This month's presenters:

Microsoft

Azure Landing Zones

25th September 2023 - External Community Call

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

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

This meeting is being recorded

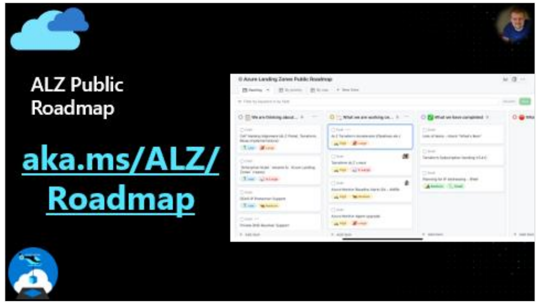
Before we get started…

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 ☺

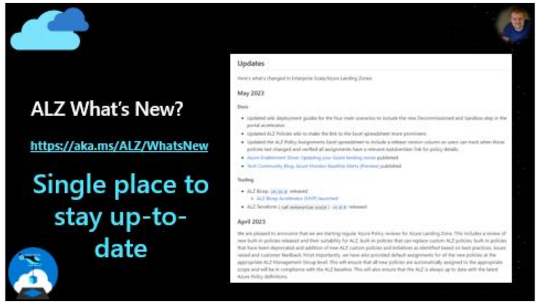
Implementation Options & Accelerators



ALZ Public Roadmap

aka.ms/ALZ/Roadmap

Azure Landing Zones Public Roadmap



ALZ What's New?

https://aka.ms/ALZ/WhatsNew

Single place to stay up-to-date

Updates

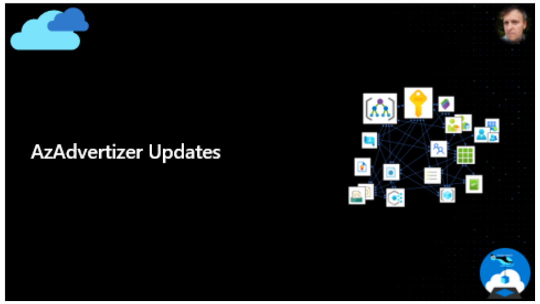
May 2023

Docs

Tooling

April 2023

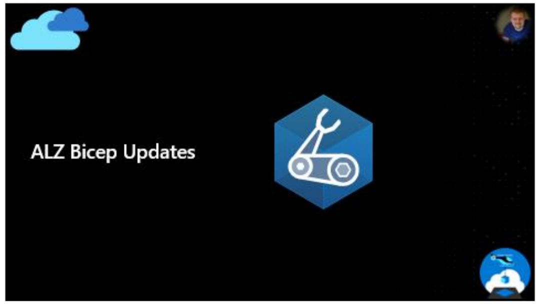
ALZ Policy Refresh Latest



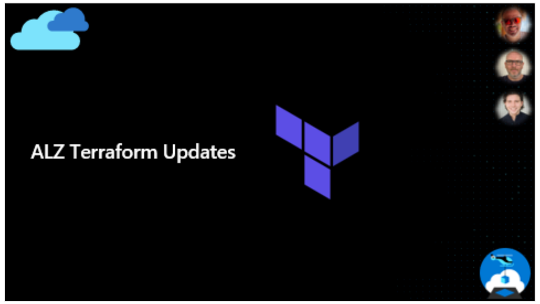
AzAdvertizer Updates

AMBA Updates

https://aka.ms/alz/monitor/repo → https://aka.ms/amba/alz



ALZ Bicep Updates



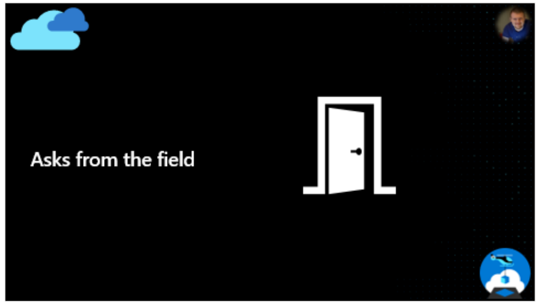
ALZ Terraform Updates

Subscription Vending Updates

Microsoft

Azure Verified Modules (AVM)

IaC Module Strategy across Microsoft for Bicep & Terraform



Asks from the field

Microsoft

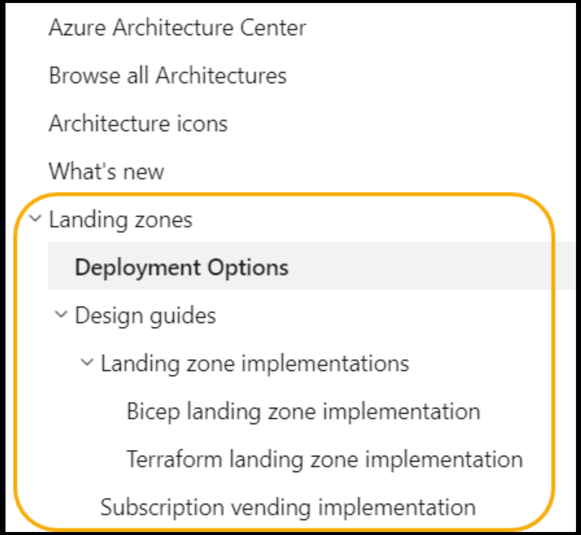
Q & A

Agenda

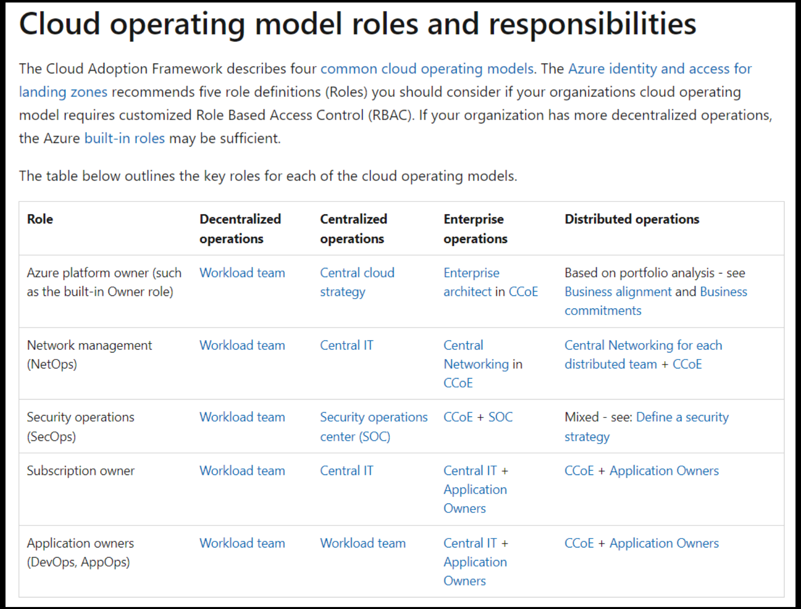
- Public Roadmap
- New CAF Docs & Updates
- Policy Refresh Updates
- AzAdvertizer & AzGovViz Updates
- AMBA Updates
- ALZ Bicep Accelerator Updates
- ALZ Terraform v.next & Accelerator Updates
- Sub Vending Updates
- Azure Verified Modules Intro
- Questions from the Field

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

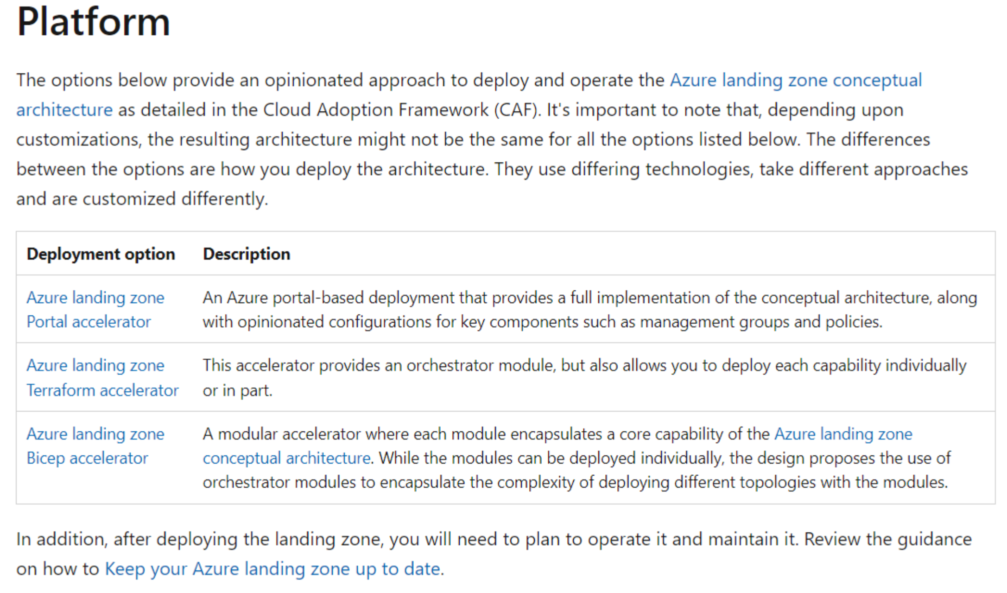


Cloud operating model roles and responsibilities

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

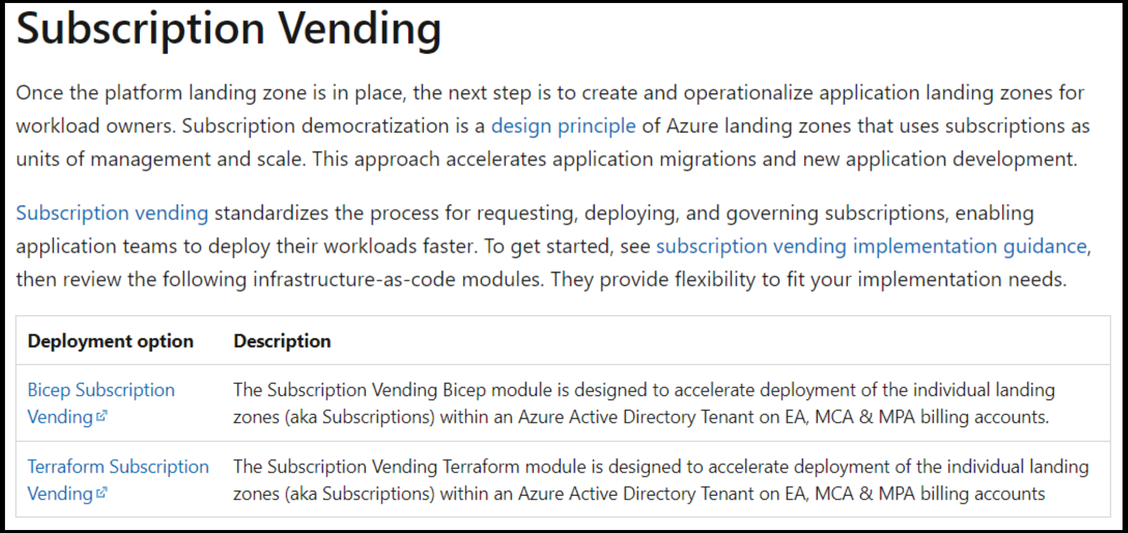


Platform

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.

