Azure Verified Modules (AVM)

Community Call, 6th February 2025

Speakers:

Microsoft: Charlie Grabiaud, Jared Holgate, Matt White, Jack Tracey, Alexander Sehr, Erika Gressi, Máté Barabás, Pankaj Meshram, René Hézser.

External: Brett Miller (Capgemini), Mohammad Reza Gashtil (NTT), Maik Wendt (NTT)

When you join this event, your name, email address and/or phone number may be viewable by other session participants in the attendee list. By joining, you're agreeing to this experience.

Also, this event will be recorded and shared publicly with others, including Microsoft's global customers, partners, employees, and service providers. The recording may include your name and any questions you submit to Q&A.

This meeting is being recorded

Meet the AVM Core Team

Technical SME's

Alex

Bilal

Chris

Erika

Jack

Jared

Jon

Matt

Rainer

Sebastian

René

PM's

Charlie

Máté

Pankaj

Agenda

- AVM Website update (*Mate*)
- Child Modules (*Alex & Jared*)
- Bicep AVM - OpenID Connect update (*Erika*)
- WIP – an inner-sourcing journey for Bicep AVM (*Brett Miller* – MVP + *Jack* hosting)
- Terraform AVMs for Platform Landing Zone (ALZ) – *Jared*
- Migrating to OR refactoring existing TF code to AVM modules – *Matt*
- Bicep AVMs for Platform Landing Zone (ALZ) – *Jack*
- Customer experience sharing with NTT (*NTT* + *Pankaj* hosting)
- Upcoming Bicep & Terraform updates – *René*
- Q & A

Microsoft

AVM Website update

Máté Barabás

https://www.youtube.com/watch?v=ifDba74rdG8

Microsoft

Child Modules

Alexander Sehr & Jared Holgate

Child Modules - Bicep

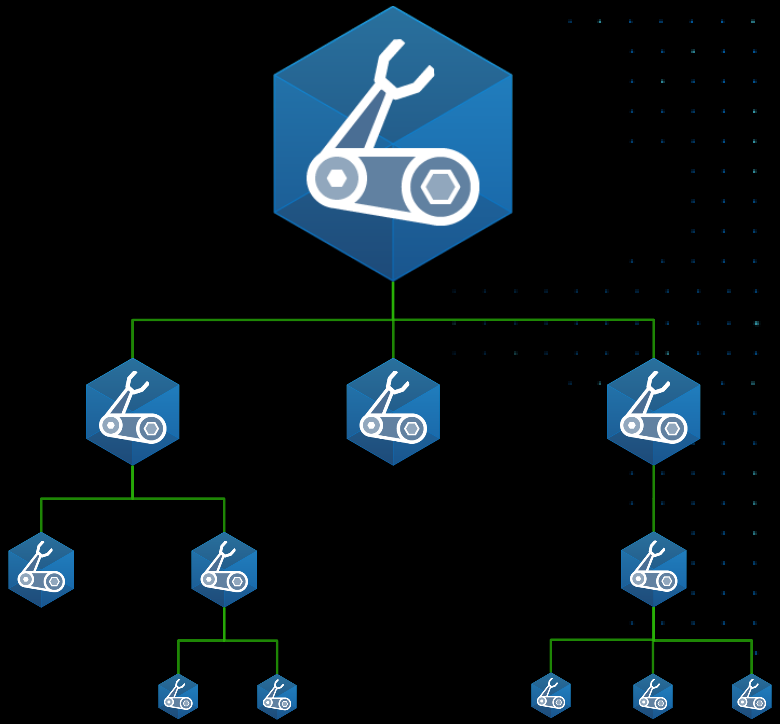
In active development 🔬

Phases

1. 🧪 PoC: Enablement
2. 🛫 Pilot: Selected publishing
3. 🌊 Bulk: General availability

Remaining challenges

- Validation against MAR file
- Scalable approach towards onboarding



Child Modules - Terraform

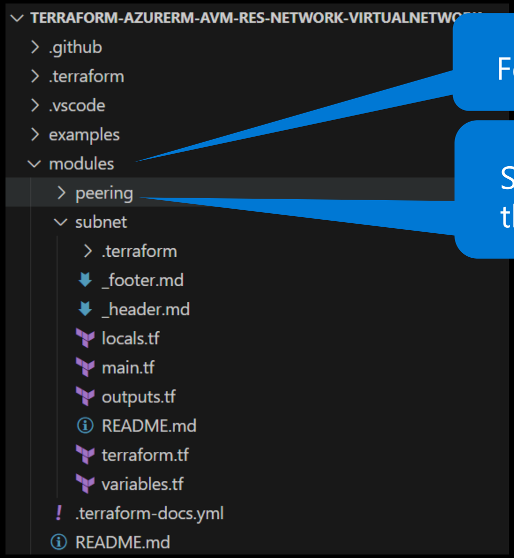
Ready to use today

Status

1. 🔬 Tested on existing modules ✔
2. 🧪 CI / Test framework updated ✔
3. 🛫 Documentation updated ❌
4. 🌊 Can use it now ✔

Usage Constraints

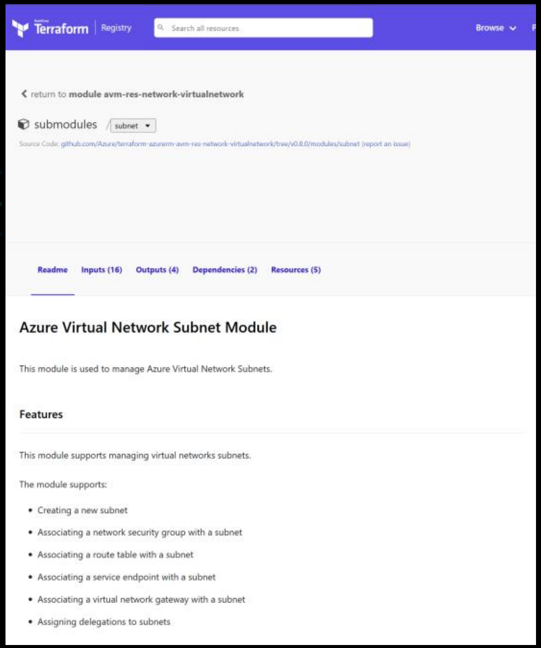
- Must only be used for true child resources
- Should create submodule for child resources
- Must follow standard interfaces and outputs
- Must be referenced from parent module
- Should be an optional variable
- Can be referenced directly from registry



```
TERRAFORM-AZURERM-AVM-RES-NETWORK-VIRTUALNETWO
  > .github
  > .terraform
  > .vscode
  > examples
  v modules
    > peering
    v subnet
      > .terraform
        _footer.md
        _header.md
        locals.tf
        main.tf
        outputs.tf
        README.md
        terraform.tf
        variables.tf
    .terraform-docs.yml
    README.md
```

