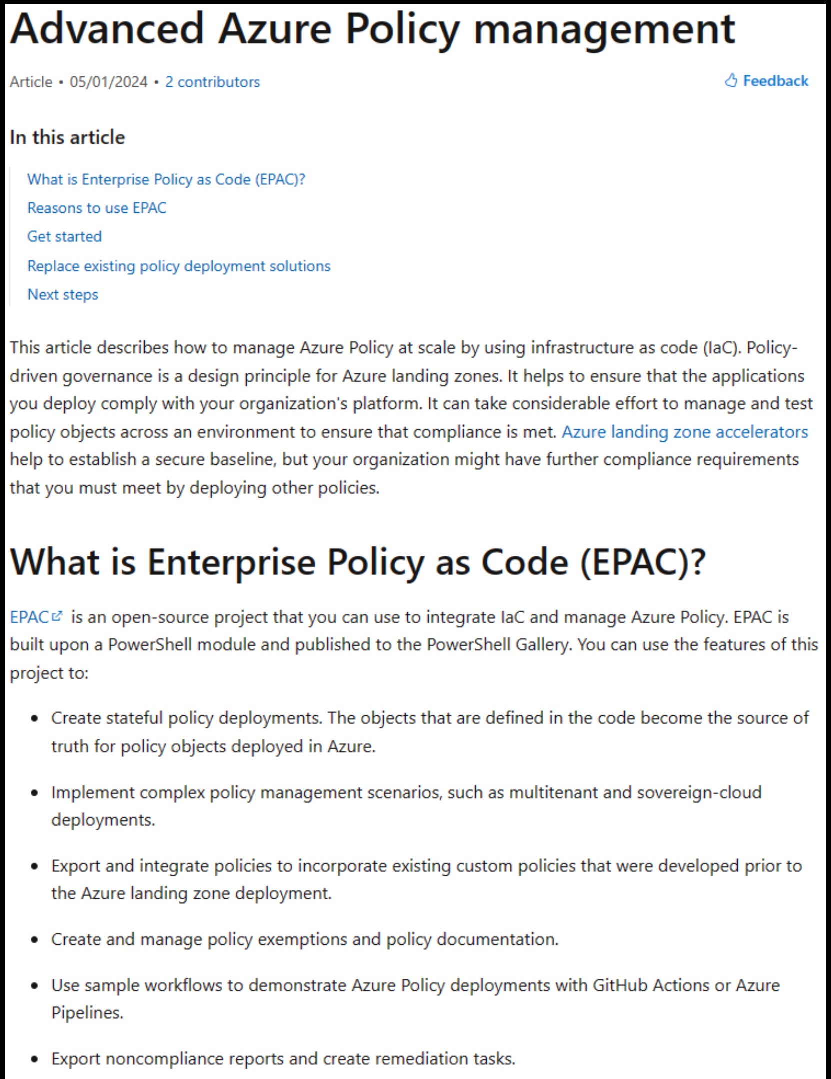
Here's a closer look at what a typical architecture might look like:

# New CAF Doc

# Advanced Azure Policy management



- Enhance
  - Expand your landing zone
  - Improve landing zone operations
  - Testing approach for Azure landing zones
  - Landing zone sandbox environments
  - Landing zone regions
  - Policy management
    - Advanced Azure Policy management



## Advanced Azure Policy management

Article • 05/01/2024 • 2 contributors

Feedback

**In this article**

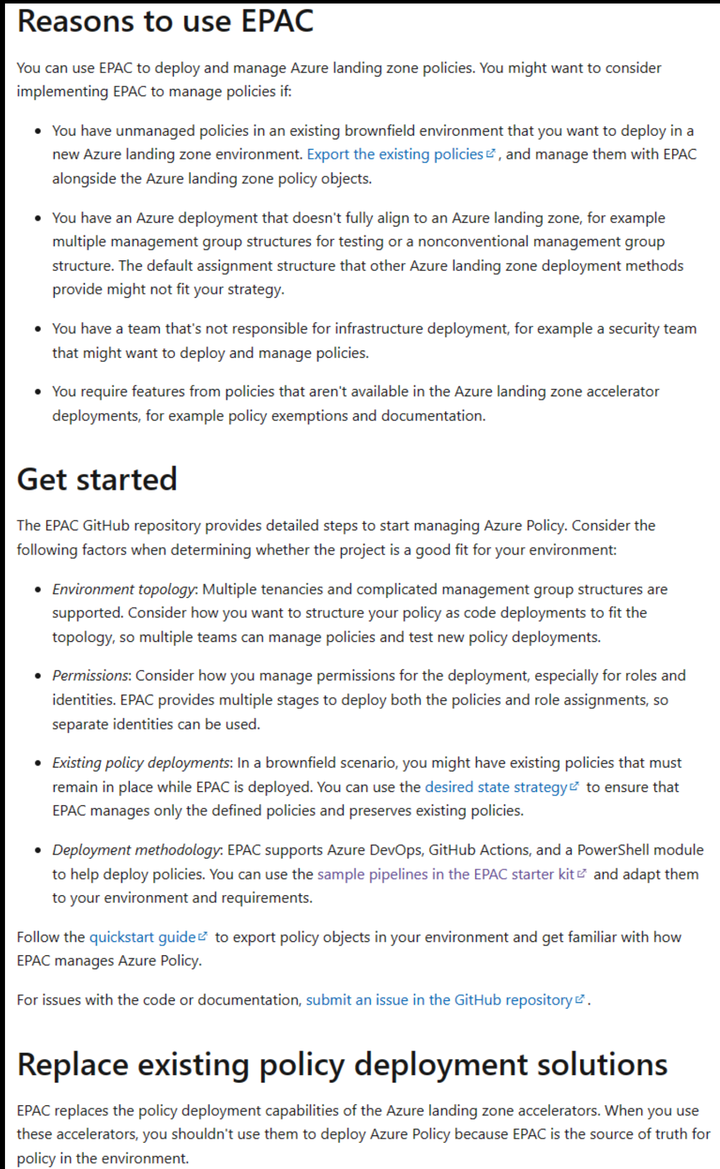
- What is Enterprise Policy as Code (EPAC)?
- Reasons to use EPAC
- Get started
- Replace existing policy deployment solutions
- Next steps

This article describes how to manage Azure Policy at scale by using infrastructure as code (IaC). Policy-driven governance is a design principle for Azure landing zones. It helps to ensure that the applications you deploy comply with your organization's platform. It can take considerable effort to manage and test policy objects across an environment to ensure that compliance is met. Azure landing zone accelerators help to establish a secure baseline, but your organization might have further compliance requirements that you must meet by deploying other policies.

## What is Enterprise Policy as Code (EPAC)?

EPAC is an open-source project that you can use to integrate IaC and manage Azure Policy. EPAC is built upon a PowerShell module and published to the PowerShell Gallery. You can use the features of this project to:

- Create stateful policy deployments. The objects that are defined in the code become the source of truth for policy objects deployed in Azure.
- Implement complex policy management scenarios, such as multitenant and sovereign-cloud deployments.
- Export and integrate policies to incorporate existing custom policies that were developed prior to the Azure landing zone deployment.
- Create and manage policy exemptions and policy documentation.
- Use sample workflows to demonstrate Azure Policy deployments with GitHub Actions or Azure Pipelines.
- Export noncompliance reports and create remediation tasks.