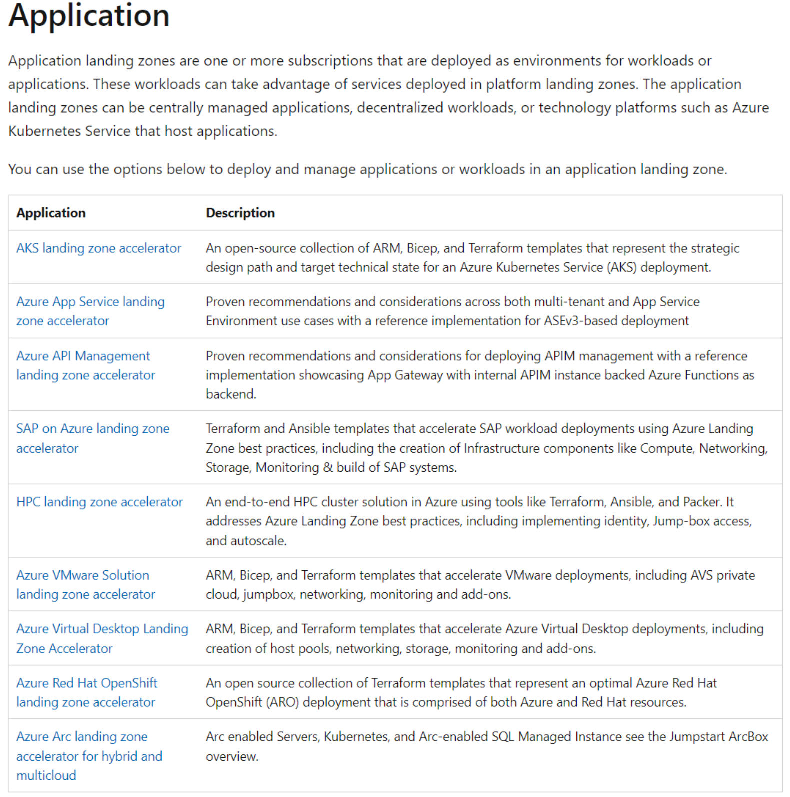


Subscription Vending

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



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.

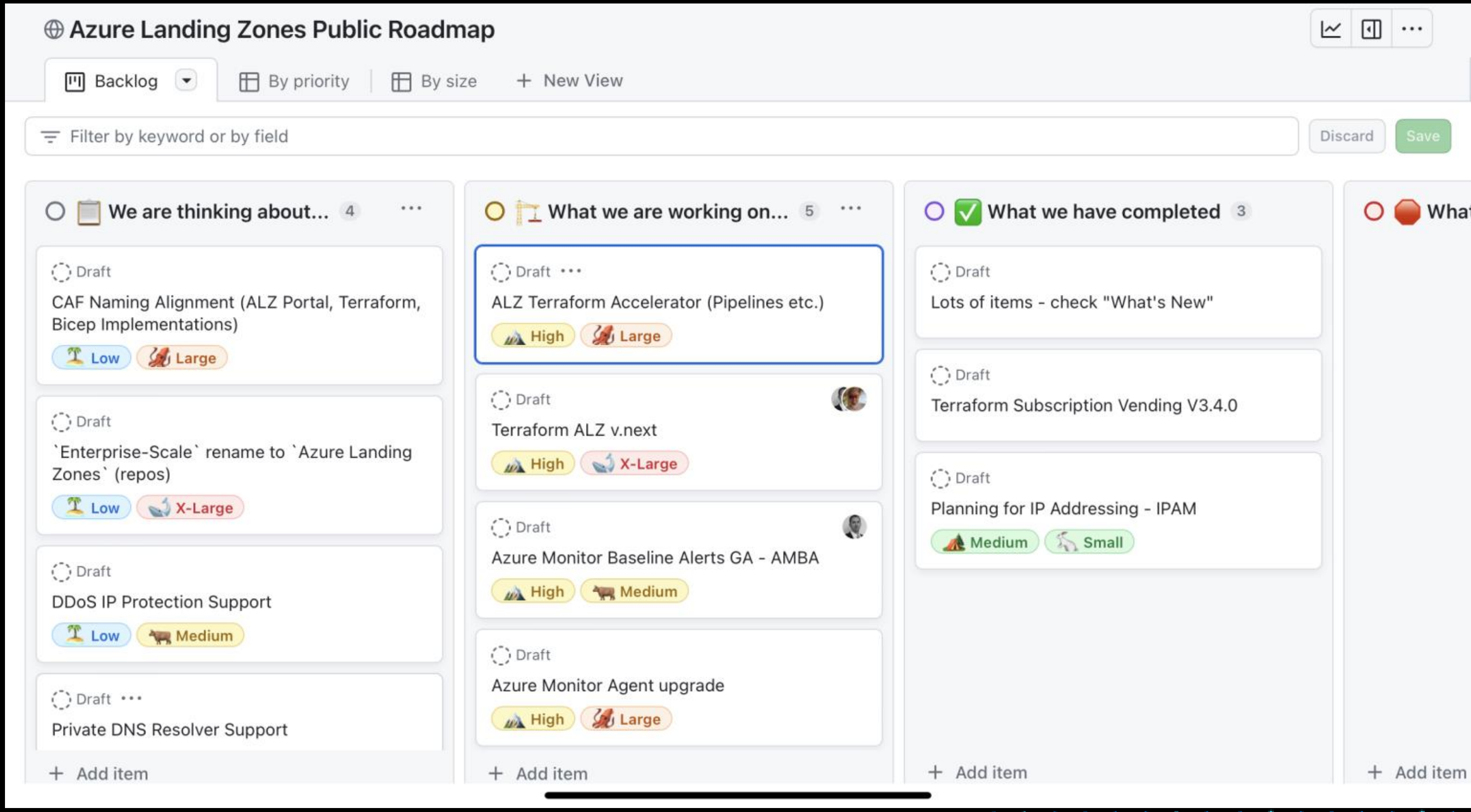
You can use the options below to deploy and manage applications or workloads in an application landing zone.

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.

aka.ms/ALZ/AAC

ALZ Public Roadmap

aka.ms/ALZ/Roadmap



Azure Landing Zones Public Roadmap

We are thinking about... 4

- Draft
  CAF Naming Alignment (ALZ Portal, Terraform, Bicep Implementations)
  Low · Large
- Draft
  `Enterprise-Scale` rename to `Azure Landing Zones` (repos)
  Low · X-Large
- Draft
  DDoS IP Protection Support
  Low · Medium
- Draft
  Private DNS Resolver Support

+ Add item

What we are working on... 5

- Draft
  ALZ Terraform Accelerator (Pipelines etc.)
  High · Large
- Draft
  Terraform ALZ v.next
  High · X-Large
- Draft
  Azure Monitor Baseline Alerts GA - AMBA
  High · Medium
- Draft
  Azure Monitor Agent upgrade
  High · Large

+ Add item

✅ What we have completed 3

- Draft
  Lots of items - check "What's New"
- Draft
  Terraform Subscription Vending V3.4.0
- Draft
  Planning for IP Addressing - IPAM
  Medium · Small

+ Add item

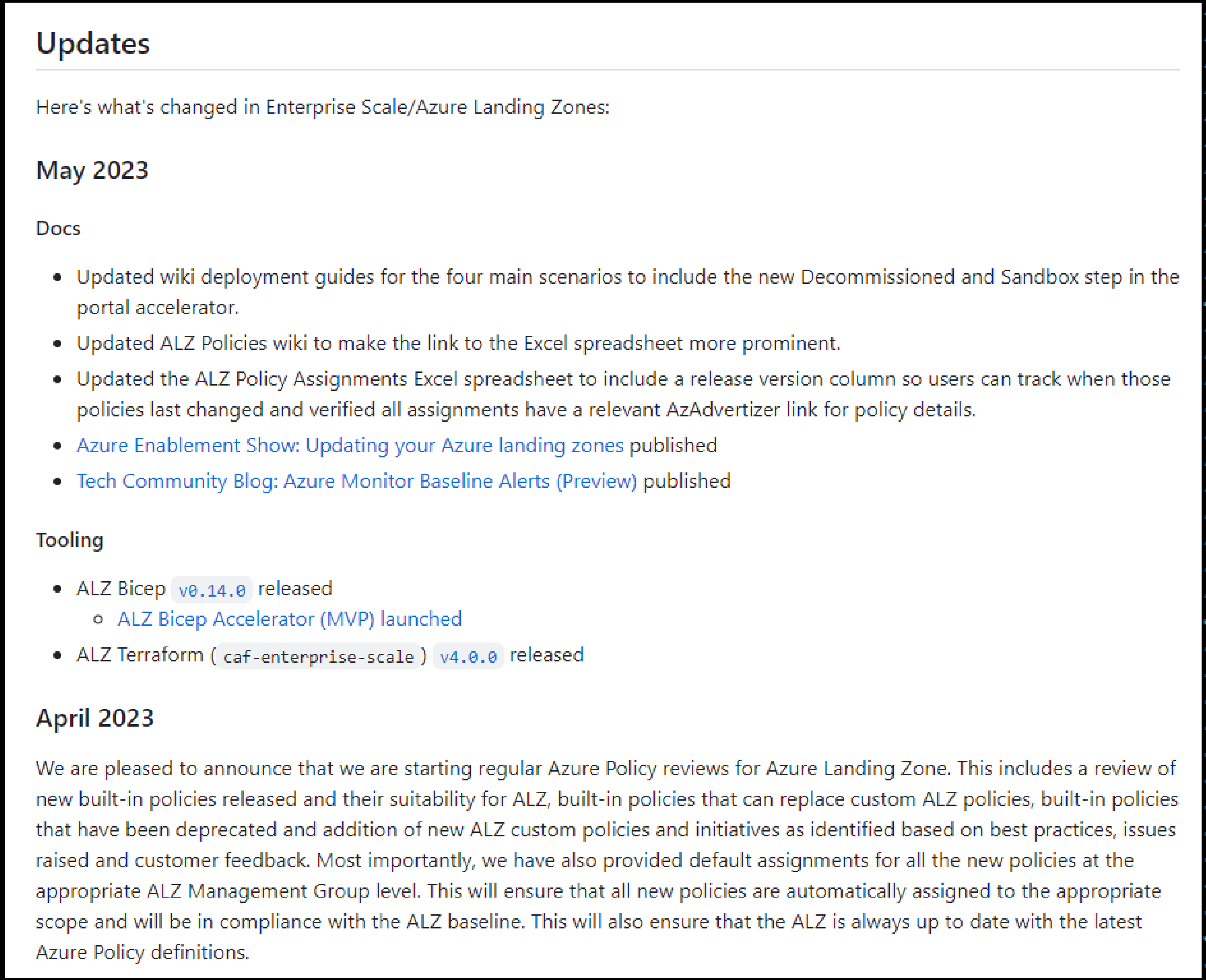
🛑 What

+ Add item

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:

May 2023

Docs

- Updated wiki deployment guides for the four main scenarios to include the new Decommissioned and Sandbox step in the portal accelerator.
- Updated ALZ Policies wiki to make the link to the Excel spreadsheet more prominent.
- Updated the ALZ Policy Assignments Excel spreadsheet to include a release version column so users can track when those policies last changed and verified all assignments have a relevant AzAdvertizer link for policy details.
- Azure Enablement Show: Updating your Azure landing zones published
- Tech Community Blog: Azure Monitor Baseline Alerts (Preview) published

Tooling

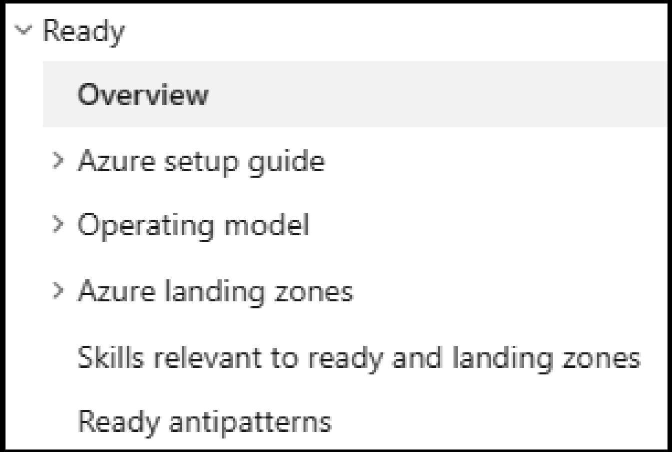
- ALZ Bicep `v0.14.0` released
  - ALZ Bicep Accelerator (MVP) launched
- ALZ Terraform (`caf-enterprise-scale`) `v4.0.0` released