Folder name must be "modules"

Subfolder name is the name of the submodule



‹ return to **module avm-res-network-virtualnetwork**

submodules / subnet ▾

Source Code: github.com/Azure/terraform-azurerm-avm-res-network-virtualnetwork/tree/v0.8.0/modules/subnet (report an issue)

Azure Virtual Network Subnet Module

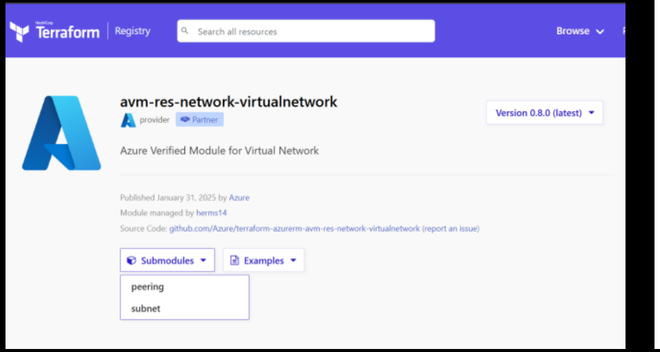
This module is used to manage Azure Virtual Network Subnets.

Features

This module supports managing virtual networks subnets.

The module supports:

- Creating a new subnet
- Associating a network security group with a subnet
- Associating a route table with a subnet
- Associating a service endpoint with a subnet
- Associating a virtual network gateway with a subnet
- Assigning delegations to subnets



avm-res-network-virtualnetwork

provider Partner

Version 0.8.0 (latest) ▾

Azure Verified Module for Virtual Network

Published January 31, 2025 by Azure

Module managed by herms14

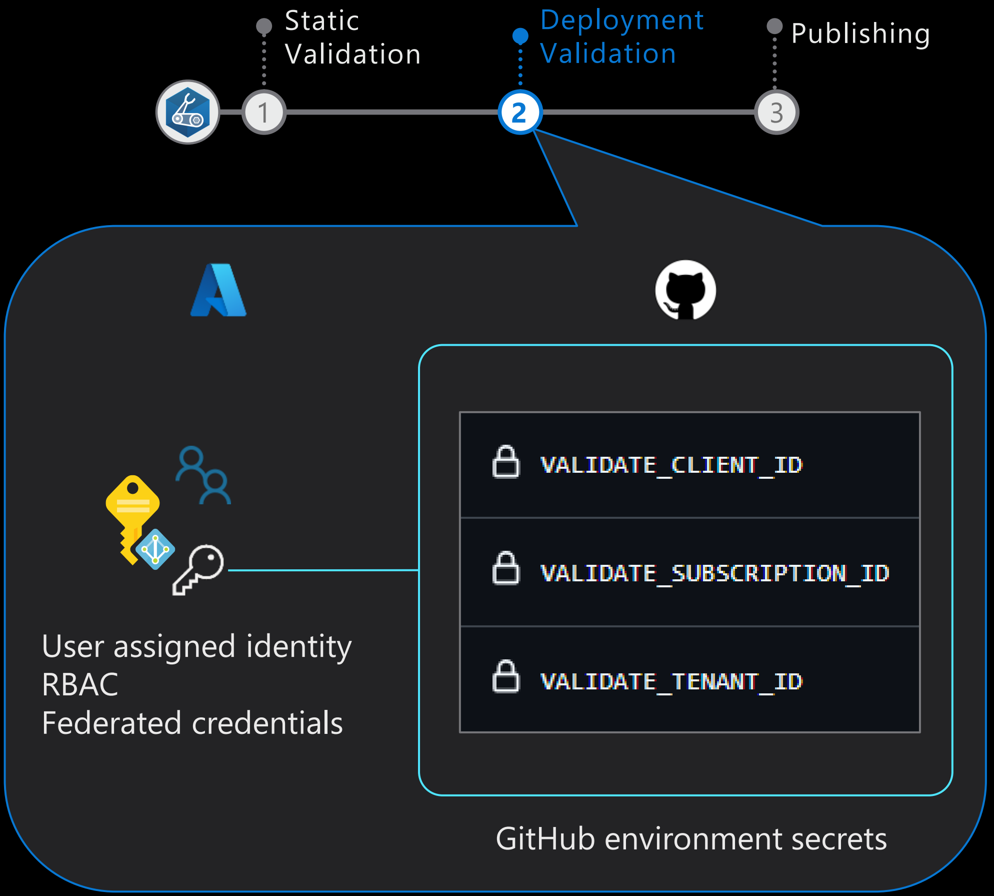
Source Code: github.com/Azure/terraform-azurerm-avm-res-network-virtualnetwork (report an issue)