## Reasons to use EPAC

You can use EPAC to deploy and manage Azure landing zone policies. You might want to consider implementing EPAC to manage policies if:

- You have unmanaged policies in an existing brownfield environment that you want to deploy in a new Azure landing zone environment. Export the existing policies, and manage them with EPAC alongside the Azure landing zone policy objects.
- You have an Azure deployment that doesn't fully align to an Azure landing zone, for example multiple management group structures for testing or a nonconventional management group structure. The default assignment structure that other Azure landing zone deployment methods provide might not fit your strategy.
- You have a team that's not responsible for infrastructure deployment, for example a security team that might want to deploy and manage policies.
- You require features from policies that aren't available in the Azure landing zone accelerator deployments, for example policy exemptions and documentation.

## Get started

The EPAC GitHub repository provides detailed steps to start managing Azure Policy. Consider the following factors when determining whether the project is a good fit for your environment:

- *Environment topology*: Multiple tenancies and complicated management group structures are supported. Consider how you want to structure your policy as code deployments to fit the topology, so multiple teams can manage policies and test new policy deployments.
- *Permissions*: Consider how you manage permissions for the deployment, especially for roles and identities. EPAC provides multiple stages to deploy both the policies and role assignments, so separate identities can be used.
- *Existing policy deployments*: In a brownfield scenario, you might have existing policies that must remain in place while EPAC is deployed. You can use the desired state strategy to ensure that EPAC manages only the defined policies and preserves existing policies.
- *Deployment methodology*: EPAC supports Azure DevOps, GitHub Actions, and a PowerShell module to help deploy policies. You can use the sample pipelines in the EPAC starter kit and adapt them to your environment and requirements.

Follow the quickstart guide to export policy objects in your environment and get familiar with how EPAC manages Azure Policy.

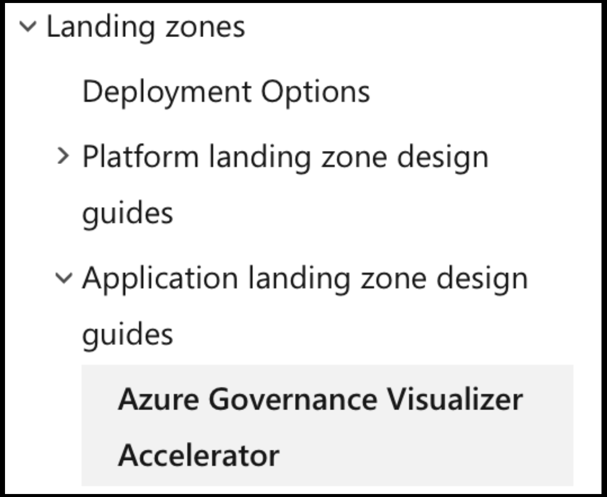
For issues with the code or documentation, submit an issue in the GitHub repository.

## Replace existing policy deployment solutions

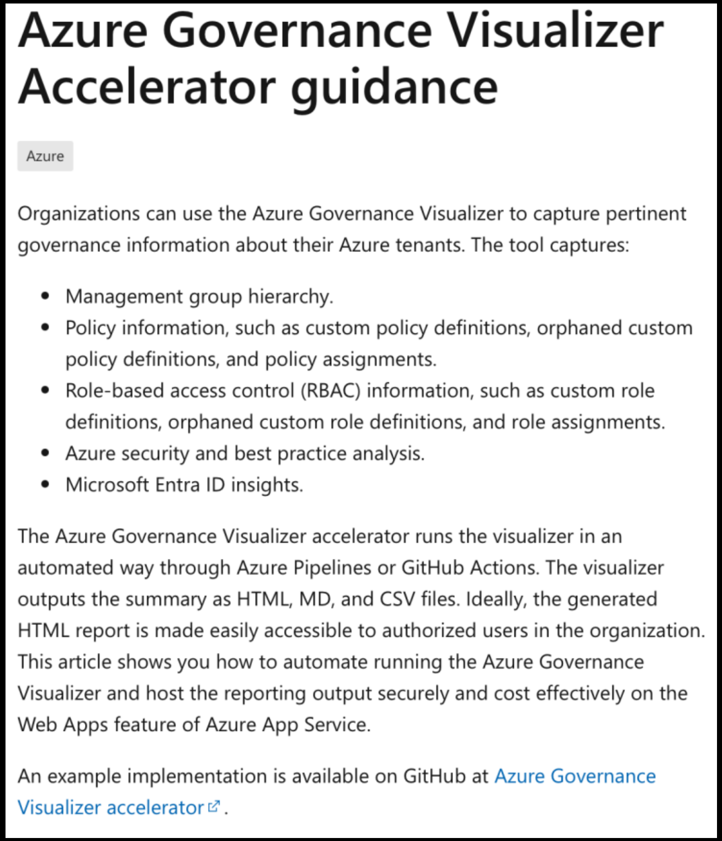
EPAC replaces the policy deployment capabilities of the Azure landing zone accelerators. When you use these accelerators, you shouldn't use them to deploy Azure Policy because EPAC is the source of truth for policy in the environment.

# New AAC Doc

# Azure Governance Visualizer Accelerator guidance



- Landing zones
  - Deployment Options
  - Platform landing zone design guides
  - Application landing zone design guides
    - **Azure Governance Visualizer Accelerator**



## Azure Governance Visualizer Accelerator guidance

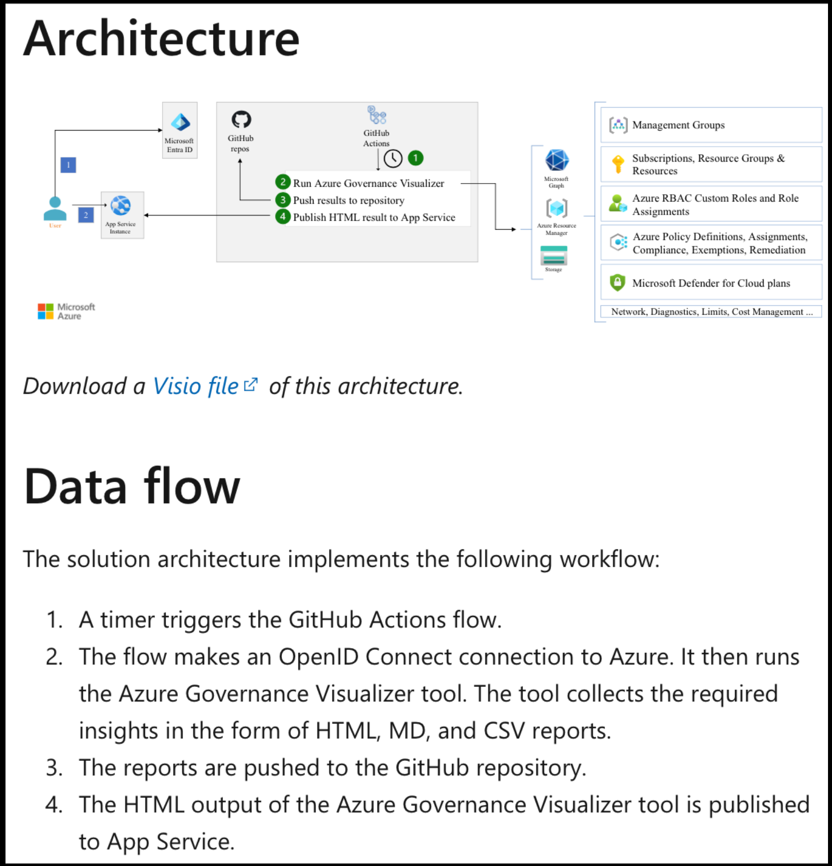
Azure

Organizations can use the Azure Governance Visualizer to capture pertinent governance information about their Azure tenants. The tool captures:

- Management group hierarchy.
- Policy information, such as custom policy definitions, orphaned custom policy definitions, and policy assignments.
- Role-based access control (RBAC) information, such as custom role definitions, orphaned custom role definitions, and role assignments.
- Azure security and best practice analysis.
- Microsoft Entra ID insights.