April 2023

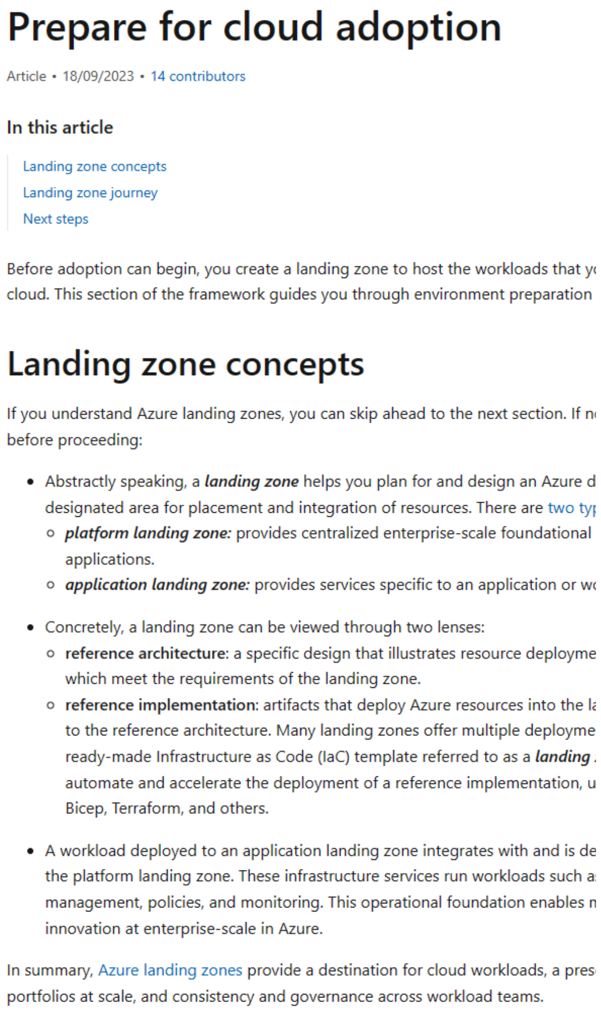
We are pleased to announce that we are starting regular Azure Policy reviews for Azure Landing Zone. This includes a review of new built-in policies released and their suitability for ALZ, built-in policies that can replace custom ALZ policies, built-in policies that have been deprecated and addition of new ALZ custom policies and initiatives as identified based on best practices, issues raised and customer feedback. Most importantly, we have also provided default assignments for all the new policies at the appropriate ALZ Management Group level. This will ensure that all new policies are automatically assigned to the appropriate scope and will be in compliance with the ALZ baseline. This will also ensure that the ALZ is always up to date with the latest Azure Policy definitions.

CAF Doc Refresh

Ready – Overview



- Ready
  - Overview
  - Azure setup guide
  - Operating model
  - Azure landing zones
  - Skills relevant to ready and landing zones
  - Ready antipatterns



Prepare for cloud adoption

Article • 18/09/2023 • 14 contributors

Feedback

In this article

- Landing zone concepts
- Landing zone journey
- Next steps

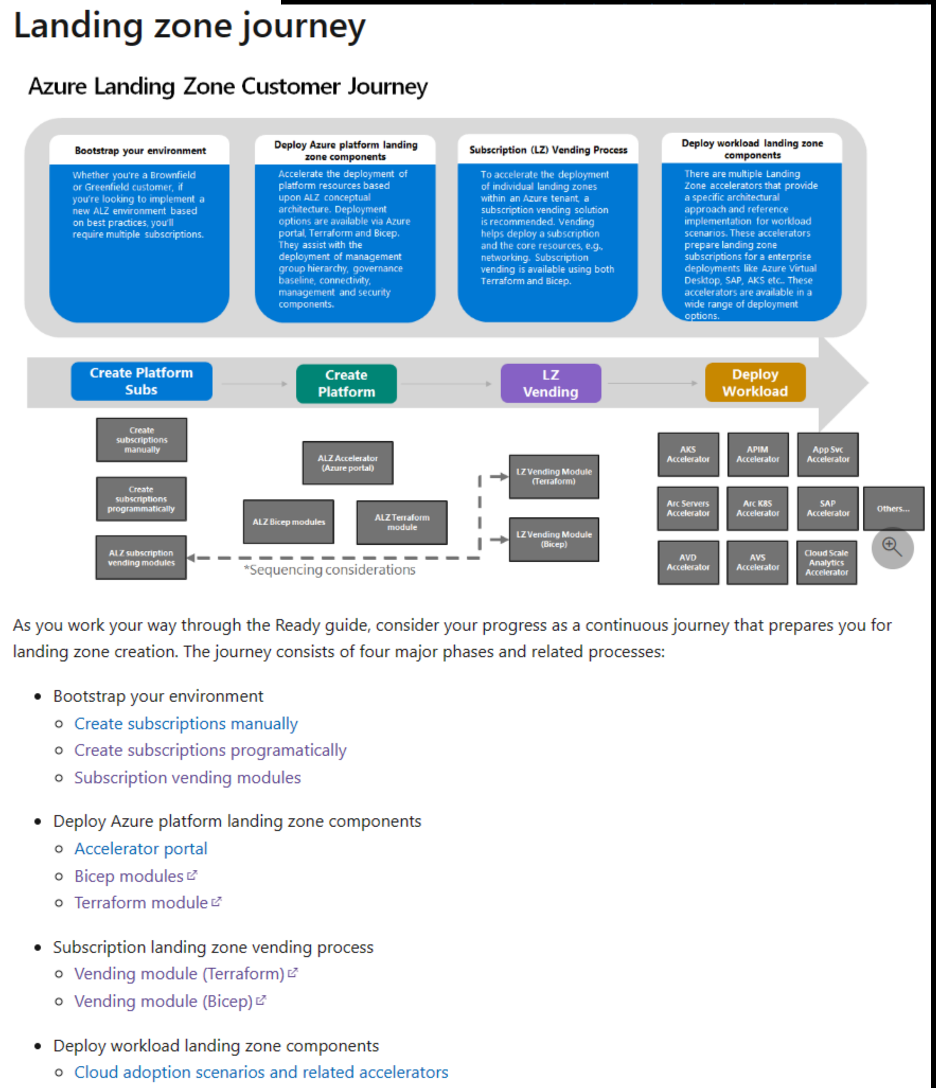
Before adoption can begin, you create a landing zone to host the workloads that y
cloud. This section of the framework guides you through environment preparation

Landing zone concepts

If you understand Azure landing zones, you can skip ahead to the next section. If n
before proceeding:

- Abstractly speaking, a ***landing zone*** helps you plan for and design an Azure d
designated area for placement and integration of resources. There are two typ
  - ***platform landing zone:*** provides centralized enterprise-scale foundational
applications.
  - ***application landing zone:*** provides services specific to an application or w
- Concretely, a landing zone can be viewed through two lenses:
  - **reference architecture**: a specific design that illustrates resource deployme
which meet the requirements of the landing zone.
  - **reference implementation**: artifacts that deploy Azure resources into the la
to the reference architecture. Many landing zones offer multiple deployme
ready-made Infrastructure as Code (IaC) template referred to as a ***landing***
automate and accelerate the deployment of a reference implementation, u
Bicep, Terraform, and others.
- A workload deployed to an application landing zone integrates with and is de
the platform landing zone. These infrastructure services run workloads such a
management, policies, and monitoring. This operational foundation enables n
innovation at enterprise-scale in Azure.

In summary, Azure landing zones provide a destination for cloud workloads, a pres
portfolios at scale, and consistency and governance across workload teams.



Landing zone journey

Azure Landing Zone Customer Journey

Bootstrap your environment

Whether you're a Brownfield or Greenfield customer, if you're looking to implement a new ALZ environment based on best practices, you'll require multiple subscriptions.

Deploy Azure platform landing zone components

Accelerate the deployment of platform resources based upon ALZ conceptual architecture. Deployment options are available via Azure portal, Terraform and Bicep. They assist with the deployment of management group hierarchy, governance baseline, connectivity, management and security components.

Subscription (LZ) Vending Process

To accelerate the deployment of individual landing zones within an Azure tenant, a subscription vending solution is recommended. Vending helps deploy a subscription and the core resources, e.g., networking. Subscription vending is available using both Terraform and Bicep.

Deploy workload landing zone components

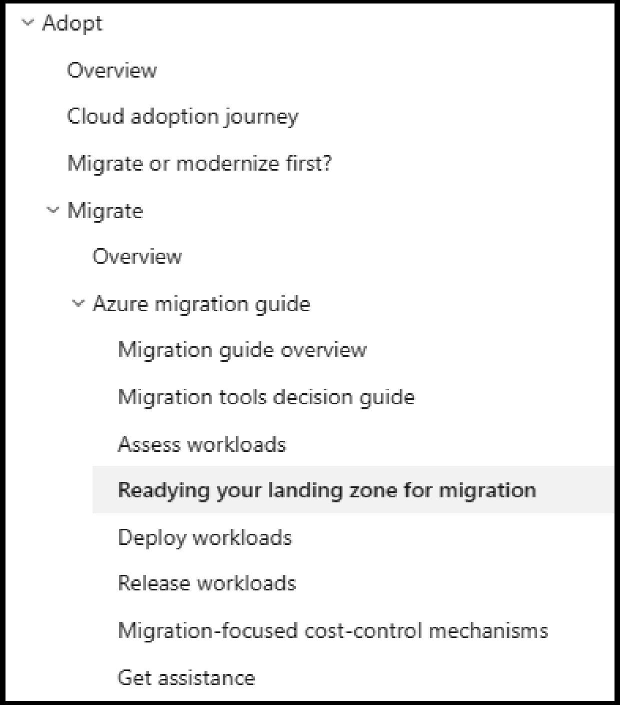
There are multiple Landing Zone accelerators that provide a specific architectural approach and reference implementation for workload scenarios. These accelerators prepare landing zone subscriptions for a enterprise deployments like Azure Virtual Desktop, SAP, AKS etc.. These accelerators are available in a wide range of deployment options.

As you work your way through the Ready guide, consider your progress as a continuous journey that prepares you for landing zone creation. The journey consists of four major phases and related processes:

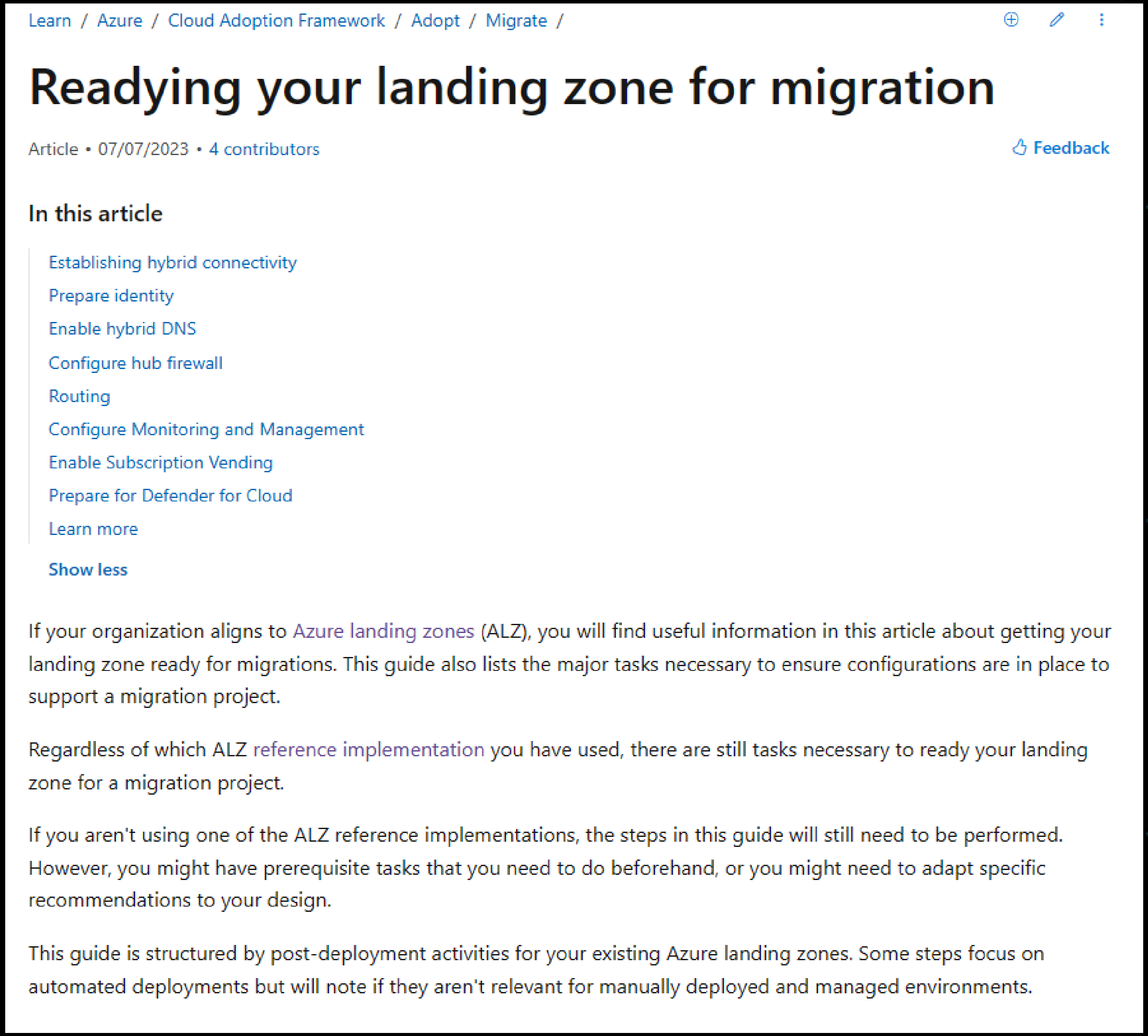
- Bootstrap your environment
  - Create subscriptions manually
  - Create subscriptions programatically
  - Subscription vending modules
- Deploy Azure platform landing zone components
  - Accelerator portal
  - Bicep modules
  - Terraform module
- Subscription landing zone vending process
  - Vending module (Terraform)
  - Vending module (Bicep)
- Deploy workload landing zone components
  - Cloud adoption scenarios and related accelerators