Microsoft

Bicep AVM – OpenID Connect update

Erika Gressi

Bicep AVM – OpenID Connect update



Static Validation

Deployment Validation

Publishing

1

2

3

User assigned identity
RBAC
Federated credentials

VALIDATE_CLIENT_ID

VALIDATE_SUBSCRIPTION_ID

VALIDATE_TENANT_ID

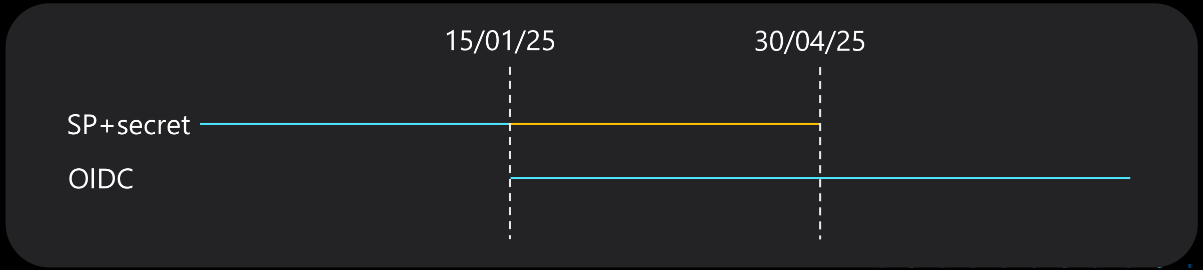
GitHub environment secrets

Adoption guidelines

1. 🖐 ClickOps - Bicep contribution step-by-step
2. 🦥 Automation - PowerShell Helper Script

Authentication method support

- 15 Jan 25: Introducing OIDC
  - Deprecating Service Principal + secret
- 30 Apr 25: Breaking change
  - Decommissioning Service Principal + secret



WIP – an inner-sourcing journey for Bicep AVM

Jack Tracey

Brett Miller
MVP, Capgemini

Internalising Microsoft-provided AVM modules for governance, customisation, applying open-source practices to foster innovation within an organisation.

Security

Pulling changes into your own container registry allows you to run tests ensuring quality and security practices are incorporated.

Reliability

Write your own tests and incorporate security standards and compliance from the beginning.

Risk Reduction

You have full control over lifecycle and retain ownership of modules, even if they originated publicly to start.

Increased collaboration

Enable other people/teams to contribute in an Agile way.

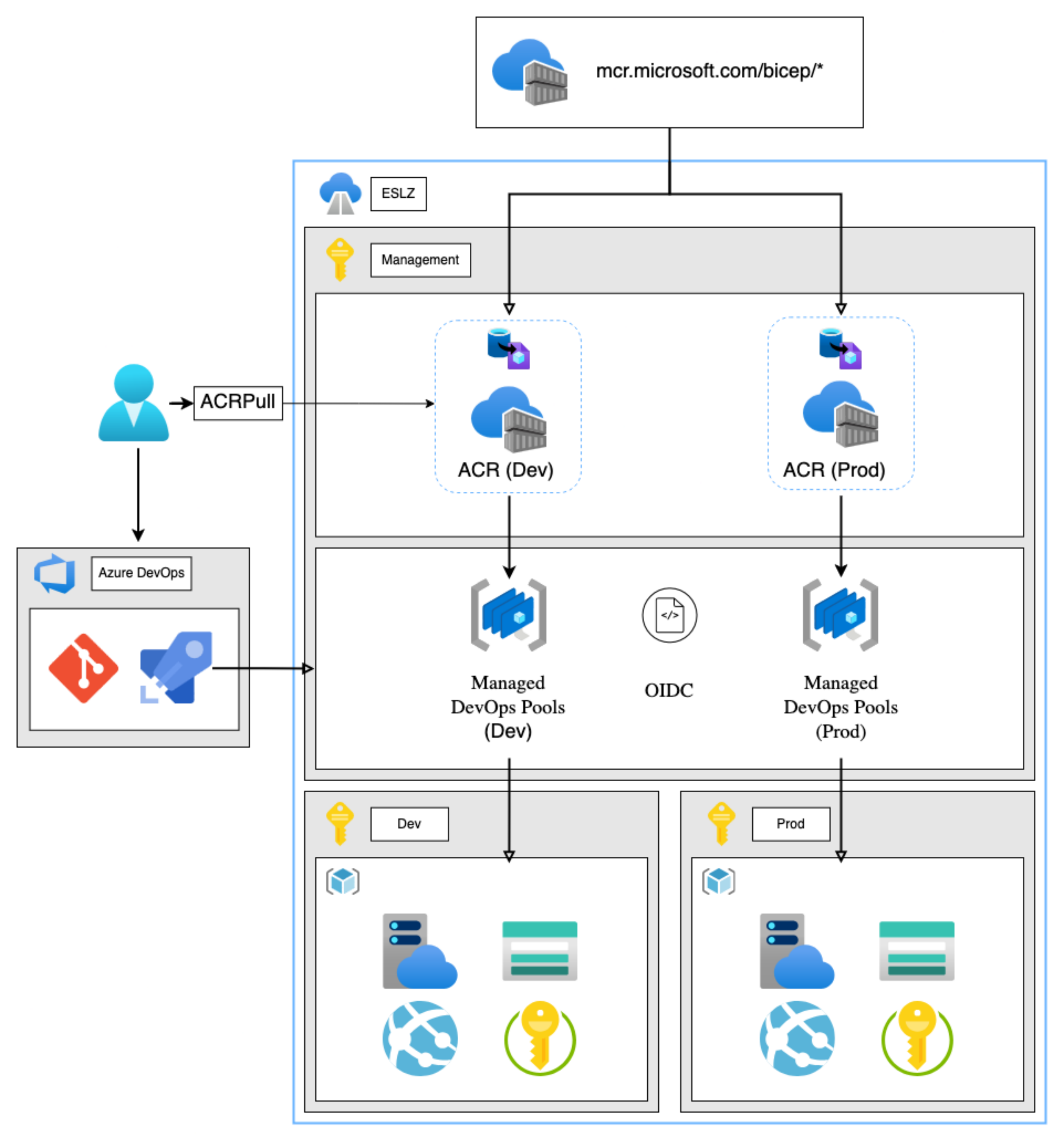
Ensures everyone is responsible for the standard of code.

Self-service

Accelerate innovation with built-in governance and control.