The Azure Governance Visualizer accelerator runs the visualizer in an automated way through Azure Pipelines or GitHub Actions. The visualizer outputs the summary as HTML, MD, and CSV files. Ideally, the generated HTML report is made easily accessible to authorized users in the organization. This article shows you how to automate running the Azure Governance Visualizer and host the reporting output securely and cost effectively on the Web Apps feature of Azure App Service.

An example implementation is available on GitHub at Azure Governance Visualizer accelerator.



## Architecture

Microsoft Entra ID
GitHub repos
GitHub Actions
1
2 Run Azure Governance Visualizer
3 Push results to repository
4 Publish HTML result to App Service
User
2
App Service Instance
Microsoft Graph
Azure Resource Manager
Storage
Management Groups
Subscriptions, Resource Groups & Resources
Azure RBAC Custom Roles and Role Assignments
Azure Policy Definitions, Assignments, Compliance, Exemptions, Remediation
Microsoft Defender for Cloud plans
Network, Diagnostics, Limits, Cost Management ...
Microsoft Azure

*Download a Visio file of this architecture.*

## Data flow

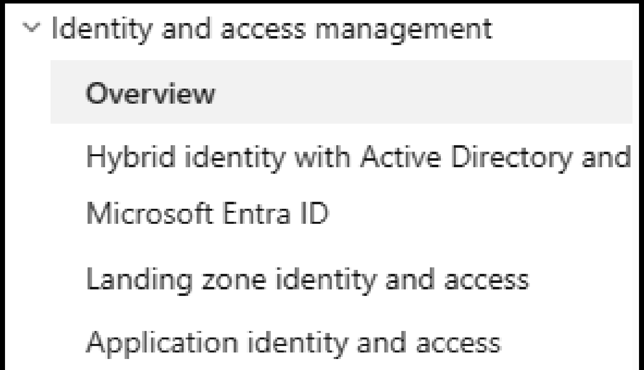
The solution architecture implements the following workflow:

1. A timer triggers the GitHub Actions flow.
2. The flow makes an OpenID Connect connection to Azure. It then runs the Azure Governance Visualizer tool. The tool collects the required insights in the form of HTML, MD, and CSV reports.
3. The reports are pushed to the GitHub repository.
4. The HTML output of the Azure Governance Visualizer tool is published to App Service.

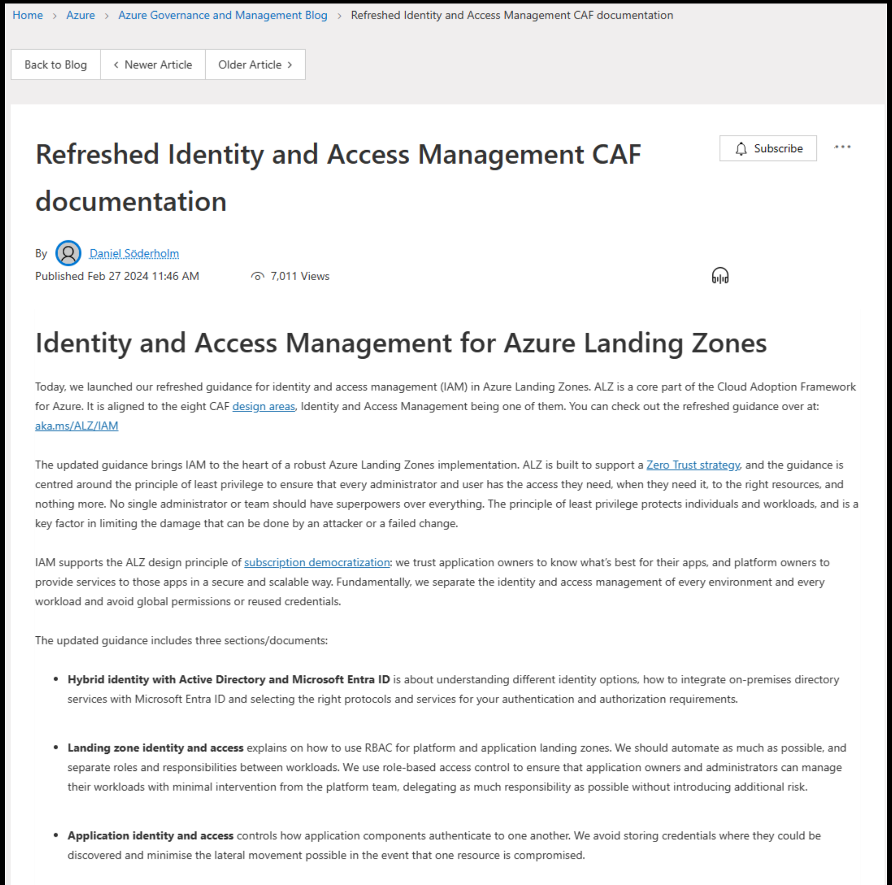
# IAM Design Area Refresh & Update

## Refreshed Identity and Access Management CAF documentation - Blog

aka.ms/alz/iam



Identity and access management
Overview
Hybrid identity with Active Directory and Microsoft Entra ID
Landing zone identity and access
Application identity and access



Home › Azure › Azure Governance and Management Blog › Refreshed Identity and Access Management CAF documentation
Back to Blog
‹ Newer Article
Older Article ›
Subscribe
...