New CAF Doc

Readying your landing zone for migration



- Adopt
  - Overview
  - Cloud adoption journey
  - Migrate or modernize first?
  - Migrate
    - Overview
    - Azure migration guide
      - Migration guide overview
      - Migration tools decision guide
      - Assess workloads
      - **Readying your landing zone for migration**
      - Deploy workloads
      - Release workloads
      - Migration-focused cost-control mechanisms
      - Get assistance



Learn / Azure / Cloud Adoption Framework / Adopt / Migrate /

Readying your landing zone for migration

Article • 07/07/2023 • 4 contributors

In this article

- Establishing hybrid connectivity
- Prepare identity
- Enable hybrid DNS
- Configure hub firewall
- Routing
- Configure Monitoring and Management
- Enable Subscription Vending
- Prepare for Defender for Cloud
- Learn more

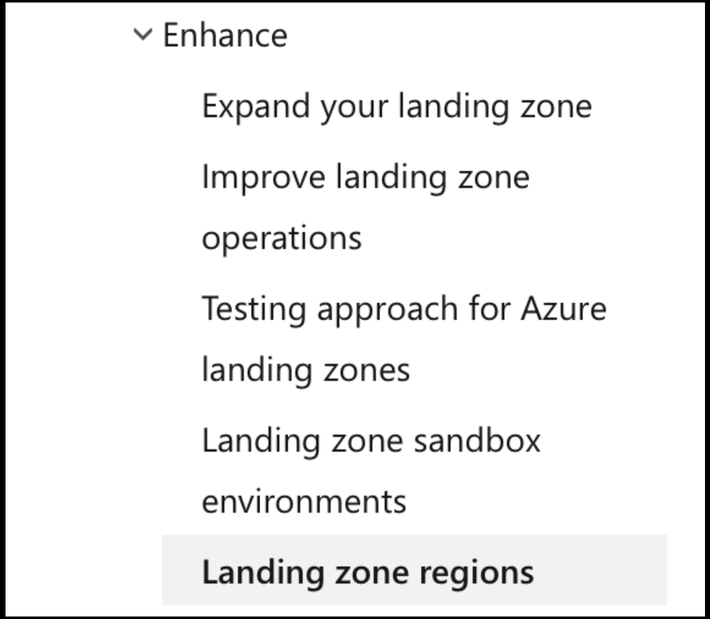
If your organization aligns to Azure landing zones (ALZ), you will find useful information in this article about getting your landing zone ready for migrations. This guide also lists the major tasks necessary to ensure configurations are in place to support a migration project.

Regardless of which ALZ reference implementation you have used, there are still tasks necessary to ready your landing zone for a migration project.

If you aren't using one of the ALZ reference implementations, the steps in this guide will still need to be performed. However, you might have prerequisite tasks that you need to do beforehand, or you might need to adapt specific recommendations to your design.

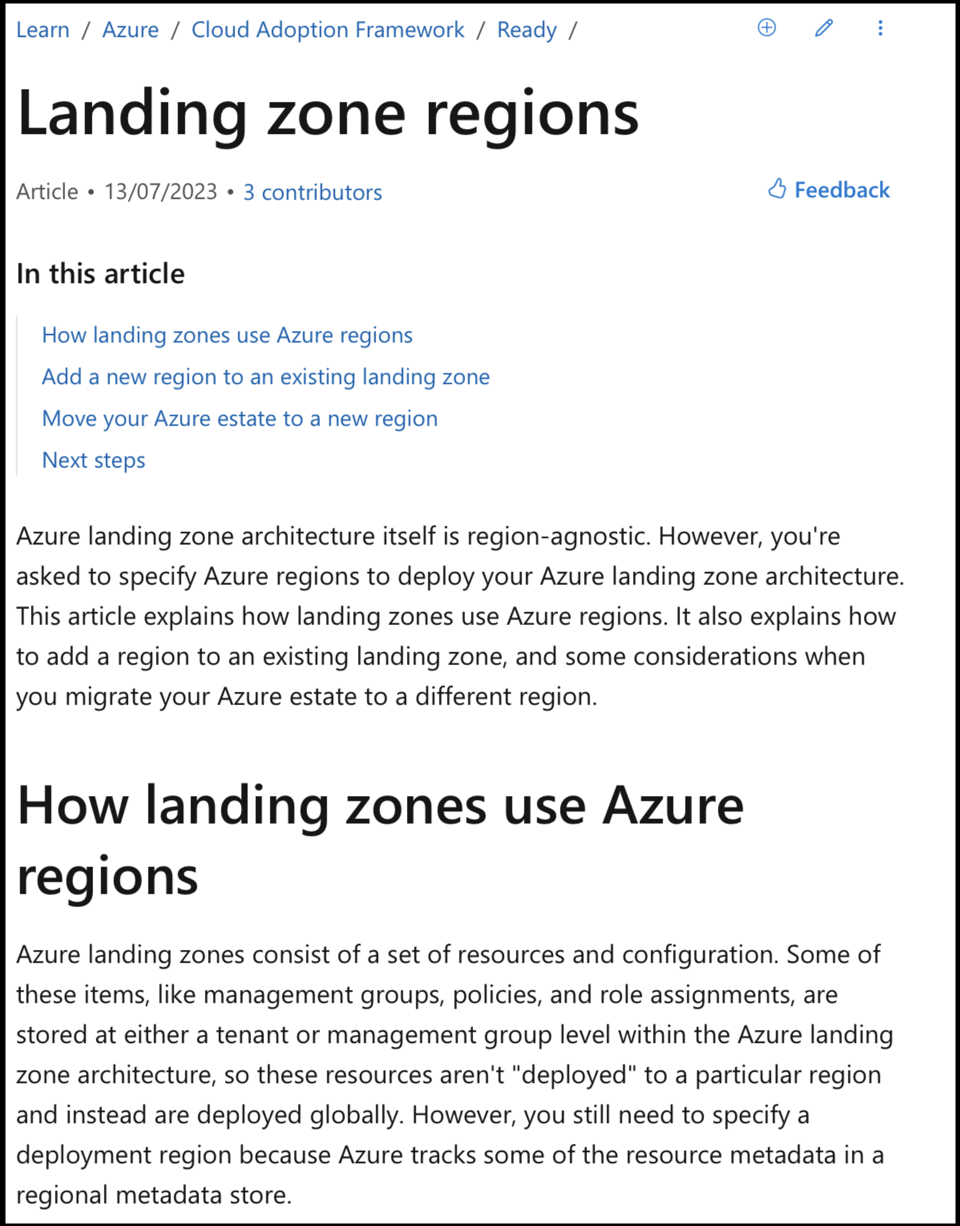
This guide is structured by post-deployment activities for your existing Azure landing zones. Some steps focus on automated deployments but will note if they aren't relevant for manually deployed and managed environments.

Landing Zone Regions



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

New CAF doc



Learn / Azure / Cloud Adoption Framework / Ready /

Landing zone regions

Article • 13/07/2023 • 3 contributors

Feedback

In this article

- How landing zones use Azure regions
- Add a new region to an existing landing zone
- Move your Azure estate to a new region
- Next steps

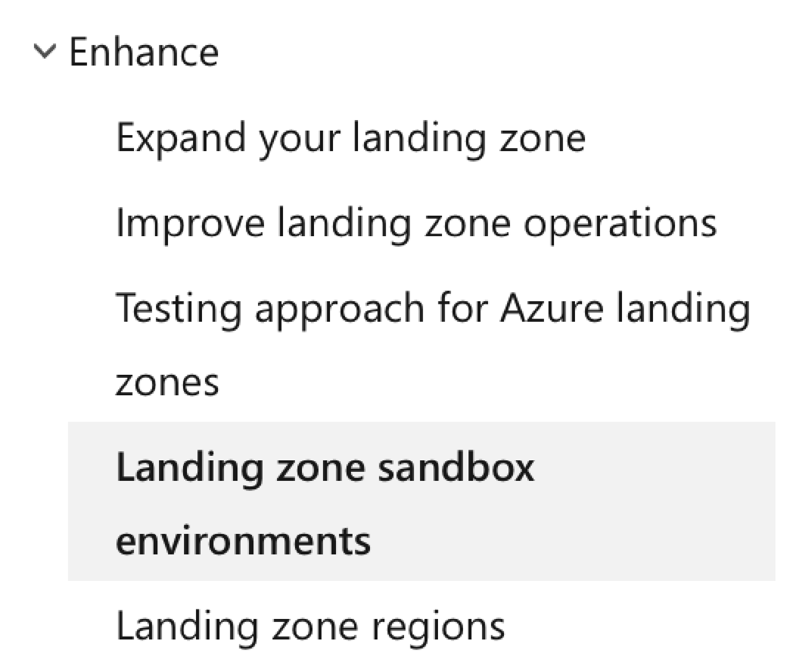
Azure landing zone architecture itself is region-agnostic. However, you're asked to specify Azure regions to deploy your Azure landing zone architecture. This article explains how landing zones use Azure regions. It also explains how to add a region to an existing landing zone, and some considerations when you migrate your Azure estate to a different region.