Reduce load on platform teams

[Enterprise infrastructure as code using Bicep and Azure Container Registry]


mcr.microsoft.com/bicep/*
ESLZ
Management
ACRPull
ACR (Dev)
ACR (Prod)
Azure DevOps
Managed DevOps Pools (Dev)
OIDC
Managed DevOps Pools (Prod)
Dev
Prod

Microsoft

Terraform Azure Verified Modules for Platform Landing Zone (ALZ)

Jared Holgate

New branding

Terraform Azure Verified Modules for Platform Landing Zones (ALZ)

Azure Verified Modules for Platform Landing Zone (ALZ)

Management Groups and Policy

avm-ptn-alz

- ✓ Management Group Hierarchy
- ✓ Policy Definitions and Assignments
- ✓ Role Assignments

Management Resources

avm-ptn-alz-management

- ✓ Log Analytics Workspace
- ✓ Data Collection Rules
- ✓ Managed Identities

Connectivity

Hub and Spoke Virtual Network

avm-ptn-hubnetworking
avm-ptn-vnetgateway
avm-ptn-network-private-link-private-dns-zones

- ✓ Virtual Networks
- ✓ Mesh Peering and Routing
- ✓ Firewalls
- ✓ Express Route and VPN Gateways
- ✓ Bastion Hosts
- ✓ Private DNS and Resolvers

OR

Virtual WAN

avm-ptn-virtualwan
avm-ptn-network-private-link-private-dns-zones

- ✓ Virtual WAN
- ✓ Secure Virtual Hubs and Sidecars
- ✓ Firewalls
- ✓ Express Route and VPN Gateways
- ✓ Bastion Hosts
- ✓ Private DNS and Resolvers

Rationale

Our largest customers said they wanted a more modular approach

Reaching the limits of what we can do with a Terraform Module

Accelerator provides the same opinionated but configurable approach than the old module, but with the benefit of CI/CD and SCM.

Two approaches

Accelerator

Recommended and supported through the VBD program

Uses the modules that we have produced

Do it yourself

Advanced

Not covered here, but documented

Here be dragons

Benefits

The provider

Ensures your hierarchy is deployable before you start

Correctly calculates the role assignments required

The Library

Super easy to add AMBA-ALZ, or other additions to your landing zones

Single source of truth for ALZ

Updates decoupled from the module and provider

Automatically generated documentation

The ALZ module

More reliable deployments thanks to retriable errors

Faster deployments thanks to AzAPI

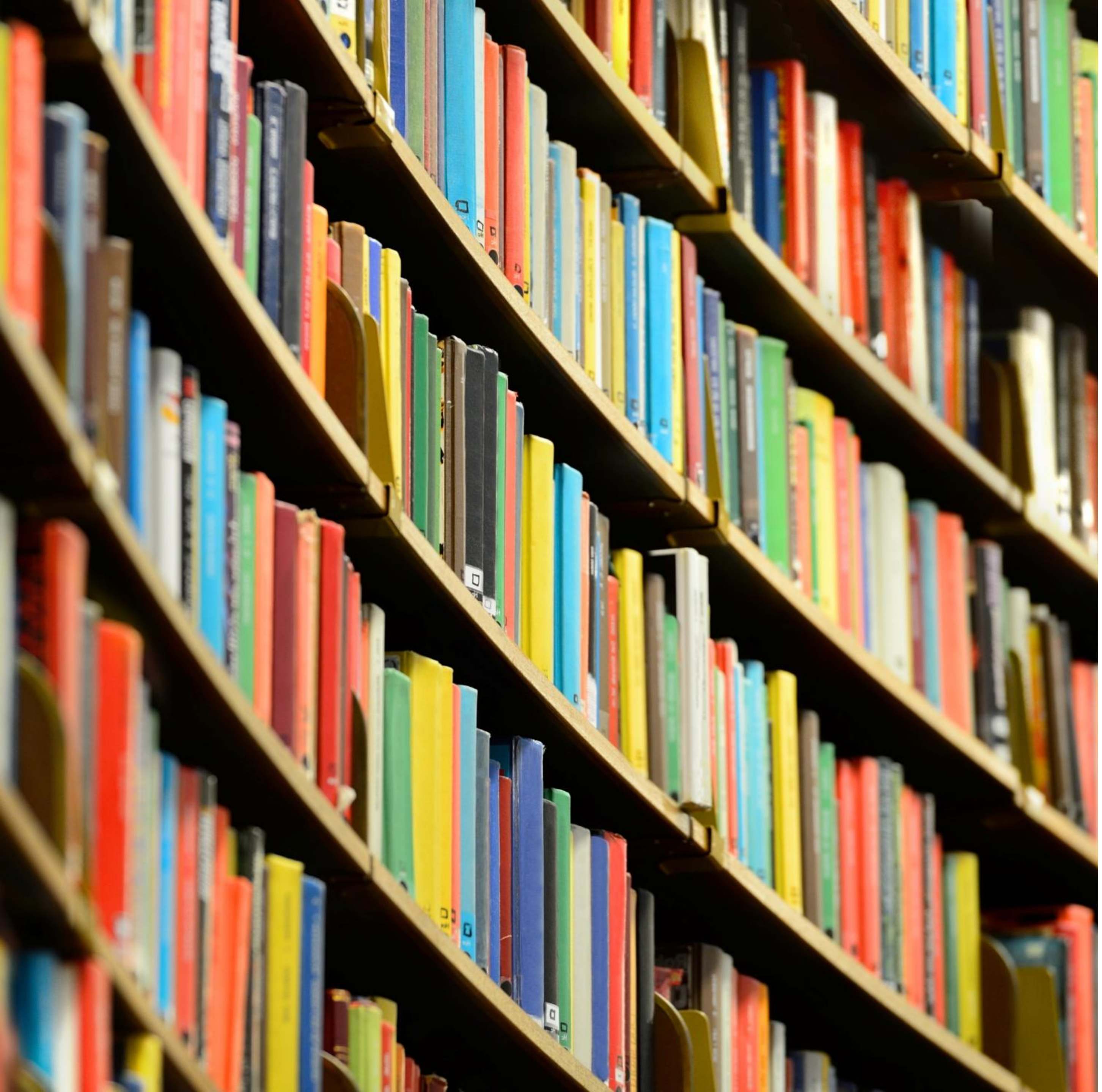
Accelerator

New features:

Bastion

DNS Resolver

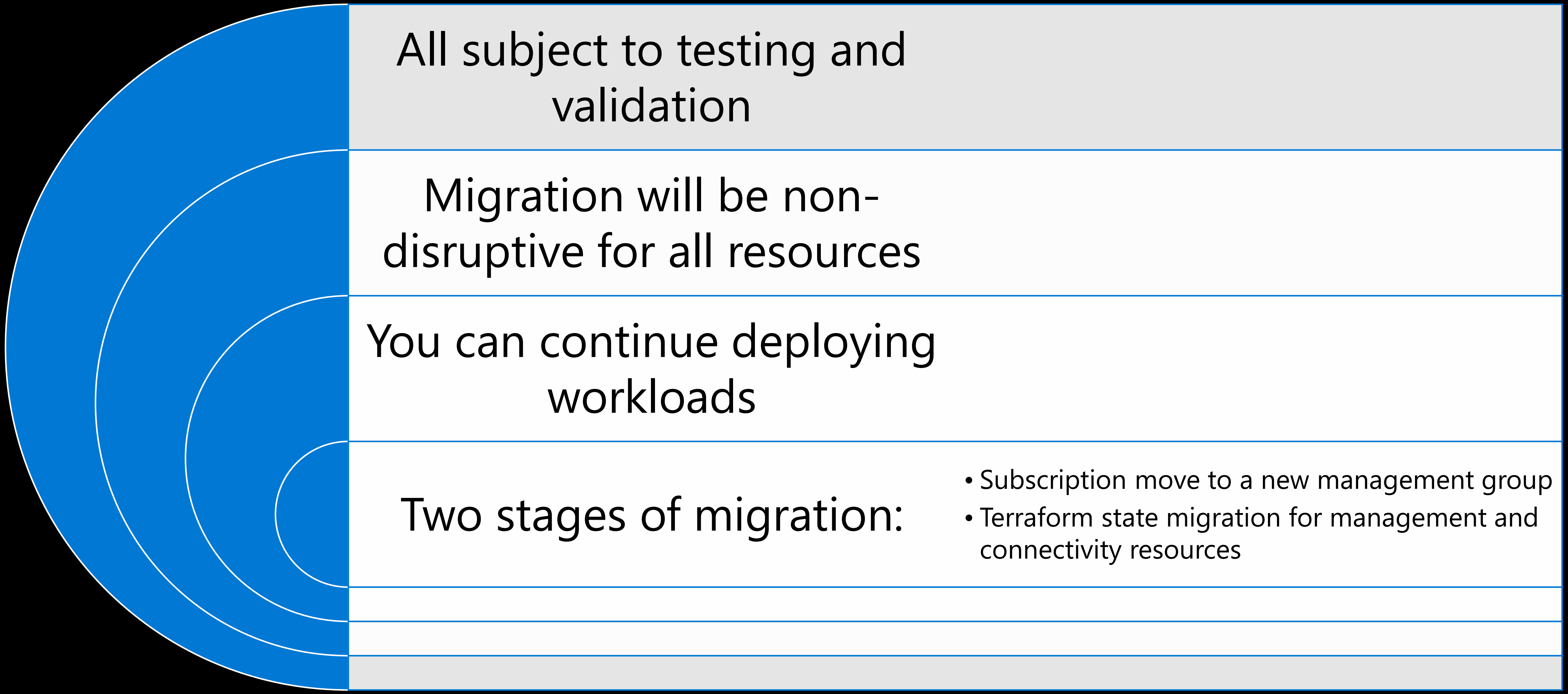
More coming…



Library

- One source of truth for ALZ, AMBA-ALZ Pattern, etc.
- Hosted in GitHub Documentation site
- A place to store Azure Landing Zones architectural data, including policies
- Extensible
- Agnostic to the implementation, we plan for the next version of ALZ Bicep to use this as a source

Proposed Migration Approach



All subject to testing and validation

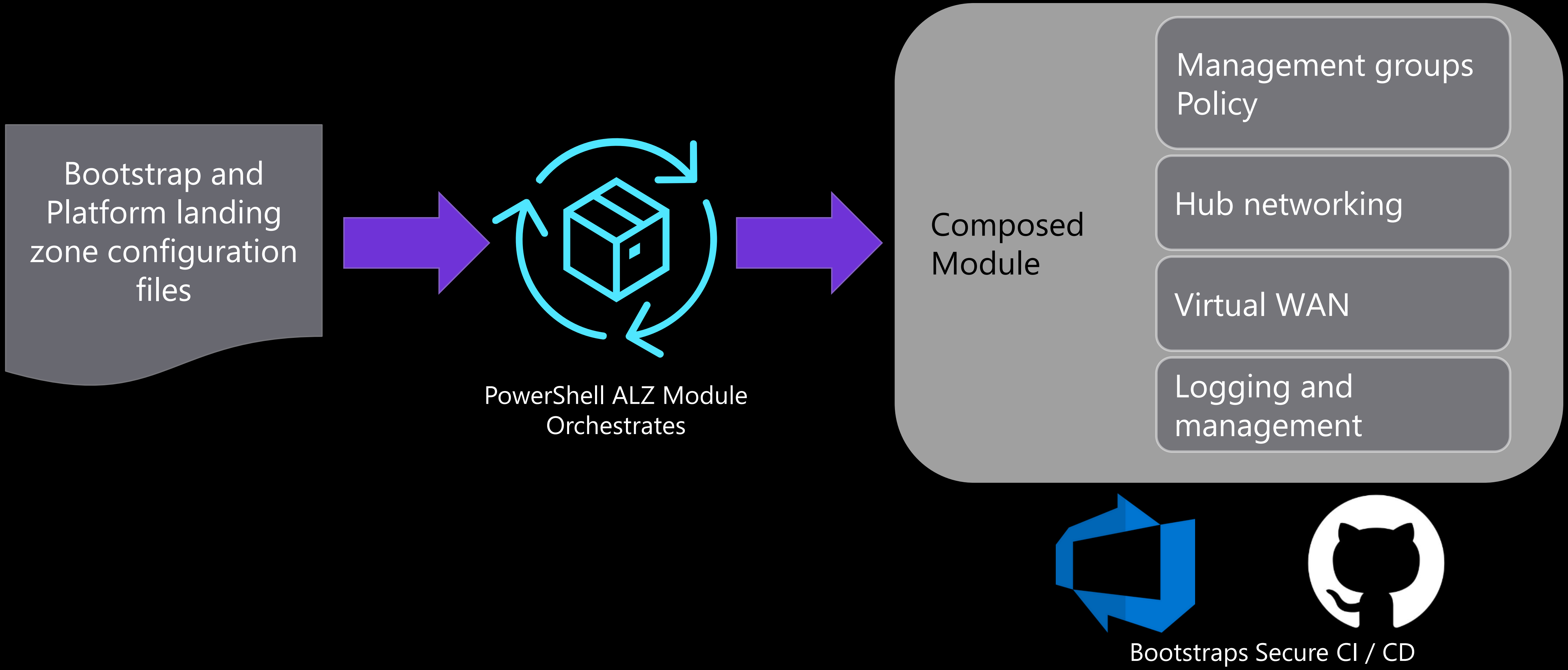
Migration will be non-disruptive for all resources

