



What's new with Microsoft Azure Infrastructure as Code?

Azure Verified Modules (AVM)
Azure Landing Zones (ALZ)
ALZ Accelerators

Azure Global – April 2024
Jared Holgate
Senior Cloud Solution Architect



Agenda

- Azure Verified Modules (AVM)
- Azure Landing Zones Modules (ALZ) vNext
- ALZ Accelerators
- Help wanted! How can you contribute and get recognition?

Hello



Jared Holgate

Senior Cloud Solution Architect at Microsoft

About:

23+ years of Software Engineering in various roles. Long-time advocate and practitioner of Continuous Delivery and DevOps. Previously a Terraform SME at HashiCorp.

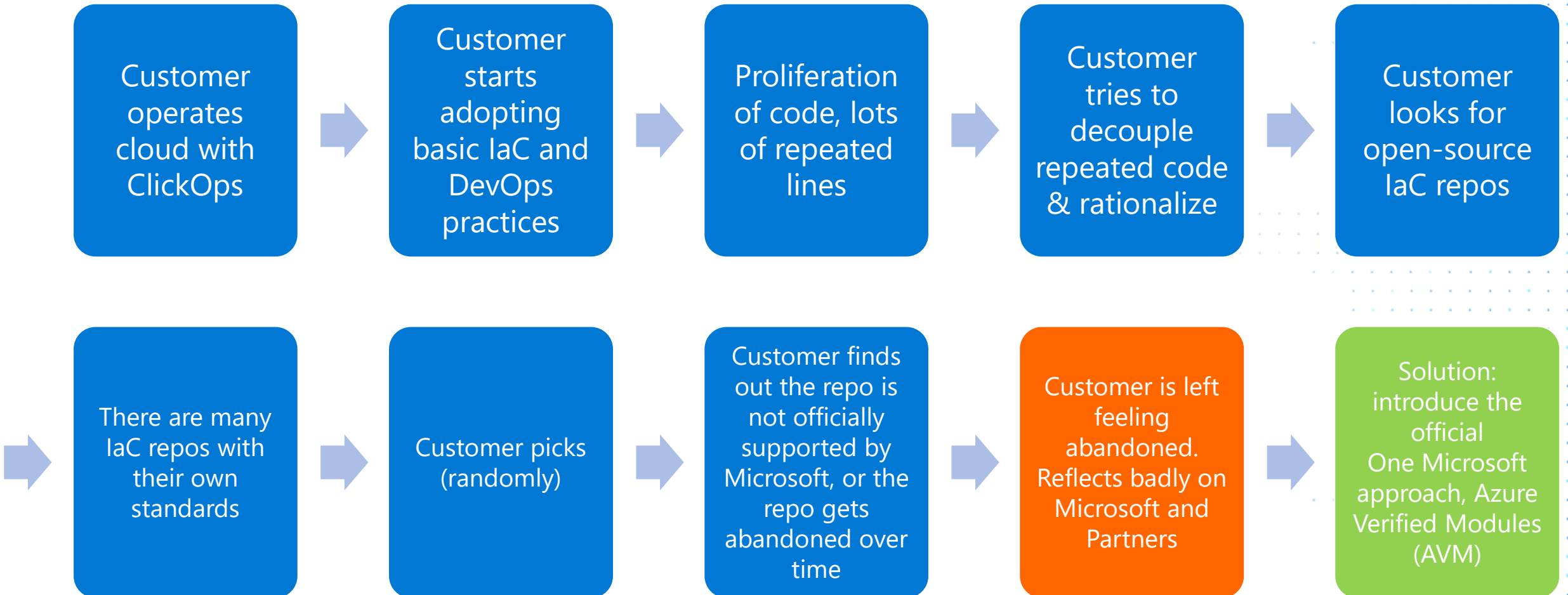
Cloud Solution Architect at Microsoft for 1.5 years. Member of the ALZ Team. Own AVM modules and maintain the ALZ Accelerator for Terraform.



Azure Verified Modules



Azure Verified Modules – Why?