How landing zones use Azure regions

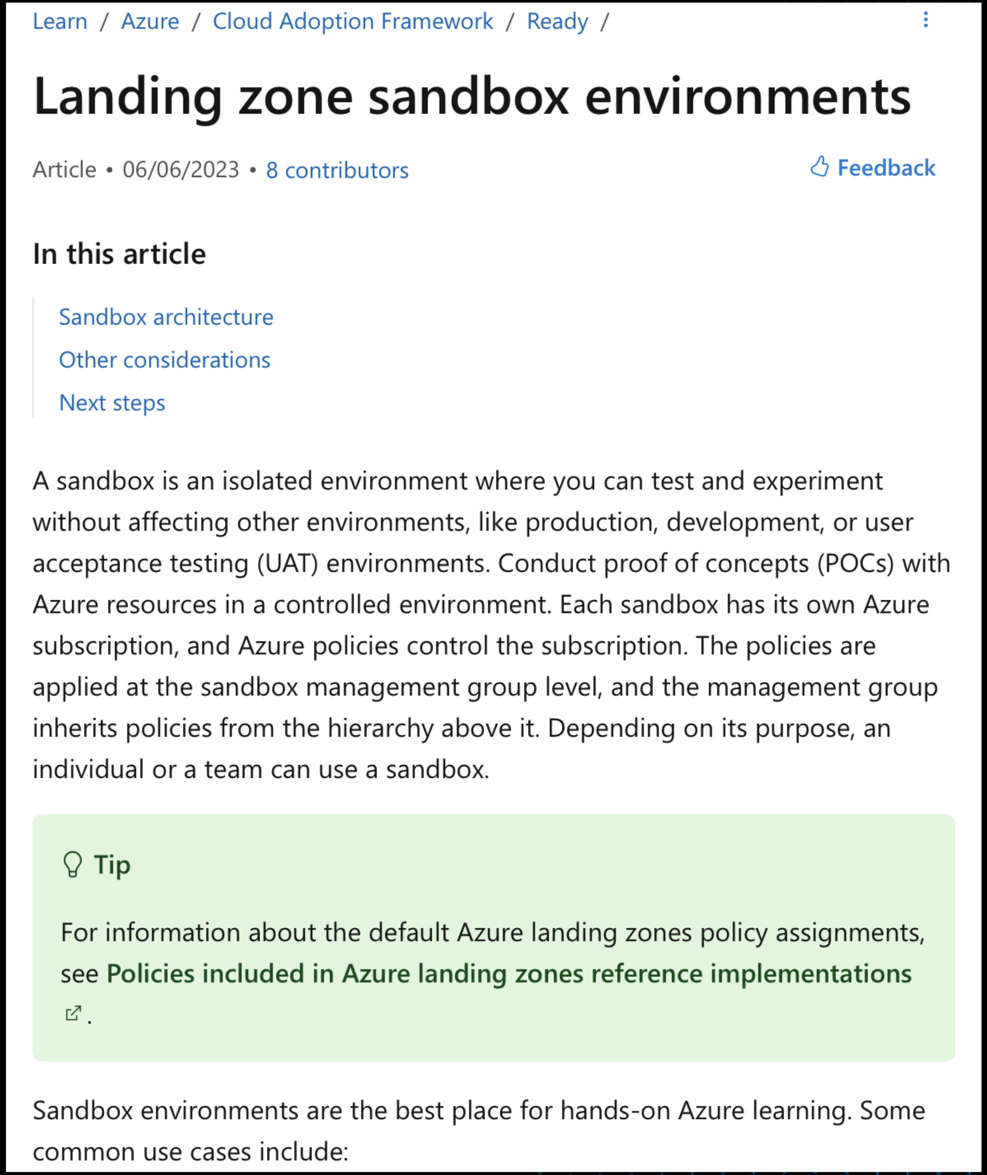
Azure landing zones consist of a set of resources and configuration. Some of these items, like management groups, policies, and role assignments, are stored at either a tenant or management group level within the Azure landing zone architecture, so these resources aren't "deployed" to a particular region and instead are deployed globally. However, you still need to specify a deployment region because Azure tracks some of the resource metadata in a regional metadata store.

New CAF doc

Landing zone sandbox environments



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



Learn / Azure / Cloud Adoption Framework / Ready /

Landing zone sandbox environments

Article • 06/06/2023 • 8 contributors

Feedback

In this article

- Sandbox architecture
- Other considerations
- Next steps

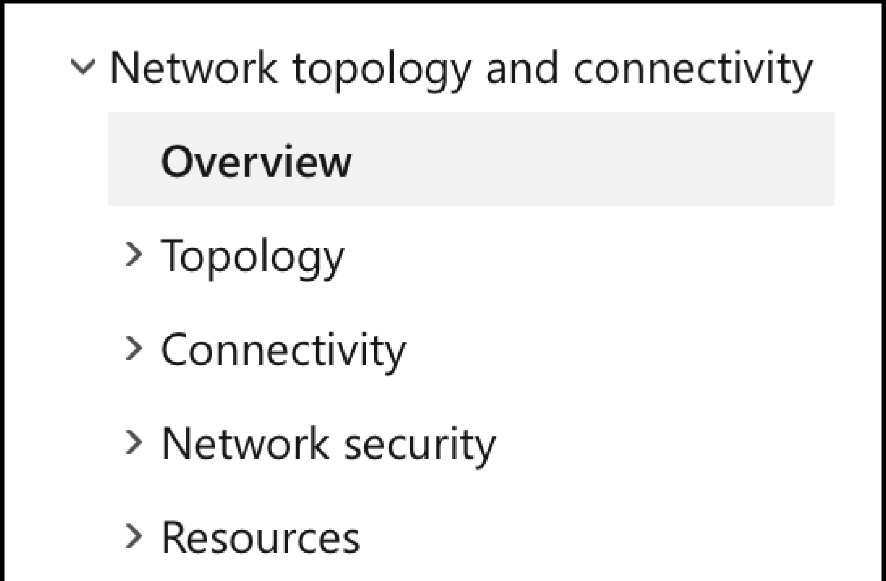
A sandbox is an isolated environment where you can test and experiment without affecting other environments, like production, development, or user acceptance testing (UAT) environments. Conduct proof of concepts (POCs) with Azure resources in a controlled environment. Each sandbox has its own Azure subscription, and Azure policies control the subscription. The policies are applied at the sandbox management group level, and the management group inherits policies from the hierarchy above it. Depending on its purpose, an individual or a team can use a sandbox.

> **Tip**
>
> For information about the default Azure landing zones policy assignments, see **Policies included in Azure landing zones reference implementations**.

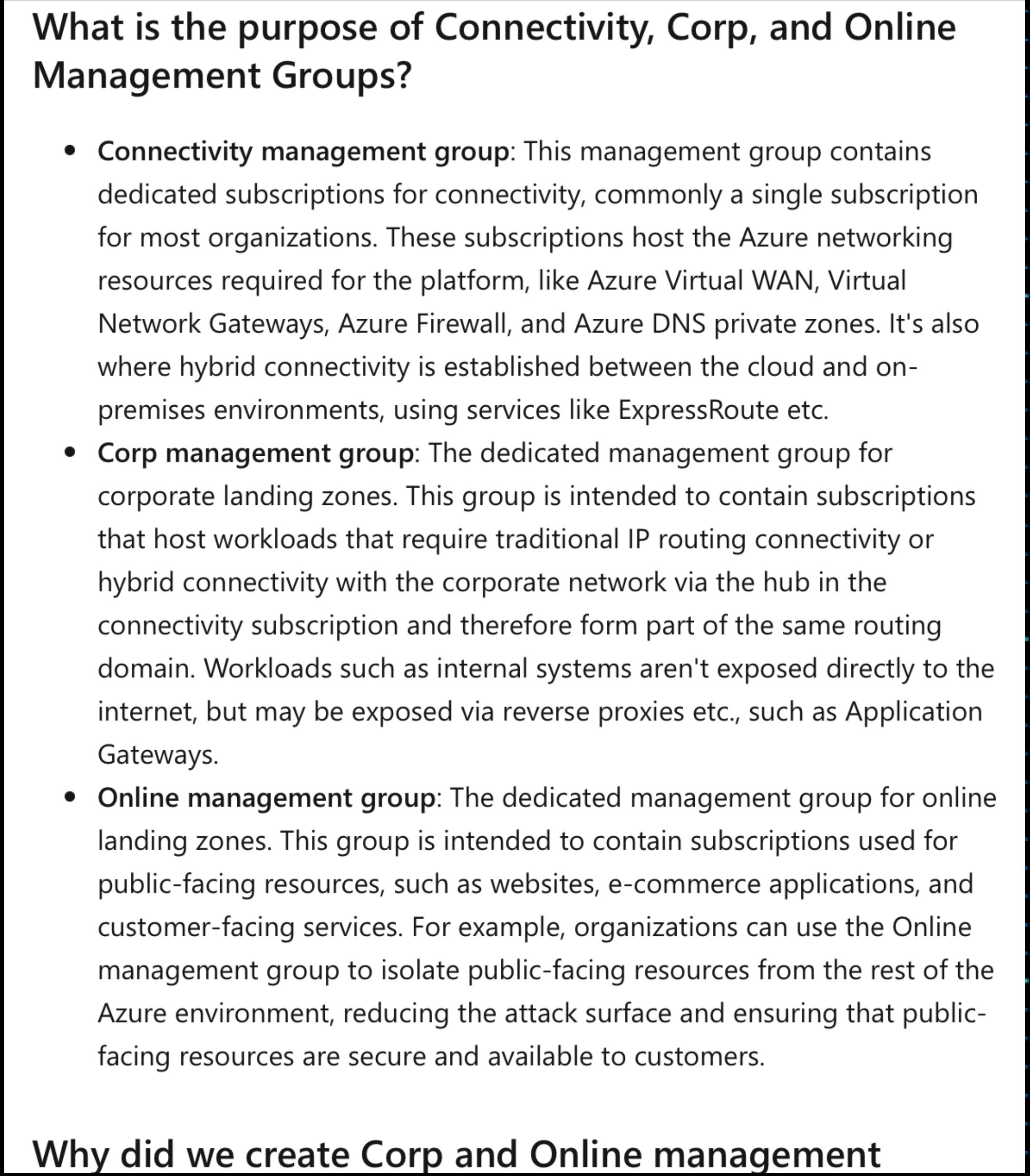
Sandbox environments are the best place for hands-on Azure learning. Some common use cases include:

New Section in CAF

Networking – Corp & Online



- Network topology and connectivity
  - **Overview**
  - Topology
  - Connectivity
  - Network security
  - Resources



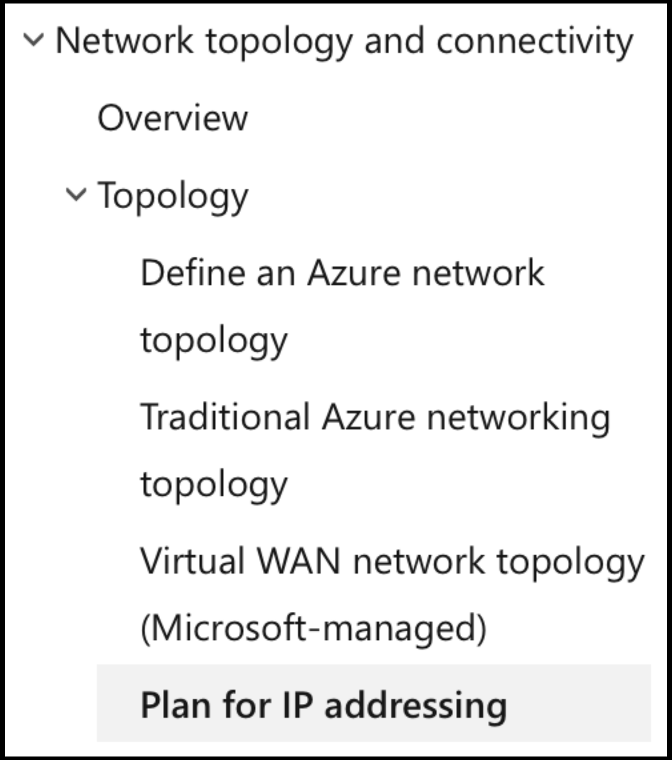
What is the purpose of Connectivity, Corp, and Online Management Groups?