You can continue deploying workloads

Two stages of migration:

- Subscription move to a new management group
- Terraform state migration for management and connectivity resources

The ALZ IaC Accelerator – the solution for customers that want a simplified experience



Bootstrap and Platform landing zone configuration files

PowerShell ALZ Module Orchestrates

Composed Module

Management groups Policy

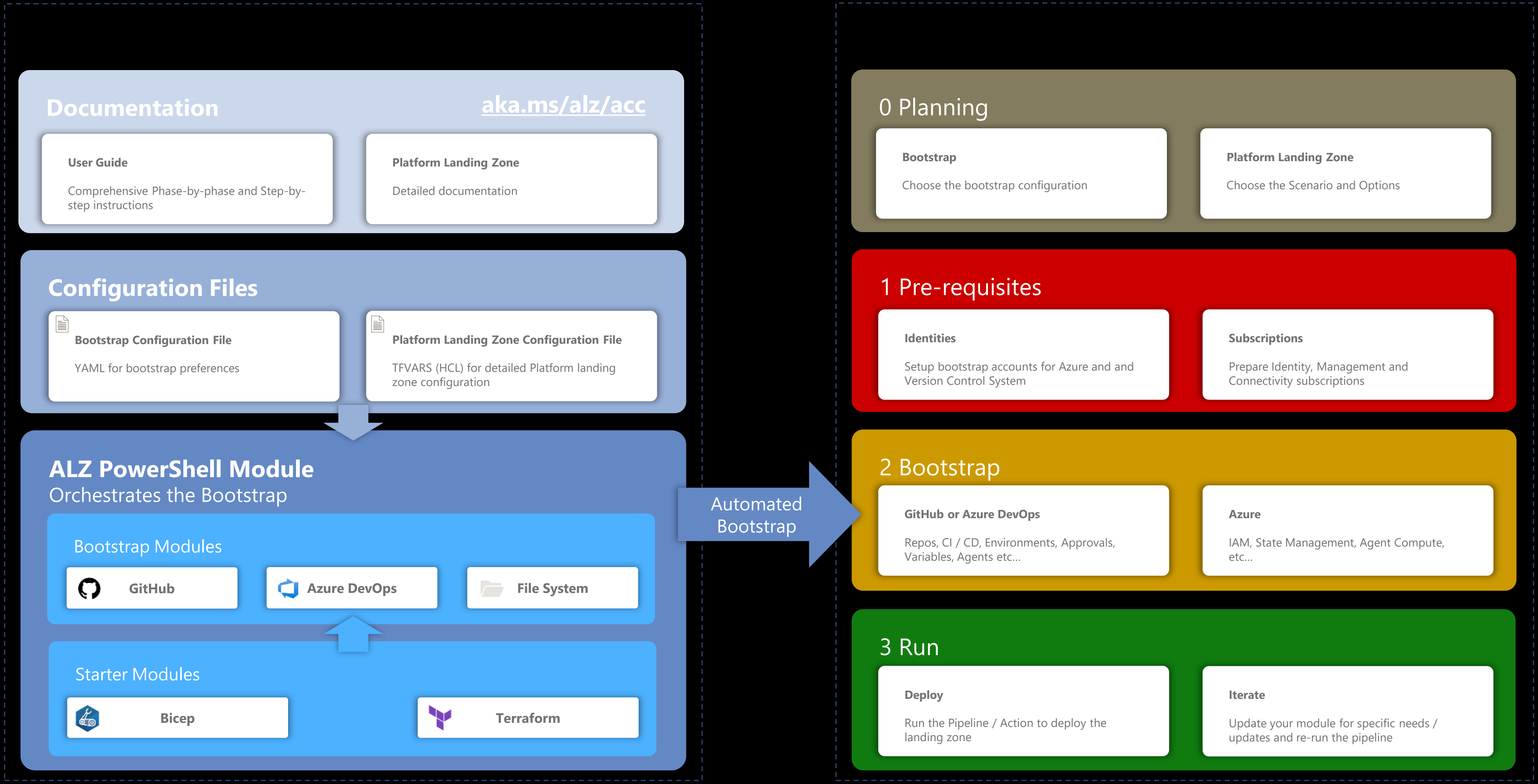
Hub networking

Virtual WAN

Logging and management

Bootstraps Secure CI / CD

Azure Landing Zones IaC Accelerator



Documentation

aka.ms/alz/acc

User Guide

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

Platform Landing Zone

Detailed documentation

Configuration Files

Bootstrap Configuration File

YAML for bootstrap preferences

Platform Landing Zone Configuration File

TFVARS (HCL) for detailed Platform landing zone configuration

ALZ PowerShell Module

Orchestrates the Bootstrap

Bootstrap Modules

- GitHub
- Azure DevOps
- File System

Starter Modules

- Bicep
- Terraform

Automated Bootstrap

0 Planning

Bootstrap

Choose the bootstrap configuration

Platform Landing Zone

Choose the Scenario and Options

1 Pre-requisites

Identities

Setup bootstrap accounts for Azure and and Version Control System

Subscriptions

Prepare Identity, Management and Connectivity subscriptions

2 Bootstrap

GitHub or Azure DevOps

Repos, CI / CD, Environments, Approvals, Variables, Agents etc...