### Refreshed Identity and Access Management CAF documentation

By Daniel Söderholm
Published Feb 27 2024 11:46 AM
7,011 Views

### Identity and Access Management for Azure Landing Zones

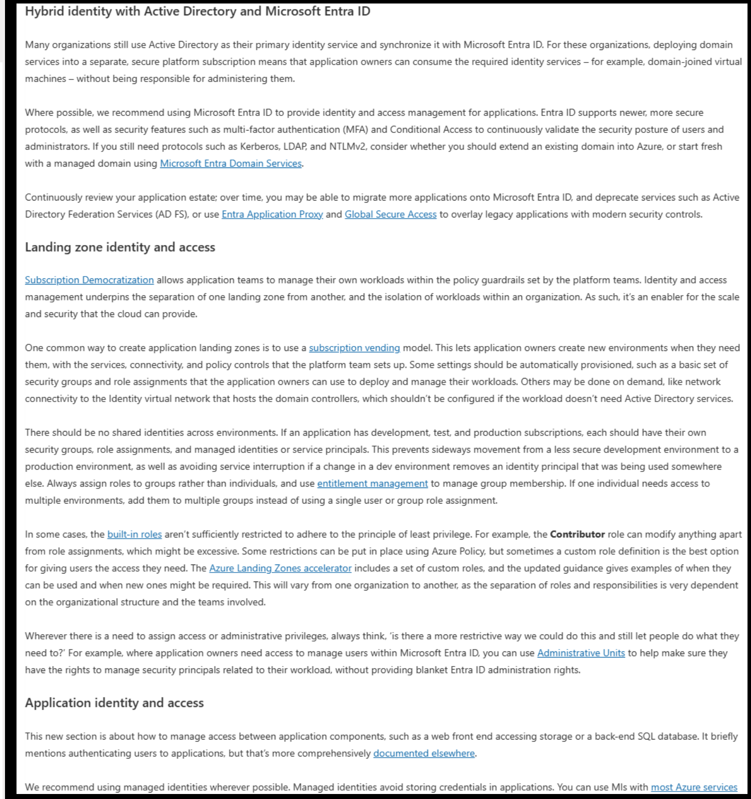
Today, we launched our refreshed guidance for identity and access management (IAM) in Azure Landing Zones. ALZ is a core part of the Cloud Adoption Framework for Azure. It is aligned to the eight CAF design areas, Identity and Access Management being one of them. You can check out the refreshed guidance over at: aka.ms/ALZ/IAM

The updated guidance brings IAM to the heart of a robust Azure Landing Zones implementation. ALZ is built to support a Zero Trust strategy, and the guidance is centred around the principle of least privilege to ensure that every administrator and user has the access they need, when they need it, to the right resources, and nothing more. No single administrator or team should have superpowers over everything. The principle of least privilege protects individuals and workloads, and is a key factor in limiting the damage that can be done by an attacker or a failed change.

IAM supports the ALZ design principle of subscription democratization: we trust application owners to know what's best for their apps, and platform owners to provide services to those apps in a secure and scalable way. Fundamentally, we separate the identity and access management of every environment and every workload and avoid global permissions or reused credentials.

The updated guidance includes three sections/documents:

- **Hybrid identity with Active Directory and Microsoft Entra ID** is about understanding different identity options, how to integrate on-premises directory services with Microsoft Entra ID and selecting the right protocols and services for your authentication and authorization requirements.
- **Landing zone identity and access** explains on how to use RBAC for platform and application landing zones. We should automate as much as possible, and separate roles and responsibilities between workloads. We use role-based access control to ensure that application owners and administrators can manage their workloads with minimal intervention from the platform team, delegating as much responsibility as possible without introducing additional risk.
- **Application identity and access** controls how application components authenticate to one another. We avoid storing credentials where they could be discovered and minimise the lateral movement possible in the event that one resource is compromised.



### Hybrid identity with Active Directory and Microsoft Entra ID

Many organizations still use Active Directory as their primary identity service and synchronize it with Microsoft Entra ID. For these organizations, deploying domain services into a separate, secure platform subscription means that application owners can consume the required identity services – for example, domain-joined virtual machines – without being responsible for administering them.

Where possible, we recommend using Microsoft Entra ID to provide identity and access management for applications. Entra ID supports newer, more secure protocols, as well as security features such as multi-factor authentication (MFA) and Conditional Access to continuously validate the security posture of users and administrators. If you still need protocols such as Kerberos, LDAP, and NTLMv2, consider whether you should extend an existing domain into Azure, or start fresh with a managed domain using Microsoft Entra Domain Services.

Continuously review your application estate; over time, you may be able to migrate more applications onto Microsoft Entra ID, and deprecate services such as Active Directory Federation Services (AD FS), or use Entra Application Proxy and Global Secure Access to overlay legacy applications with modern security controls.

### Landing zone identity and access

Subscription Democratization allows application teams to manage their own workloads within the policy guardrails set by the platform teams. Identity and access management underpins the separation of one landing zone from another, and the isolation of workloads within an organization. As such, it's an enabler for the scale and security that the cloud can provide.

One common way to create application landing zones is to use a subscription vending model. This lets application owners create new environments when they need them, with the services, connectivity, and policy controls that the platform team sets up. Some settings should be automatically provisioned, such as a basic set of security groups and role assignments that the application owners can use to deploy and manage their workloads. Others may be done on demand, like network connectivity to the Identity virtual network that hosts the domain controllers, which shouldn't be configured if the workload doesn't need Active Directory services.

There should be no shared identities across environments. If an application has development, test, and production subscriptions, each should have their own security groups, role assignments, and managed identities or service principals. This prevents sideways movement from a less secure development environment to a production environment, as well as avoiding service interruption if a change in a dev environment removes an identity principal that was being used somewhere else. Always assign roles to groups rather than individuals, and use entitlement management to manage group membership. If one individual needs access to multiple environments, add them to multiple groups instead of using a single user or group role assignment.

In some cases, the built-in roles aren't sufficiently restricted to adhere to the principle of least privilege. For example, the **Contributor** role can modify anything apart from role assignments, which might be excessive. Some restrictions can be put in place using Azure Policy, but sometimes a custom role definition is the best option for giving users the access they need. The Azure Landing Zones accelerator includes a set of custom roles, and the updated guidance gives examples of when they can be used and when new ones might be required. This will vary from one organization to another, as the separation of roles and responsibilities is very dependent on the organizational structure and the teams involved.

Wherever there is a need to assign access or administrative privileges, always think, 'is there a more restrictive way we could do this and still let people do what they need to?' For example, where application owners need access to manage users within Microsoft Entra ID, you can use Administrative Units to help make sure they have the rights to manage security principals related to their workload, without providing blanket Entra ID administration rights.

### Application identity and access

This new section is about how to manage access between application components, such as a web front end accessing storage or a back-end SQL database. It briefly mentions authenticating users to applications, but that's more comprehensively documented elsewhere.

We recommend using managed identities wherever possible. Managed identities avoid storing credentials in applications. You can use MIs with most Azure services

# ALZ Identity & Access Management

| | |
|---|---|
| Overview | • Identity is the enabler for subscription democratization<br>• Think about where security boundaries are created, and how to avoid crossing them |
| Hybrid Identity, Entra ID, and Active Directory | • Do we need AD DS, or can we use Entra ID/Entra DS?<br>• Don’t enable access to the Identity VNet unless required |
| Landing zone identity and access | • Create groups, role assignments, and security principals during subscription vending<br>• Use custom roles where built-ins are too permissive |
| Application access | • Use separate identity principals for each application environment<br>• Phase out credentials and SPNs, and use managed/workload identities |