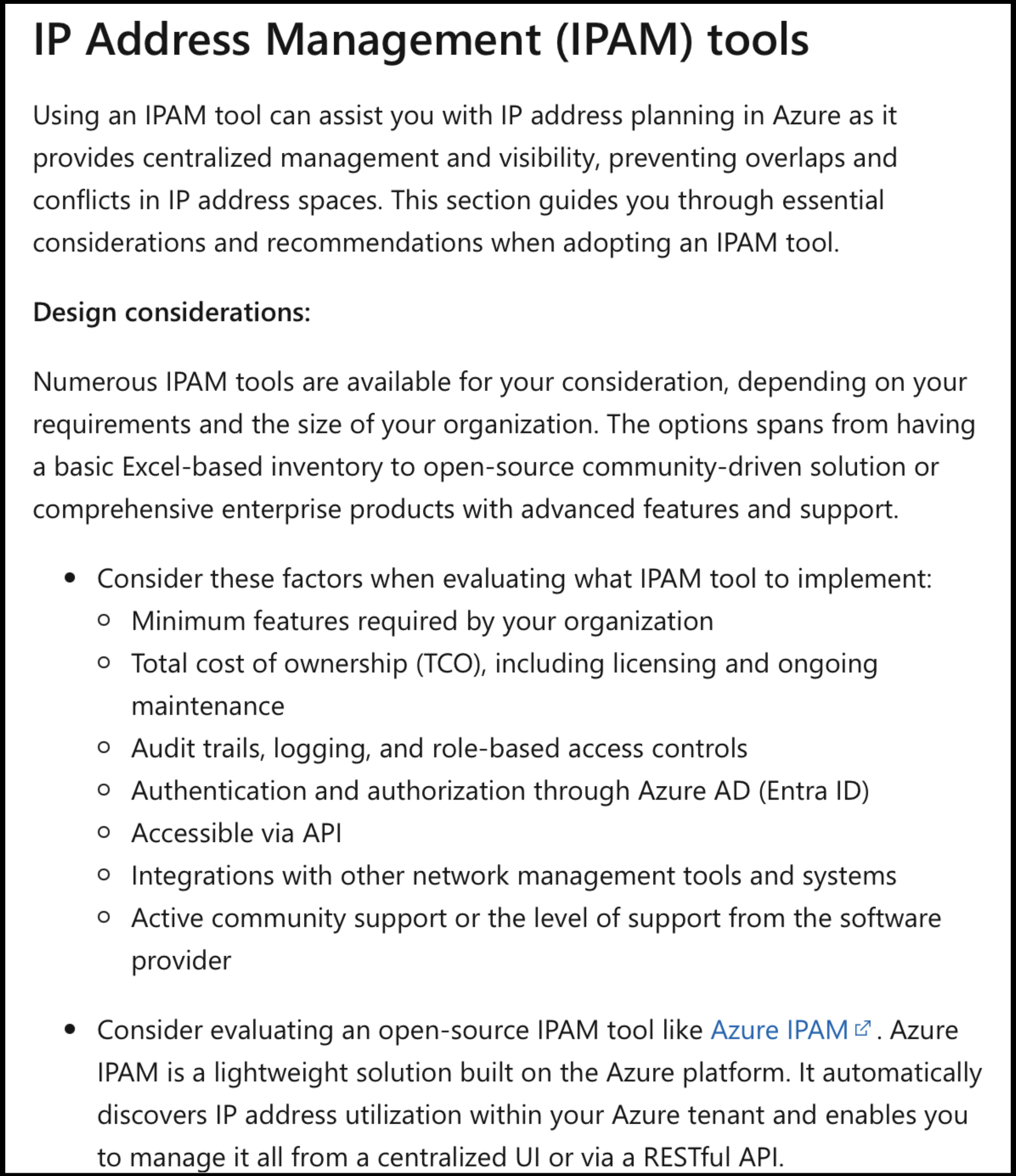
- **Connectivity management group**: This management group contains dedicated subscriptions for connectivity, commonly a single subscription for most organizations. These subscriptions host the Azure networking resources required for the platform, like Azure Virtual WAN, Virtual Network Gateways, Azure Firewall, and Azure DNS private zones. It's also where hybrid connectivity is established between the cloud and on-premises environments, using services like ExpressRoute etc.
- **Corp management group**: The dedicated management group for corporate landing zones. This group is intended to contain subscriptions that host workloads that require traditional IP routing connectivity or hybrid connectivity with the corporate network via the hub in the connectivity subscription and therefore form part of the same routing domain. Workloads such as internal systems aren't exposed directly to the internet, but may be exposed via reverse proxies etc., such as Application Gateways.
- **Online management group**: The dedicated management group for online landing zones. This group is intended to contain subscriptions used for public-facing resources, such as websites, e-commerce applications, and customer-facing services. For example, organizations can use the Online management group to isolate public-facing resources from the rest of the Azure environment, reducing the attack surface and ensuring that public-facing resources are secure and available to customers.

Why did we create Corp and Online management

New Section in CAF

Networking – Corp & Online


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



IP Address Management (IPAM) tools

Using an IPAM tool can assist you with IP address planning in Azure as it provides centralized management and visibility, preventing overlaps and conflicts in IP address spaces. This section guides you through essential considerations and recommendations when adopting an IPAM tool.

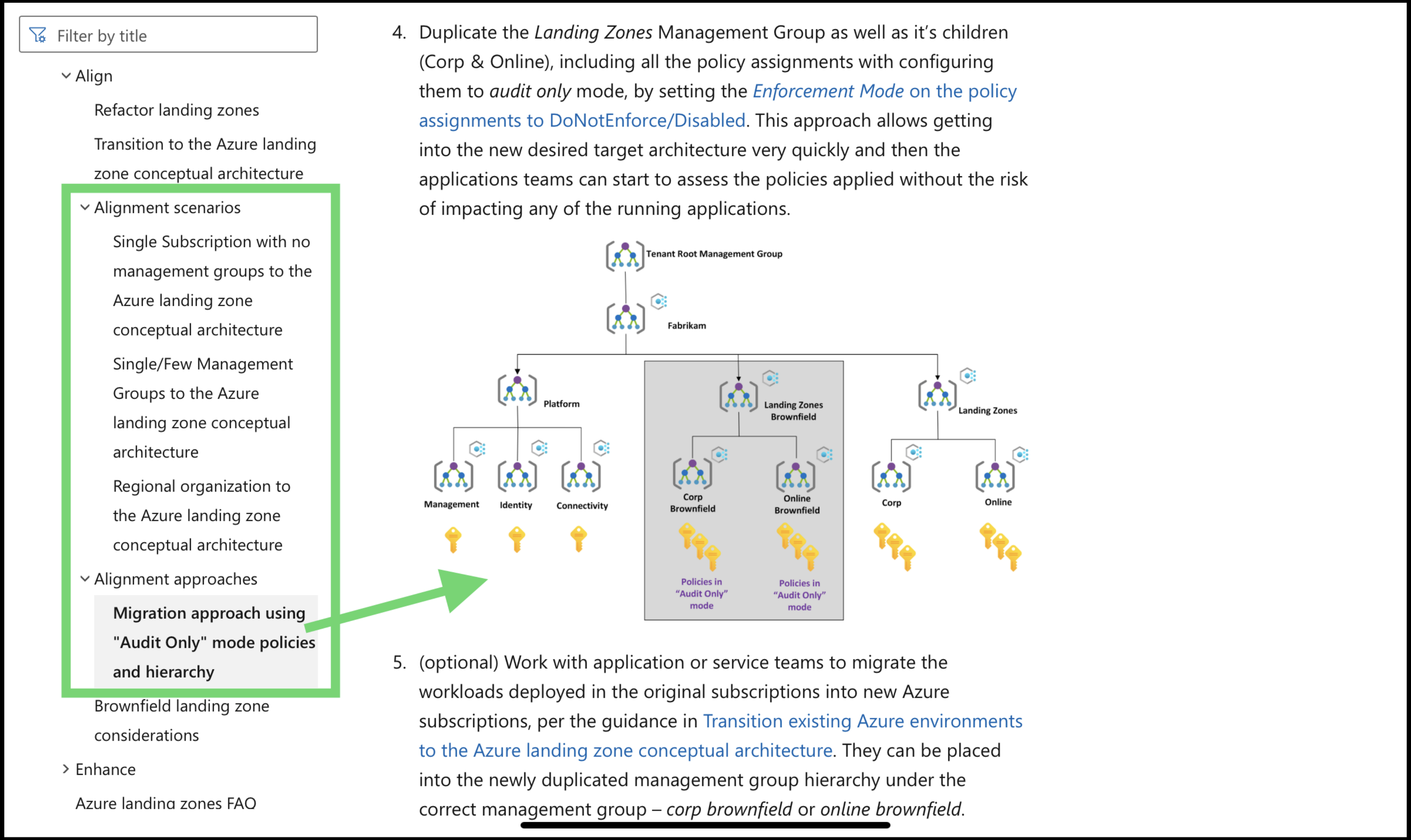
Design considerations:

Numerous IPAM tools are available for your consideration, depending on your requirements and the size of your organization. The options spans from having a basic Excel-based inventory to open-source community-driven solution or comprehensive enterprise products with advanced features and support.

- Consider these factors when evaluating what IPAM tool to implement:
  - Minimum features required by your organization
  - Total cost of ownership (TCO), including licensing and ongoing maintenance
  - Audit trails, logging, and role-based access controls
  - Authentication and authorization through Azure AD (Entra ID)
  - Accessible via API
  - Integrations with other network management tools and systems
  - Active community support or the level of support from the software provider
- Consider evaluating an open-source IPAM tool like Azure IPAM. Azure IPAM is a lightweight solution built on the Azure platform. It automatically discovers IP address utilization within your Azure tenant and enables you to manage it all from a centralized UI or via a RESTful API.

More Brownfield Guidance

Coming soon to CAF



Filter by title

- Align
  - Refactor landing zones
  - Transition to the Azure landing zone conceptual architecture
  - Alignment scenarios
    - Single Subscription with no management groups to the Azure landing zone conceptual architecture
    - Single/Few Management Groups to the Azure landing zone conceptual architecture
    - Regional organization to the Azure landing zone conceptual architecture
  - Alignment approaches
    - **Migration approach using "Audit Only" mode policies and hierarchy**
  - Brownfield landing zone considerations
- Enhance
- Azure landing zones FAQ

4. Duplicate the *Landing Zones* Management Group as well as it's children (Corp & Online), including all the policy assignments with configuring them to *audit only* mode, by setting the *Enforcement Mode* on the policy assignments to DoNotEnforce/Disabled. This approach allows getting into the new desired target architecture very quickly and then the applications teams can start to assess the policies applied without the risk of impacting any of the running applications.

5. (optional) Work with application or service teams to migrate the workloads deployed in the original subscriptions into new Azure subscriptions, per the guidance in Transition existing Azure environments to the Azure landing zone conceptual architecture. They can be placed into the newly duplicated management group hierarchy under the correct management group – *corp brownfield* or *online brownfield*.