Azure

IAM, State Management, Agent Compute, etc...

3 Run

Deploy

Run the Pipeline / Action to deploy the landing zone

Iterate

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

ALZ IaC Accelerator – New Features!

tfvars (HCL) as input for Platform landing zone configuration

- Retains customer updates, formatting, comments and ordering
- Easy to test

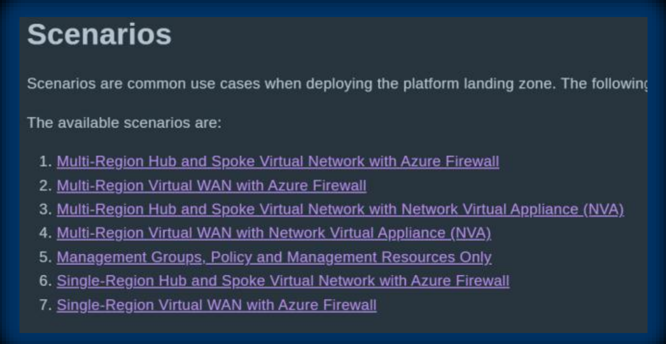
Phase 0 – Planning

- Guides you through decisions about bootstrap and Platform landing zone
- Checklist to help record decisions

Options and Scenarios

- Scenarios: 7 high level Platform landing zone architectures
- Options: 14 common customisations

aka.ms/alz/acc/starter/avm-plz

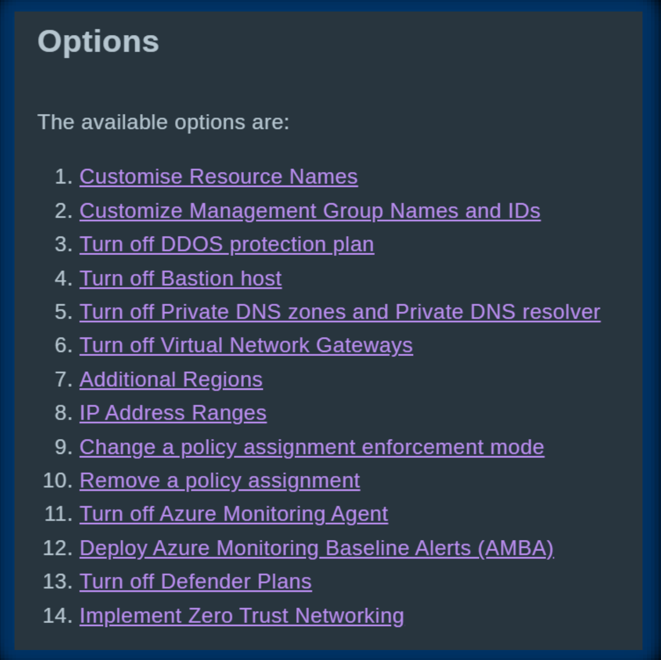


Scenarios

Scenarios are common use cases when deploying the platform landing zone. The followin

The available scenarios are:

1. Multi-Region Hub and Spoke Virtual Network with Azure Firewall
2. Multi-Region Virtual WAN with Azure Firewall
3. Multi-Region Hub and Spoke Virtual Network with Network Virtual Appliance (NVA)
4. Multi-Region Virtual WAN with Network Virtual Appliance (NVA)
5. Management Groups, Policy and Management Resources Only
6. Single-Region Hub and Spoke Virtual Network with Azure Firewall
7. Single-Region Virtual WAN with Azure Firewall



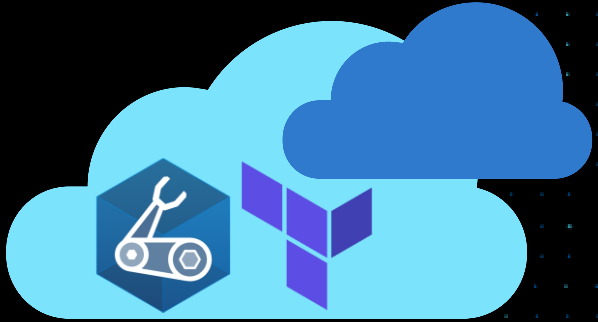
Options

The available options are:

1. Customise Resource Names
2. Customize Management Group Names and IDs
3. Turn off DDOS protection plan
4. Turn off Bastion host
5. Turn off Private DNS zones and Private DNS resolver
6. Turn off Virtual Network Gateways
7. Additional Regions
8. IP Address Ranges
9. Change a policy assignment enforcement mode
10. Remove a policy assignment
11. Turn off Azure Monitoring Agent
12. Deploy Azure Monitoring Baseline Alerts (AMBA)
13. Turn off Defender Plans
14. Implement Zero Trust Networking

Microsoft

Migrating to OR refactoring existing TF code to AVM modules



Matt White

Microsoft

Bicep AVMs
for Platform Landing Zone (ALZ)

Jack Tracey

ALZ Bicep

- MVP for vNext: Anticipated for March!
  - We're looking for **teams interested in testing the MVP** before its official launch.
    - 📌 **Scan the QR Code** to sign up and participate!
- ALZ-Bicep (Release of v0.20.2 two weeks ago)
  - Added the option to specify **virtual network gateway IP configuration names**.
  - Added missing **DNS zones** for policy assignment: `Deploy-Private-DNS-Zones`.
  - Fix role assignments for **AMA Policies**
  - **Az.Resources 7.8.0**
    - Released with **Azure PowerShell v13.1.0**.
    - Resolves the **deployment issue** when using the Accelerator.