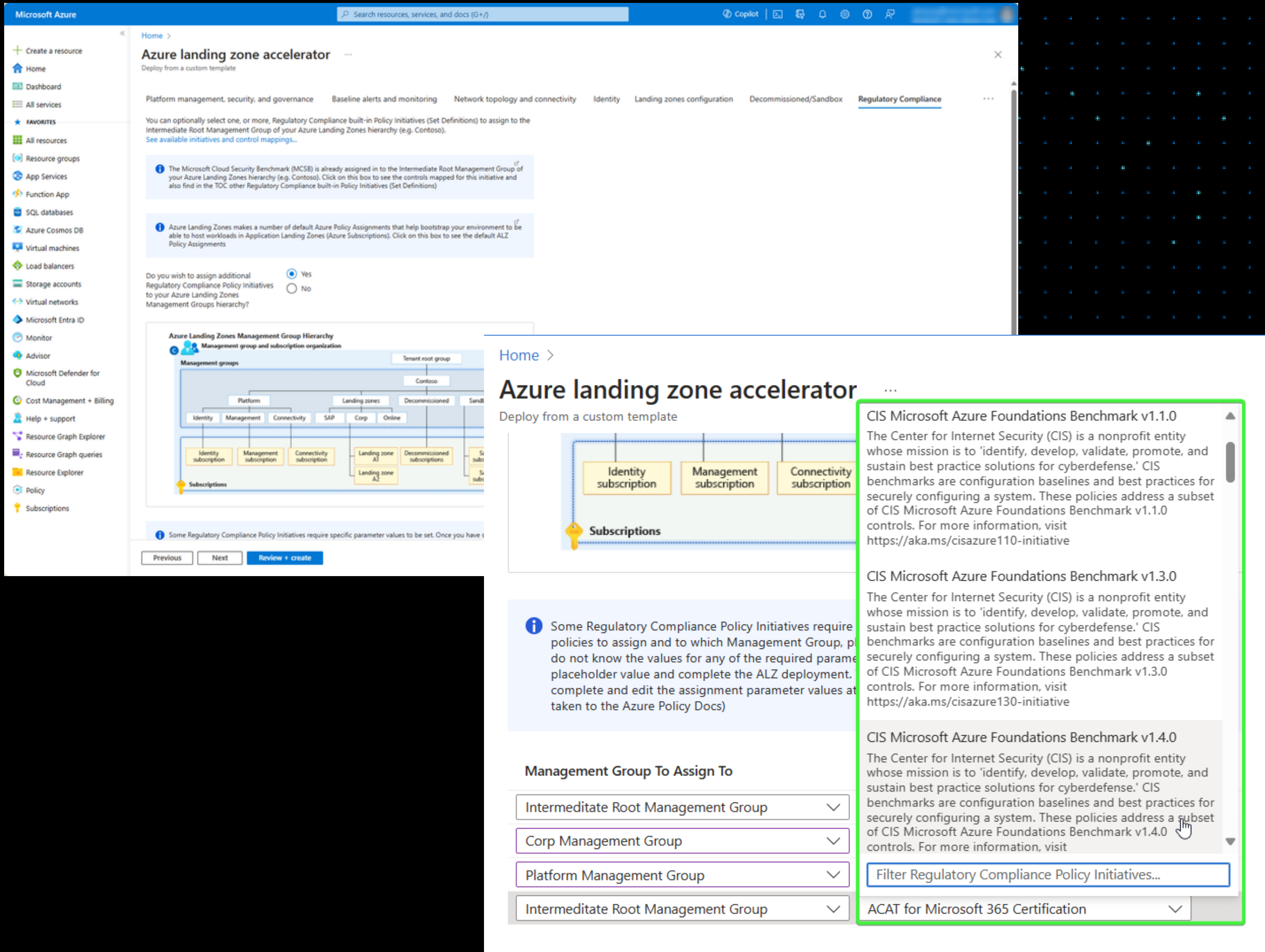
Subscription Democratization

Zero Trust

# New ALZ Portal Accelerator Feature

## aka.ms/alz/portal

New feature: easily assign regulatory compliance policies to your Azure Landing Zone - Microsoft Community Hub



Azure landing zone accelerator

Deploy from a custom template

You can optionally select one, or more, Regulatory Compliance built-in Policy Initiatives (Set Definitions) to assign to the Intermediate Root Management Group of your Azure Landing Zones hierarchy (e.g. Contoso).
See available initiatives and control mappings...

The Microsoft Cloud Security Benchmark (MCSB) is already assigned in to the Intermediate Root Management Group of your Azure Landing Zones hierarchy (e.g. Contoso). Click on this box to see the controls mapped for this initiative and also find in the TOC other Regulatory Compliance built-in Policy Initiatives (Set Definitions)

Azure Landing Zones makes a number of default Azure Policy Assignments that help bootstrap your environment to be able to host workloads in Application Landing Zones (Azure Subscriptions). Click on this box to see the default ALZ Policy Assignments

Do you wish to assign additional Regulatory Compliance Policy Initiatives to your Azure Landing Zones Management Groups hierarchy? ● Yes ○ No

Some Regulatory Compliance Policy Initiatives require specific parameter values to be set. Once you have s

Some Regulatory Compliance Policy Initiatives require policies to assign and to which Management Group, pl do not know the values for any of the required parame placeholder value and complete the ALZ deployment. complete and edit the assignment parameter values at taken to the Azure Policy Docs)

Management Group To Assign To

| |
|---|
| Intermediate Root Management Group |
| Corp Management Group |
| Platform Management Group |
| Intermediate Root Management Group |

CIS Microsoft Azure Foundations Benchmark v1.1.0
The Center for Internet Security (CIS) is a nonprofit entity whose mission is to 'identify, develop, validate, promote, and sustain best practice solutions for cyberdefense.' CIS benchmarks are configuration baselines and best practices for securely configuring a system. These policies address a subset of CIS Microsoft Azure Foundations Benchmark v1.1.0 controls. For more information, visit https://aka.ms/cisazure110-initiative

CIS Microsoft Azure Foundations Benchmark v1.3.0
The Center for Internet Security (CIS) is a nonprofit entity whose mission is to 'identify, develop, validate, promote, and sustain best practice solutions for cyberdefense.' CIS benchmarks are configuration baselines and best practices for securely configuring a system. These policies address a subset of CIS Microsoft Azure Foundations Benchmark v1.3.0 controls. For more information, visit https://aka.ms/cisazure130-initiative

CIS Microsoft Azure Foundations Benchmark v1.4.0
The Center for Internet Security (CIS) is a nonprofit entity whose mission is to 'identify, develop, validate, promote, and sustain best practice solutions for cyberdefense.' CIS benchmarks are configuration baselines and best practices for securely configuring a system. These policies address a subset of CIS Microsoft Azure Foundations Benchmark v1.4.0 controls. For more information, visit

Filter Regulatory Compliance Policy Initiatives...