ALZ Policy Refresh Latest

ALZ Policy Refresh

Update

- Focus for this quarter has been quality, security and stability
  - Policy Testing Framework established (quality and regression)
    - Pipeline tests for all assigned DENY policies – using Pester
  - Remediating policies and assignments using `Owner` RBAC role as far as possible to least privilege (3 policies and 7 assignments)
    - Some security related policies require `Owner`
  - Policy improvements and bug fixes:
    - E.g., adding evaluation delay for SQL MI TLS policy because the resource takes 4 hours to deploy
  - Coverage:
    - Key Vault Guardrails assignment added to Platform Management Group as well
  - Documentation enhancements

Planning to merge the changes this week into the ALZ portal – Bicep & TF will follow in October

ALZ Policy Refresh

Looking Forward

- Planning for large policy updates - diagnostic settings v2, **versioning**, Defender for Cloud, Azure Monitor Baseline Alerts

Ask

- Submit Azure Policy suggestions and issues on GitHub
  - These must be policies that all customers across all industries/countries/verticals would benefit from

Relevant Links

- Official Release: aka.ms/alz/whatsnew and aka.ms/alz/policies

AzAdvertizer Updates

AMBA Updates

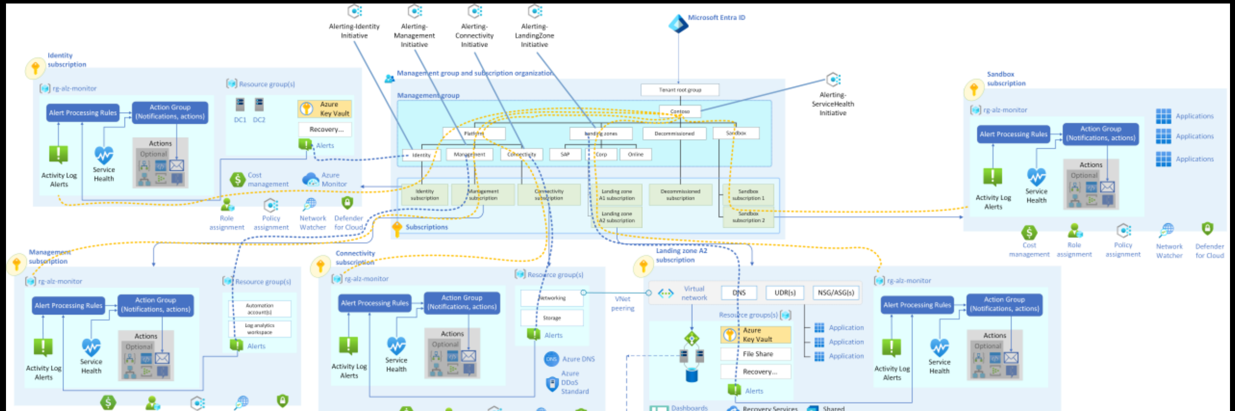
https://aka.ms/alz/monitor/repo → https://aka.ms/amba/alz

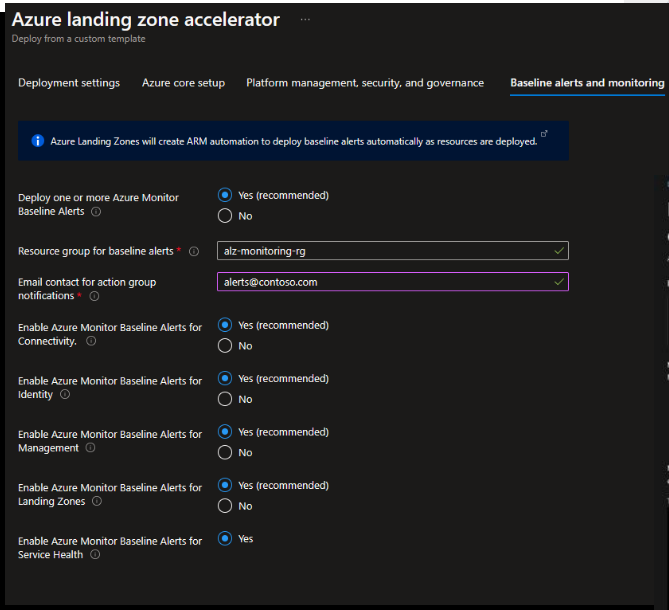
Azure Monitor Baseline Alerts (AMBA) – GA very soon…

Updates:

- We are moving to https://aka.ms/amba ~ Sept/Oct 2023
- Portal integration into ALZ coming soon (TF and Bicep to follow)
- CAF Documentation is out https://aka.ms/amba/alz/docs
- New detailed and downloadable AMBA Visio diagram
- We are part of https://learn.microsoft.com/en-us/training/technical-support/intro-to-azure-incident-readiness/
- We have released a YouTube Azure Enablement Show video https://aka.ms/alz/monitor/video
- Working closely with Service Health team regarding enhancements to alerting at scale

https://aka.ms/alz/monitor/repo → https://aka.ms/amba/alz





Azure landing zone accelerator

Deploy from a custom template

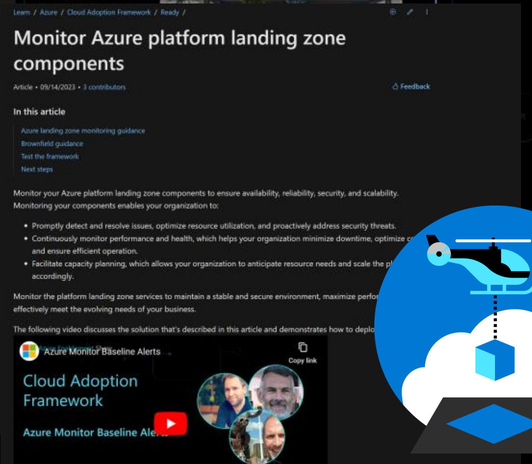
Deployment settings
Azure core setup
Platform management, security, and governance
Baseline alerts and monitoring

Azure Landing Zones will create ARM automation to deploy baseline alerts automatically as resources are deployed.

Deploy one or more Azure Monitor Baseline Alerts	● Yes (recommended) ○ No
Resource group for baseline alerts *	alz-monitoring-rg
Email contact for action group notifications	alerts@contoso.com
Enable Azure Monitor Baseline Alerts for Connectivity	● Yes (recommended) ○ No
Enable Azure Monitor Baseline Alerts for Identity	● Yes (recommended) ○ No
Enable Azure Monitor Baseline Alerts for Management	● Yes (recommended) ○ No
Enable Azure Monitor Baseline Alerts for Landing Zones	● Yes (recommended) ○ No
Enable Azure Monitor Baseline Alerts for Service Health	● Yes

Microsoft Azure @Azure

Accelerate your observability journey and adoption of Azure Monitor by learning how to set up baseline alerts: msft.it/60109GwYo #AzureEnablementShow



Learn / Azure / Cloud Adoption Framework / Ready /

Monitor Azure platform landing zone components

Article • 09/14/2023 • 3 contributors

Feedback

In this article

- Azure landing zone monitoring guidance
- Brownfield guidance
- Test the framework
- Next steps

Monitor your Azure platform landing zone components to ensure availability, reliability, security, and scalability. Monitoring your components enables your organization to:

- Promptly detect and resolve issues, optimize resource utilization, and proactively address security threats.
- Continuously monitor performance and health, which helps your organization minimize downtime, optimize c and ensure efficient operation.
- Facilitate capacity planning, which allows your organization to anticipate resource needs and scale the pl accordingly.

Monitor the platform landing zone services to maintain a stable and secure environment, maximize perfor effectively meet the evolving needs of your business.

The following video discusses the solution that's described in this article and demonstrates how to deplo

ALZ Bicep Updates

ALZ Bicep Updates

V0.16.3

NOW LIVE!

Policies

- Latest from Upstream ALZ Repo Refresh

ALZ Bicep Accelerator

- What-If now enabled on PR workflows
- Pipelines for Management Group Diagnostic Settings, now registers required RP
- Exposed line endings function in ALZ PowerShell module for use in customizing policies

Other enhancements

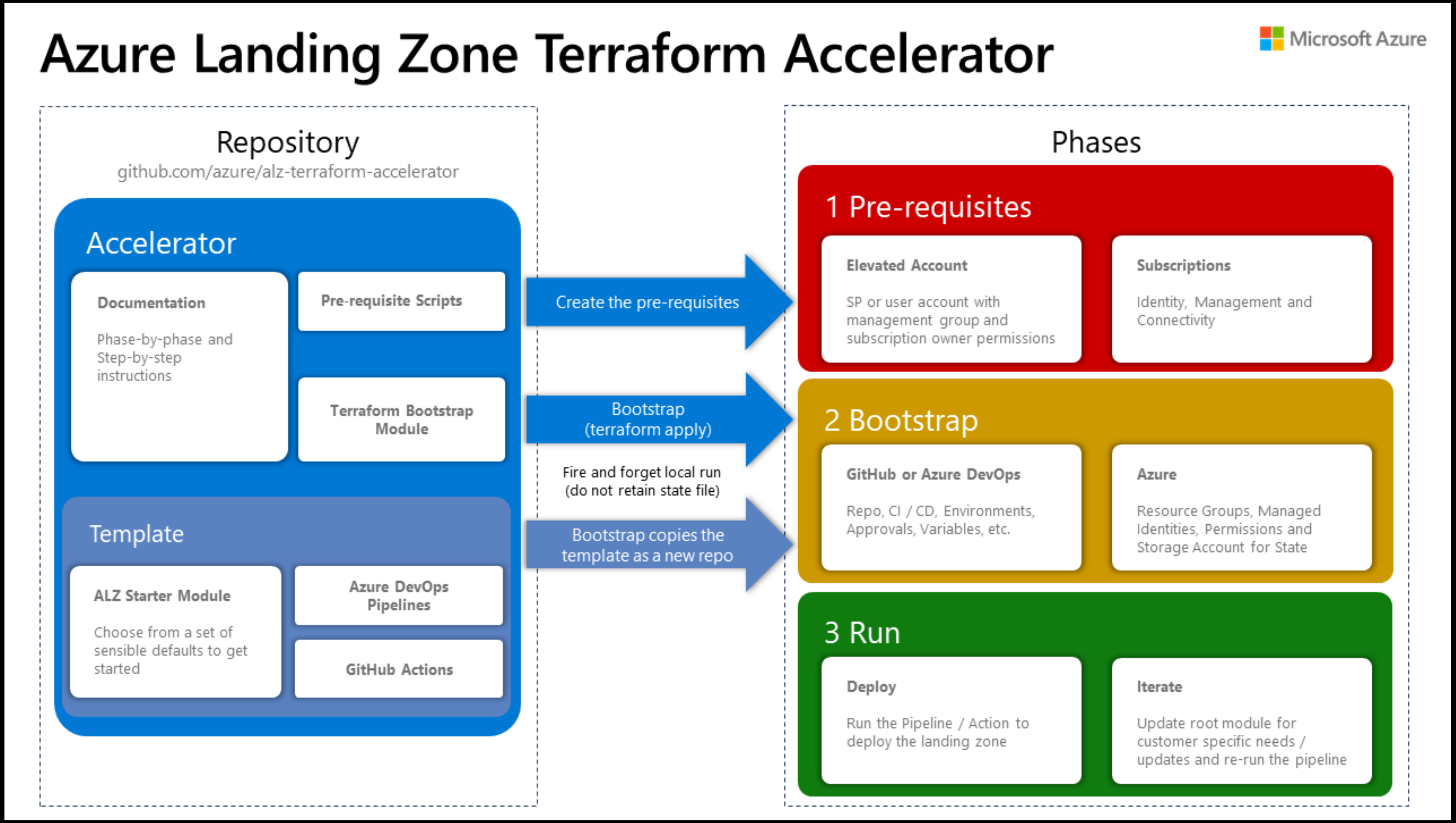
- Bastion
  - Bastion NSG now only deploys when Bastion is deployed 🐞
  - Bastion Native Client/Tunnelling Now Supported
- Virtual WAN
  - VWAN Routing Intent now supported
  - VWAN 'enableInternetSecurity' property now able to be set
  - Now able to customize name of VWAN Hub Connections
- Simplified linting rules config (bicepconfig.json)
- Migrated to new Sentinel simplified pricing tier

ALZ Terraform Updates

Modules, modules, modules

- Hub networking - Azure/hubnetworking/azurerm | Terraform Registry
- Vnet gateway - Azure/vnet-gateway/azurerm | Terraform Registry
- VWAN - https://github.com/Azure/terraform-azurerm-vwan
- ALZ Management - Azure/alz-management/azurerm | Terraform Registry

```
provider "alz" {}
```



Azure Landing Zone Terraform Accelerator

Microsoft Azure

Repository

github.com/azure/alz-terraform-accelerator

Accelerator

Documentation

Phase-by-phase and Step-by-step instructions

Pre-requisite Scripts

Terraform Bootstrap Module

Template

ALZ Starter Module

Choose from a set of sensible defaults to get started

Azure DevOps Pipelines

GitHub Actions

Create the pre-requisites

Bootstrap (terraform apply)

Fire and forget local run (do not retain state file)

Bootstrap copies the template as a new repo

Phases

1 Pre-requisites

Elevated Account

SP or user account with management group and subscription owner permissions

Subscriptions

Identity, Management and Connectivity

2 Bootstrap

GitHub or Azure DevOps

Repo, CI / CD, Environments, Approvals, Variables, etc.