Customer experience sharing

Pankaj Meshram

Mohammad Reza Gashtil (NTT)

Maik Wendt (NTT)

Microsoft

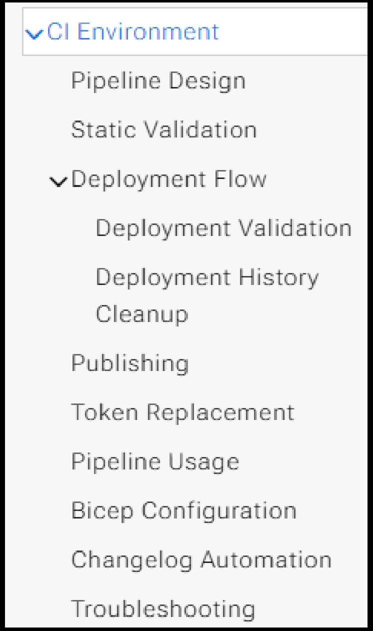
More updates…

René Hézser

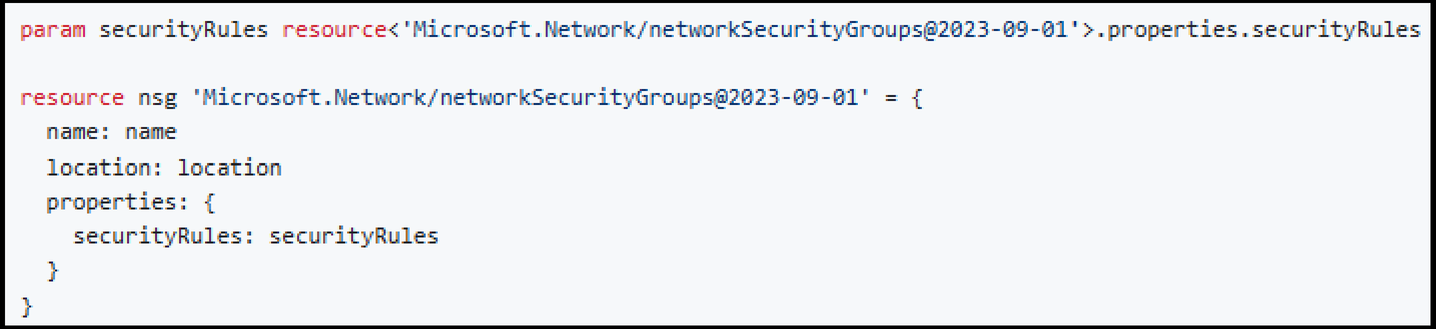
What’s in the Pipeline

Bicep

- CI documentation
- Changelogs
- Resource derived types

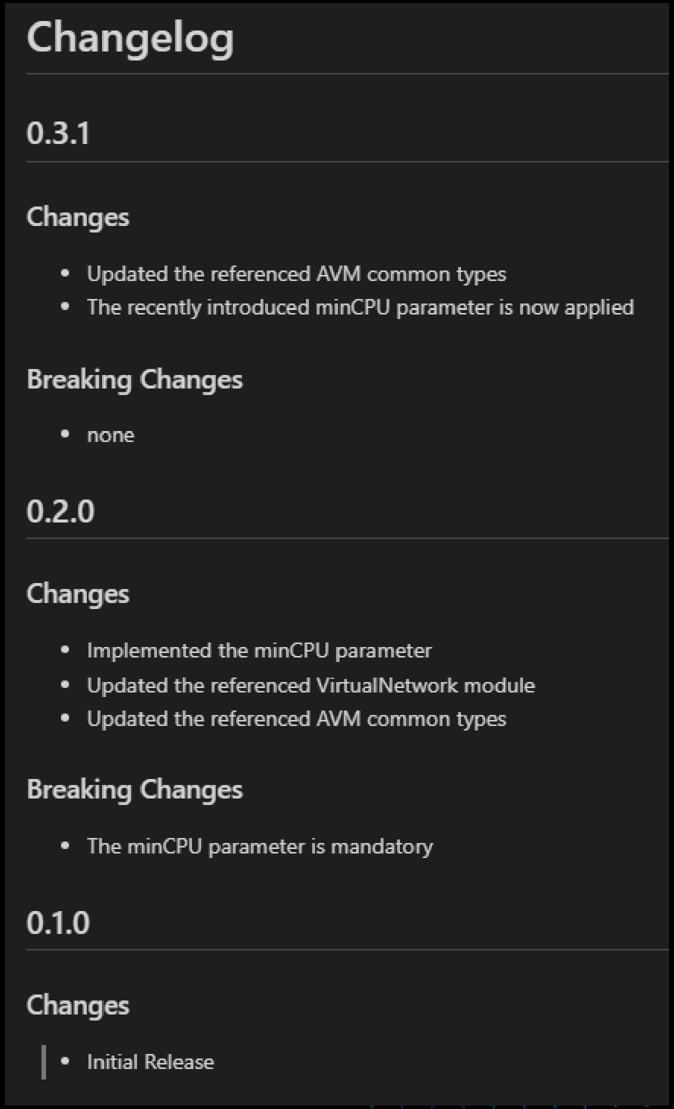


- CI Environment
  - Pipeline Design
  - Static Validation
  - Deployment Flow
    - Deployment Validation
    - Deployment History Cleanup
  - Publishing
  - Token Replacement
  - Pipeline Usage
  - Bicep Configuration
  - Changelog Automation
  - Troubleshooting



```
param securityRules resource<'Microsoft.Network/networkSecurityGroups@2023-09-01'>.properties.securityRules

resource nsg 'Microsoft.Network/networkSecurityGroups@2023-09-01' = {
  name: name
  location: location
  properties: {
    securityRules: securityRules
  }
}
```



Changelog

0.3.1

Changes

- Updated the referenced AVM common types
- The recently introduced minCPU parameter is now applied

Breaking Changes

- none

0.2.0

Changes

- Implemented the minCPU parameter
- Updated the referenced VirtualNetwork module
- Updated the referenced AVM common types

Breaking Changes

- The minCPU parameter is mandatory

0.1.0

Changes

- Initial Release

Q & A

Getting Involved – aka.ms/AVM

AVM is open for everyone to contribute

- Devolved ownership, not centralised!
- AVM welcomes contributors from all over the world!

Learn

- AVM Resources – aka.ms/AVM/resources
  - Labs, blog posts, podcasts, videos and more
- Leverage aka.ms/AVM/specs & aka.ms/AVM/contributing
- Stay informed – aka.ms/avm/monthly/latest

Contribute

- Identify which proposed modules you would like to contribute to:
  - Bicep AVM modules looking for contributors
  - Terraform AVM modules looking for contributors
- Propose a new module: aka.ms/AVM/ModuleProposal