ACAT for Microsoft 365 Certification

# Policy Refresh Updates

# ALZ Policy News

aka.ms/alz/policies

- New Backup initiative and updates (in progress)
  - Immutability audit
  - Storage account backup
  - Vault private endpoints
  - Working with PG to create new policies (MUA)
  - *New Assignment*

- New Resilience initiative
  - Audit Zone Resiliency based for supporting resources
  - Audit resource and resource groups in same region
  - *New Assignments*

- Diagnostics Settings
  - See next slide

# Diagnostic Settings Updates

# Diagnostic Settings Updates

- New policies and initiatives coming soon
- ALZ to deprecate all Diagnostic Settings custom policies
- *New* Diagnostic Settings Initiatives (covering 137 Azure services)
- ALZ will default to Log Analytics as target
  - Option for Storage or Event Hubs

- NOTE: AllLogs or AuditLogs is not ubiquitous across services (eg. AzFW)
  - Recommendation for the short term is "AllLogs"
    - NOTE: Consider cost implications storing all logs
  - We are working hard to address this, it’s complex and takes time to remediate

# MMA Deprecation Update

# MMA Deprecation

- Portal reference implementation is now using AMA
- New resources:
  - User Assigned Managed Identity
  - Data Collection Rules
    - VM Insights
    - Change Tracking
    - MDFC Defender for SQL
- New policies:
  - Enable Change Tracking for Azure VMs
  - Enable Change Tracking for Arc-enabled Servers
  - Enable Change Tracking for VM scale sets
  - Enable MDFC Defender for SQL
  - Deploy User Assigned Managed Identity Enable VM Insights for Azure VMs
  - Enable VM Insights for Arc-enabled Servers
  - Enable VM Insights for VM scale sets
  - Enable update checking with Azure Update Manager
- Parity statements added to AMA [product docs]

# MMA Deprecation

- AMA for Bicep and Terraform is coming!
- Brownfield guidance on updating existing ALZ deployments to use AMA
- User Assigned Managed Identity (UAMI)
  - Scaling
  - Centralizing

- Policy updates
  - Adding additional flexibility to built-in Policies
  - Policy changes to enable centralizing UAMI

# AMBA Updates

# AMBA Updates

aka.ms/amba/patterns/alz

- The action group has been updated to include:
  - Email Azure Resource Manager Role
  - Azure Function
  - Event Hubs
  - Logic App
  - Webhook
- New Notification Assets initiative
- Updated Policy Remediation script.
- Documentation updates
- Decoupling Service Health initiative deployment from Action Group and Alert Processing rules
- Updated Existence Condition to detect and remediate configuration drift
  - **Static:** *EvaluationFrequency, WindowSize, Threshold, Severity, Operator, autoMitigate*
  - **Dynamic:** *alertSensitivity, numberOfEvaluationPeriods, minFailingPeriodsToAlert*

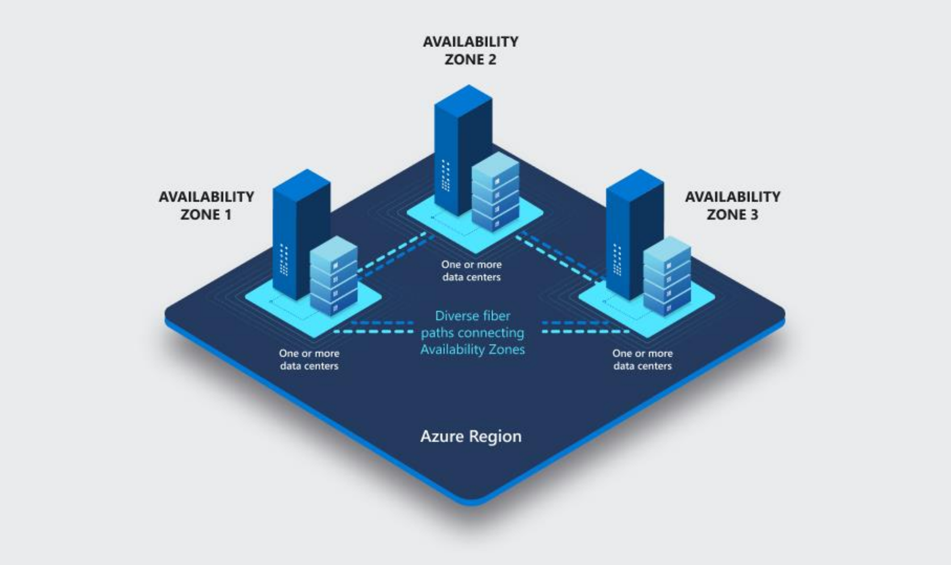
# AMBA Roadmap

aka.ms/amba/patterns/alz

- ALZ Portal updates
  - Action groups
  - Service health
  - Notification Assets
  - Existence Condition
- AMBA for ALZ Bicep/ Terraform
- Alert Processing Rule for alert suppression
- Bring your own Action Group and/ or Alert Processing Rule

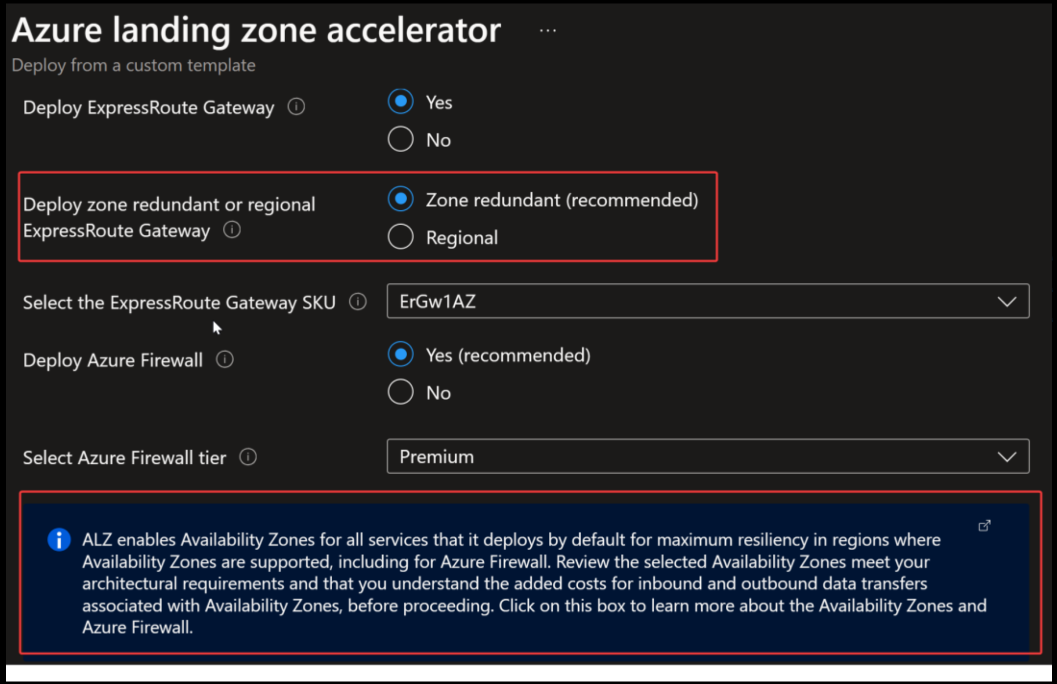
- Email will not be mandatory for action group deployment
- Look out for the Preparing for the unexpected session (End of April) https://aka.ms/readiness/videos

# Zone Redundancy Updates



# Zone Redundancy Updates

- Objective – to make ALZ Zone Redundant by Default
- 154 survey responses for Bicep and TF – Thank you
- Phased Approach
  - Phase 1 – Portal, Bicep and Terraform *Accelerators* zone redundant by default by end of Q2 CY24
  - Phase 2 – Bicep and Terraform Modules zone redundant by default by end of CY24
- Blog planned within next month to provide details
- Portal is already complete!