Azure

Resource Groups, Managed Identities, Permissions and Storage Account for State

3 Run

Deploy

Run the Pipeline / Action to deploy the landing zone

Iterate

Update root module for customer specific needs / updates and re-run the pipeline

- Opinionated bootstrapping of the ALZ Terraform Module
- Supports GitHub and Azure DevOps
- PowerShell module prompts for inputs
- Initially 2 starter module choices
- Advanced scenarios and subscription vending on the roadmap

Call to Action

Try it out and give us feedback in the issues section

WARNING v0.0.X!

https://aka.ms/alz/terraform/accelerator

HashiConf

San Francisco & Online | October 10-12, 2023

Get in the (Landing) Zone with Terraform on Azure

(thanks Luke Taylor for the title!)

Subscription Vending Updates

Subscription Vending Updates

Terraform

Bicep

- User Assigned Managed Identity & OIDC support added
- Ability to register RPs and features added
- VWAN Routing Intent support added
- Manage Network Watcher RG
- Coming Soon:

  Create subscription directly under target MG

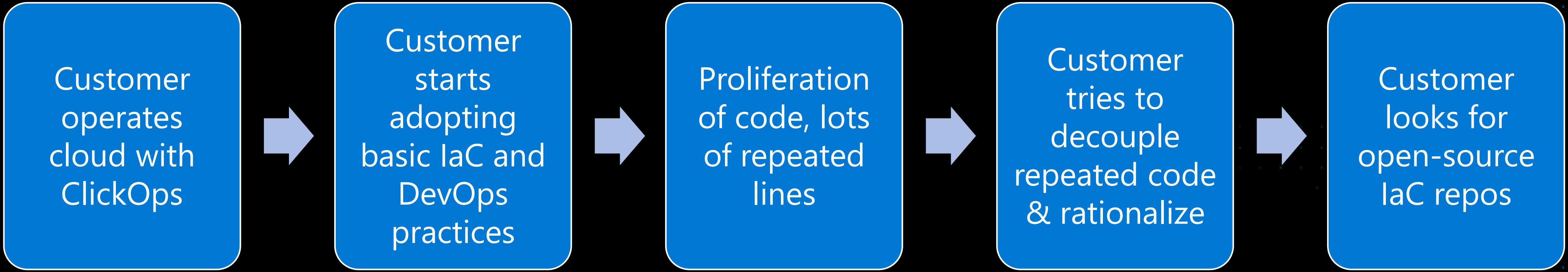
  One-way VNET peering
- Reduced RBAC requirements for "deployments" at "/" scope – only require on MG scope now
- Metadata changes made to support BRM changes
- Added 2 optional parameters for MCA Multi-Tenant scenarios

Microsoft

Azure Verified Modules (AVM)

IaC Module Strategy across Microsoft for Bicep & Terraform

Problem Statement from our Customers



Customer operates cloud with ClickOps

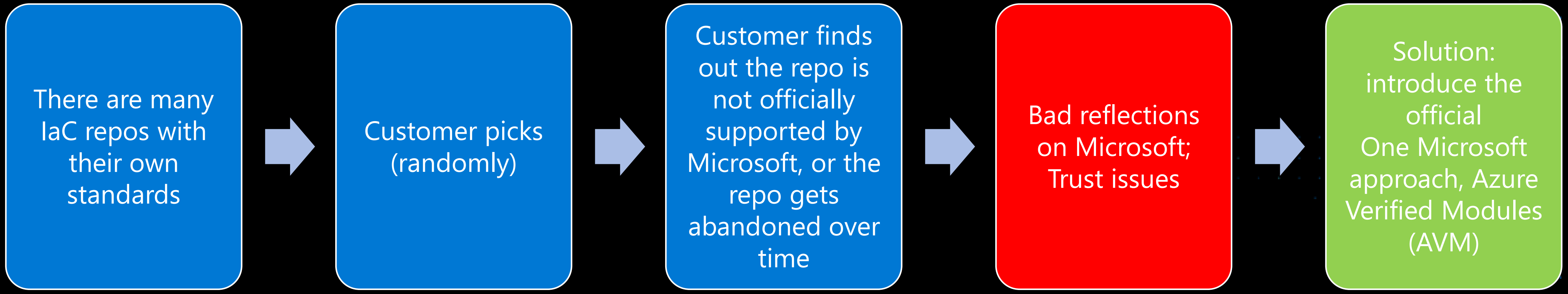
Customer starts adopting basic IaC and DevOps practices

Proliferation of code, lots of repeated lines

Customer tries to decouple repeated code & rationalize

Customer looks for open-source IaC repos

Problem Statement Continued…



There are many IaC repos with their own standards

Customer picks (randomly)

Customer finds out the repo is not officially supported by Microsoft, or the repo gets abandoned over time

Bad reflections on Microsoft; Trust issues

Solution: introduce the official One Microsoft approach, Azure Verified Modules (AVM)

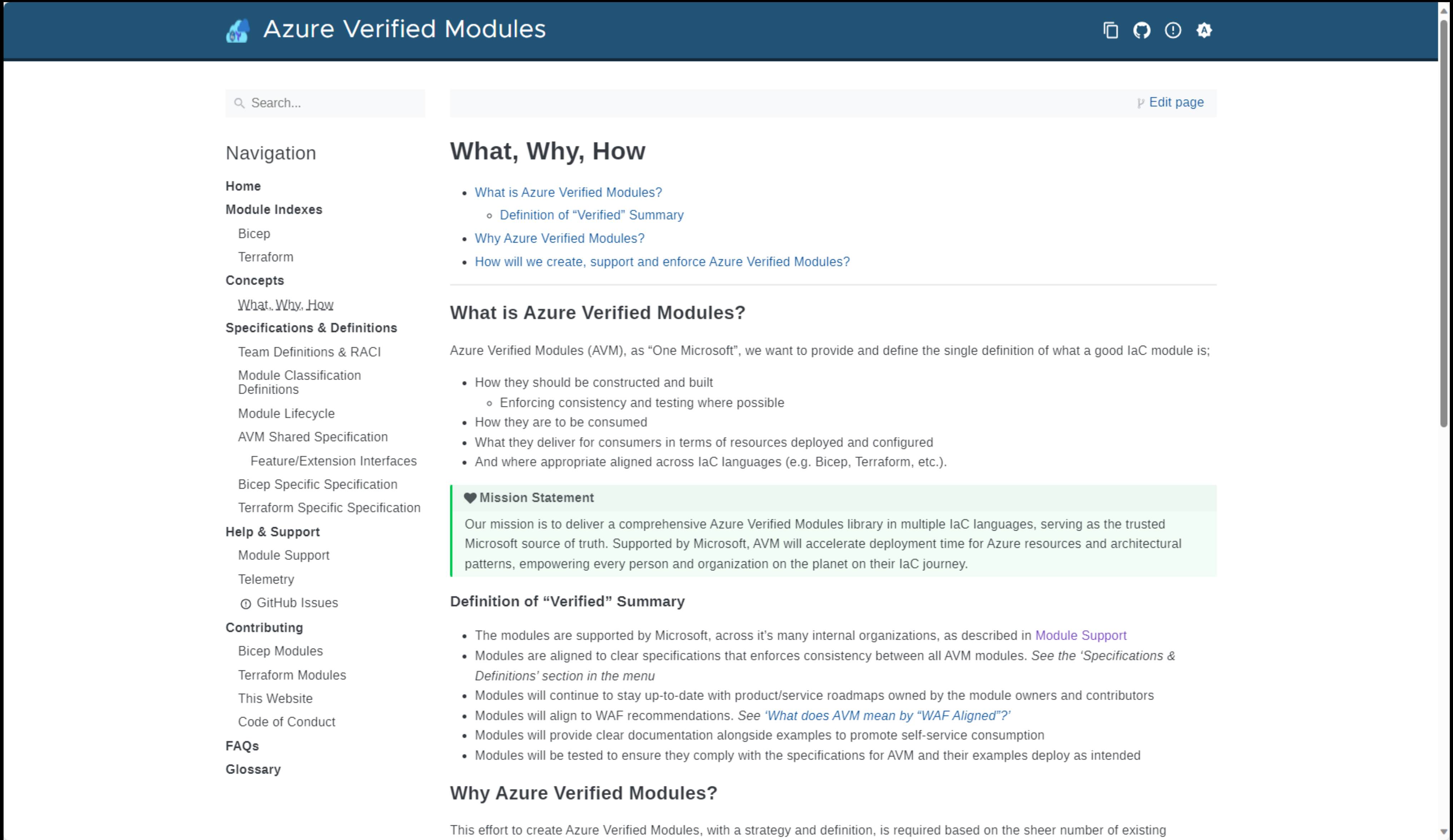
What is our mission?

“Our mission is to deliver a **comprehensive Azure Verified Modules library** in **multiple IaC languages**, serving as the **trusted Microsoft source of truth**.

Supported by Microsoft, AVM will **standardize and accelerate the deployment** of Azure **resources** and **architectural patterns**, empowering every person and organization on the planet on their IaC journey.”

Provide common IP for our Customers, Partners and Microsoft

https://aka.ms/AVM



Navigation

- **Home**
- **Module Indexes**
  - Bicep
  - Terraform
- **Concepts**
  - What, Why, How
- **Specifications & Definitions**
  - Team Definitions & RACI
  - Module Classification Definitions
  - Module Lifecycle
  - AVM Shared Specification
    - Feature/Extension Interfaces
  - Bicep Specific Specification
  - Terraform Specific Specification
- **Help & Support**
  - Module Support
  - Telemetry
  - GitHub Issues
- **Contributing**
  - Bicep Modules
  - Terraform Modules
  - This Website
  - Code of Conduct
- **FAQs**
- **Glossary**

What, Why, How

- What is Azure Verified Modules?
  - Definition of "Verified" Summary
- Why Azure Verified Modules?
- How will we create, support and enforce Azure Verified Modules?

What is Azure Verified Modules?

Azure Verified Modules (AVM), as "One Microsoft", we want to provide and define the single definition of what a good IaC module is;

- How they should be constructed and built
  - Enforcing consistency and testing where possible
- How they are to be consumed
- What they deliver for consumers in terms of resources deployed and configured
- And where appropriate aligned across IaC languages (e.g. Bicep, Terraform, etc.).

> **Mission Statement**
>
> Our mission is to deliver a comprehensive Azure Verified Modules library in multiple IaC languages, serving as the trusted Microsoft source of truth. Supported by Microsoft, AVM will accelerate deployment time for Azure resources and architectural patterns, empowering every person and organization on the planet on their IaC journey.

Definition of "Verified" Summary

- The modules are supported by Microsoft, across it's many internal organizations, as described in Module Support
- Modules are aligned to clear specifications that enforces consistency between all AVM modules. *See the 'Specifications & Definitions' section in the menu*
- Modules will continue to stay up-to-date with product/service roadmaps owned by the module owners and contributors
- Modules will align to WAF recommendations. *See 'What does AVM mean by "WAF Aligned"?'*
- Modules will provide clear documentation alongside examples to promote self-service consumption
- Modules will be tested to ensure they comply with the specifications for AVM and their examples deploy as intended

Why Azure Verified Modules?

This effort to create Azure Verified Modules, with a strategy and definition, is required based on the sheer number of existing

Asks from the field

Questions from the field

- **How do I make ALZ for my customer meet their regulatory compliance controls (e.g. PCI,-DSS etc.)?**
  - Security control mapping with Azure landing zones
  - Tailor the Azure landing zone architecture
  - Review built-in initiatives also review MDFC regulatory compliance (uses policy)
  - Remember that ALZ already assigns MCSB (ASB) to the Intermediate Root MG
- **What resource providers need to be registered for ALZ subscriptions?**
  - We are working on a user story, this month, to publish this info to the wiki for guidance per subscription (e.g. Management, Connectivity, Identity, and LZ subs etc.) ✍

Questions to the field

- **Enable DDoS on vNets Policy RBAC Challenges**

- **Are you being asked about multi-region ALZ support by your customers/partners?**
  - If so, what are they asking for specifically?
  - Do we have gaps in tooling?
  - Something else?

Microsoft

Q & A

Next Community Call will be in December 👍

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

Stay tuned to issue #1431 (ALZ/ESLZ Repo)

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

Microsoft

This month's presenters:

Thank You!

Stay up-to-date:

https://aka.ms/ALZ/WhatsNew