## Azure landing zone accelerator ···

Deploy from a custom template

Deploy ExpressRoute Gateway ⓘ ● Yes ○ No

Deploy zone redundant or regional ExpressRoute Gateway ⓘ ● Zone redundant (recommended) ○ Regional

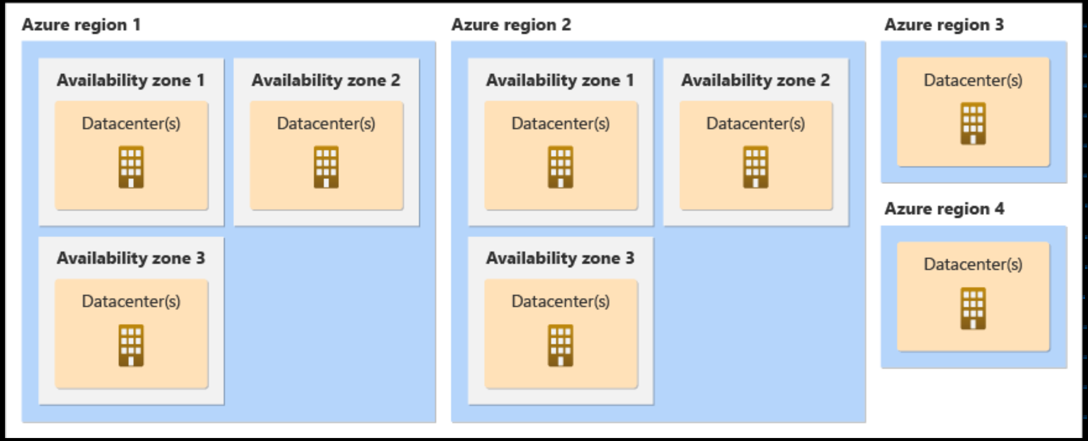
Select the ExpressRoute Gateway SKU ⓘ ErGw1AZ

Deploy Azure Firewall ⓘ ● Yes (recommended) ○ No

Select Azure Firewall tier ⓘ Premium

ALZ enables Availability Zones for all services that it deploys by default for maximum resiliency in regions where Availability Zones are supported, including for Azure Firewall. Review the selected Availability Zones meet your architectural requirements and that you understand the added costs for inbound and outbound data transfers associated with Availability Zones, before proceeding. Click on this box to learn more about the Availability Zones and Azure Firewall.

# Multi-Region Updates



Azure region 1

Availability zone 1

Datacenter(s)

Availability zone 2

Datacenter(s)

Availability zone 3

Datacenter(s)

Azure region 2

Availability zone 1

Datacenter(s)

Availability zone 2

Datacenter(s)

Availability zone 3

Datacenter(s)

Azure region 3

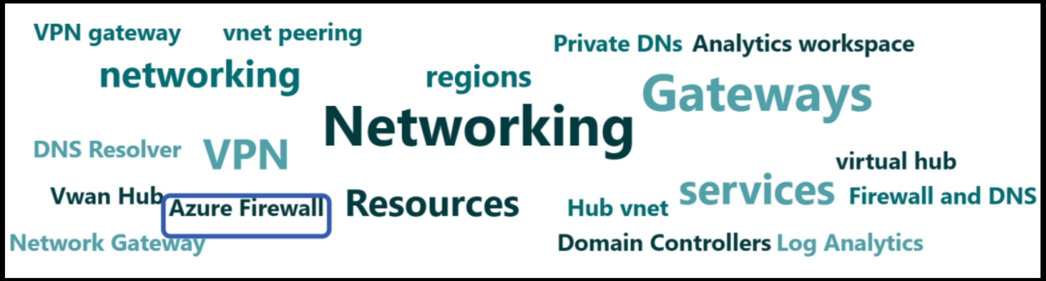
Datacenter(s)

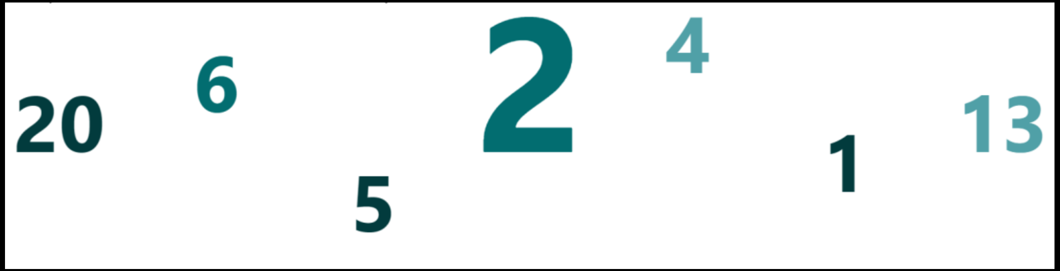
Azure region 4

Datacenter(s)

# Multi-Region Updates

- We had 56 responses to our detailed multi-region survey
- Networking was top ask
- Majority of respondents have 2 region deployments
- More than half deploying using ALZ Terraform





# Multi-Region Updates

- We’ve assessed all the feedback and locked in focus areas
  - Multiple Hub networks, Private DNS Zones, VPN / ER Gateways, Azure Firewall (and Policies) and Multiple vWAN Hubs
- Work kicked-off this month on Portal Reference Implementation to include changes
- Bicep and Terraform will follow
- Planning for completion ~Q3 CY2024

# ALZ Bicep Updates

# ALZ-Bicep Updates

## v0.17.2 just released!

- Introduced Resource Locks to all ALZ Bicep Modules.
- Added policy assignments for baseline Sovereign Landing Zone initiatives.
- Added parameter files and associated wiki for connectivity modules to incorporate resources with availability zones configured by default.

- Implemented new deployment toggles in hub-spoke configurations, providing users with increased flexibility and control over deployment of the VPN and ExpressRoute Gateways
- Add support for new Azure Regions
  - Israel Central
  - Italy North
  - Poland Central

# ALZ-Bicep Roadmap

## Public Roadmap

- Integrate Azure Monitor Baseline Alerts and associated documentation.
- Updates to accommodate MMA Deprecation with AMA.
- Automate the setup of Azure DevOps and GitHub within the Accelerator.
- Add ability to customize subnets and add conditions for Hub-Spoke module.
- Simplify policy updates and customizations within the Accelerator framework.

# ALZ Terraform vNext Update

# ALZ Terraform Module vNext

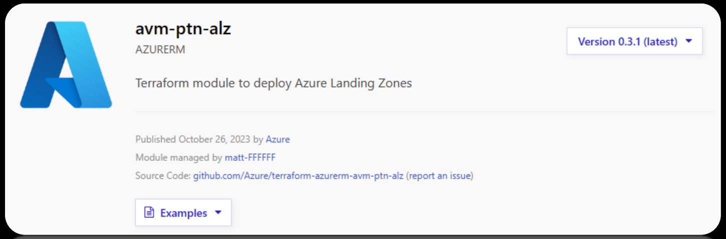
New Pattern Module: aka.ms/avm-ptn-alz

(Backed by the ALZ Terraform Provider: aka.ms/tf-pdr-alz)

Example usage: aka.ms/avm-ptn-alz-example

## Scope of the new module

- Management groups
- Policy
- Role Assignments



avm-ptn-alz

AZURERM

Version 0.3.1 (latest)

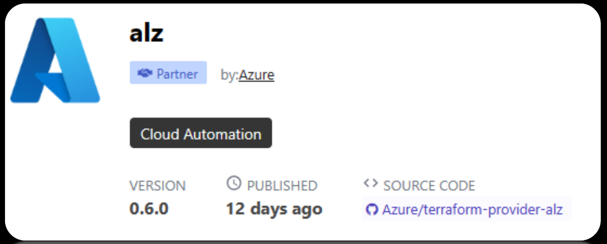
Terraform module to deploy Azure Landing Zones

Published October 26, 2023 by Azure

Module managed by matt-FFFFFF

Source Code: github.com/Azure/terraform-azurerm-avm-ptn-alz (report an issue)

Examples



alz

Partner by:Azure

Cloud Automation

VERSION 0.6.0

PUBLISHED 12 days ago

SOURCE CODE Azure/terraform-provider-alz

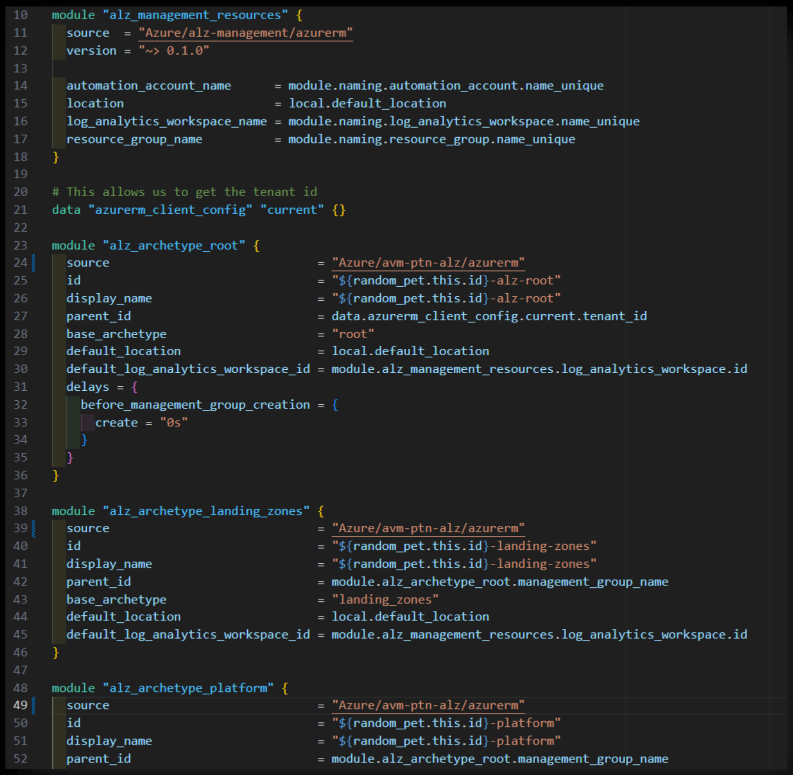
# How to build a Landing Zone

## Compose the modules together

- Azure/avm-ptn-alz: Management groups and policy
- Azure/alz-management: Management resources like log analytics, etc
- Azure/hubnetworking: Hub networking with vNet or vWan
- Azure/vnet-gateway: vNet gateways
- Etc…

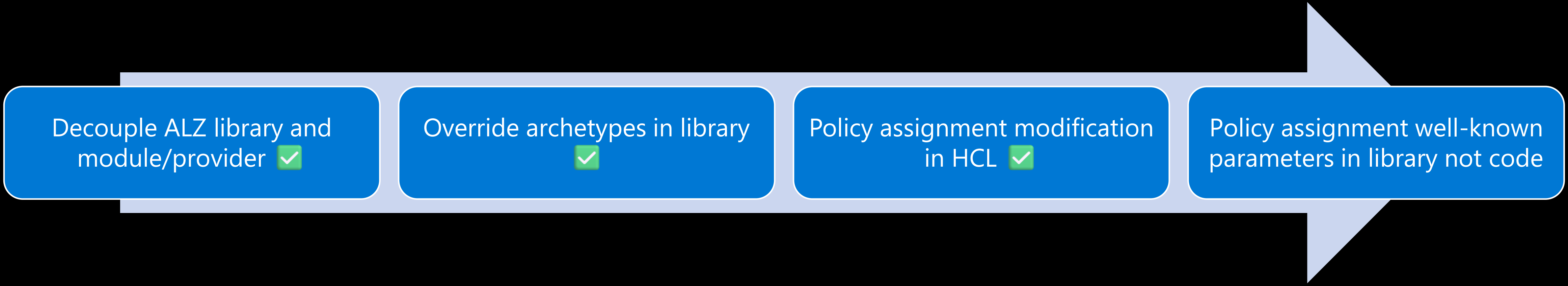
## Azure Verified Modules (AVM)?

- These modules will be renamed to align with AVM soon!



```
module "alz_management_resources" {
  source  = "Azure/alz-management/azurerm"
  version = "~> 0.1.0"

  automation_account_name      = module.naming.automation_account.name_unique
  location                     = local.default_location
  log_analytics_workspace_name = module.naming.log_analytics_workspace.name_unique
  resource_group_name          = module.naming.resource_group.name_unique
}

# This allows us to get the tenant id
data "azurerm_client_config" "current" {}

module "alz_archetype_root" {
  source                            = "Azure/avm-ptn-alz/azurerm"
  id                                = "${random_pet.this.id}-alz-root"
  display_name                      = "${random_pet.this.id}-alz-root"
  parent_id                         = data.azurerm_client_config.current.tenant_id
  base_archetype                    = "root"
  default_location                  = local.default_location
  default_log_analytics_workspace_id = module.alz_management_resources.log_analytics_workspace.id
  delays = {
    before_management_group_creation = {
      create = "0s"
    }
  }
}

module "alz_archetype_landing_zones" {
  source                            = "Azure/avm-ptn-alz/azurerm"
  id                                = "${random_pet.this.id}-landing-zones"
  display_name                      = "${random_pet.this.id}-landing-zones"
  parent_id                         = module.alz_archetype_root.management_group_name
  base_archetype                    = "landing_zones"
  default_location                  = local.default_location
  default_log_analytics_workspace_id = module.alz_management_resources.log_analytics_workspace.id
}

module "alz_archetype_platform" {
  source                            = "Azure/avm-ptn-alz/azurerm"
  id                                = "${random_pet.this.id}-platform"
  display_name                      = "${random_pet.this.id}-platform"
  parent_id                         = module.alz_archetype_root.management_group_name
```

# Pathway to v1.0



Decouple ALZ library and module/provider ✅

Override archetypes in library ✅

Policy assignment modification in HCL ✅

Policy assignment well-known parameters in library not code

# Demo and Roadmap

## Can I use it now?

- Yes. We want you to try it out now!
- Give us feedback by raising issues and / or PRs in GitHub.
- End to end example in the ALZ Terraform Accelerator: aka.ms/alz-tf-acc

## What's coming next?

## What does it look like?

- Demo Time!

Microsoft

# Q & A

Next Community Call will be on 12th June 2024 👍

Back to an APAC friendly time slot for this occurrence and then the one after will be back to this time slot 👍

Stay tuned to issue #1596 (ALZ/ESLZ Repo)

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

# This month’s presenters:

# Thank You! 👋

**Stay up-to-date:**

**https://aka.ms/ALZ/WhatsNew**