Azure Verified Modules – Mission

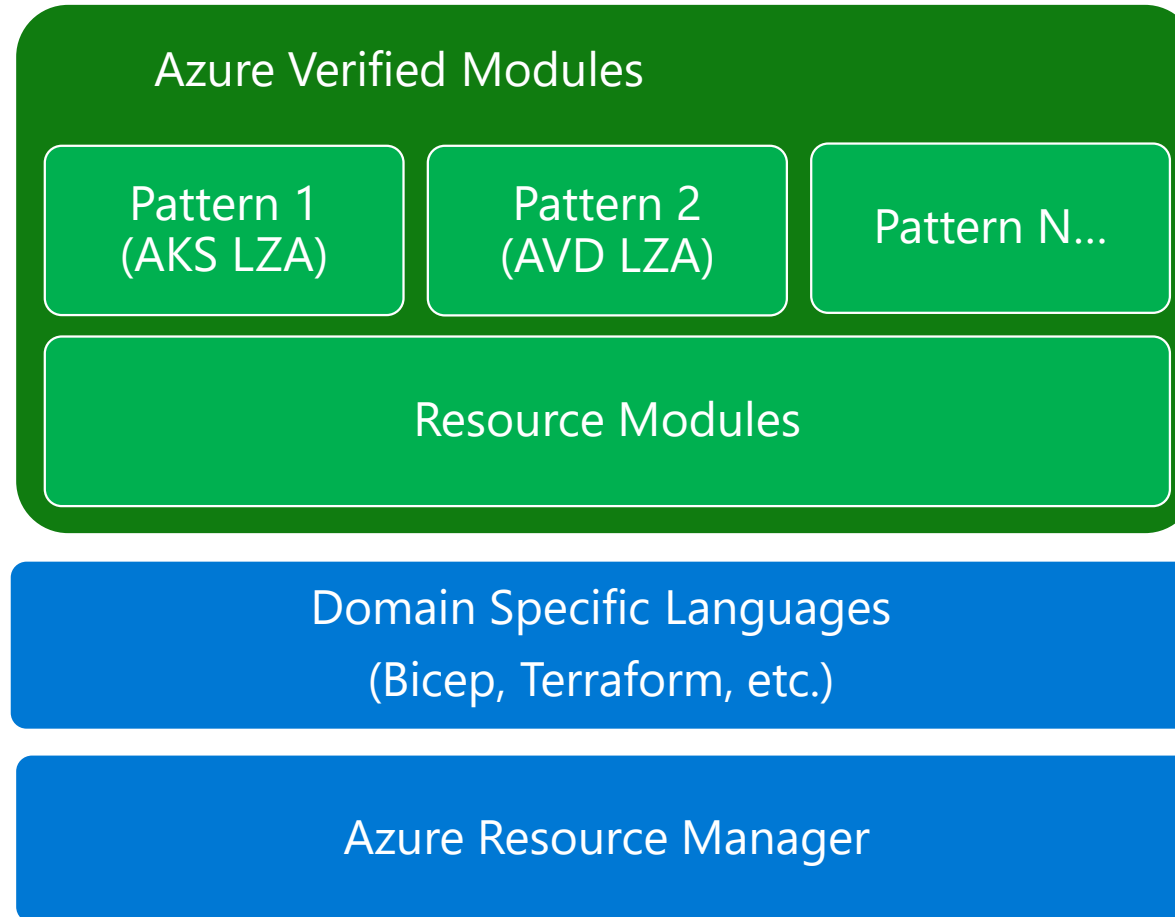
“Our mission is to deliver a **comprehensive Azure Verified Modules library** in **multiple IaC languages**, serving as the **trusted Microsoft source of truth**.

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.”





Azure Verified Modules – Structure

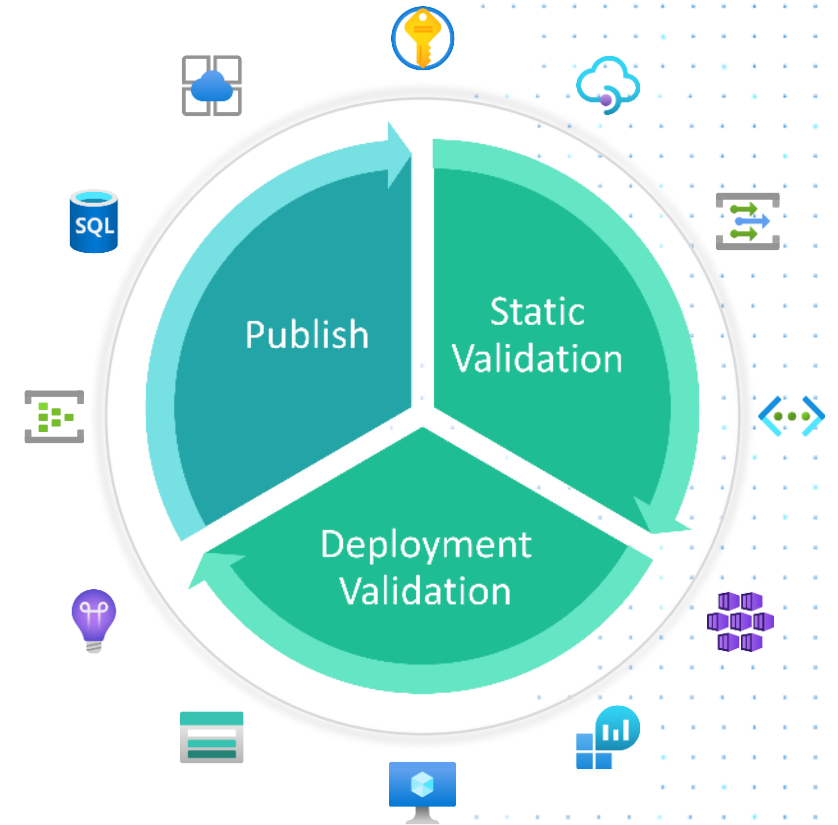




Azure Verified Modules – Toolkit

AVM is a common code base, a toolkit **for our Customers, our Partners, and Microsoft**

- Azure Verified Modules enable **and accelerate consistent solution development** and delivery by **codifying Microsoft guidance** (WAF), with best practice configurations.
- The experience builds from solution to solution as it illustrates end-to-end IaC solution and highlights advanced DevOps capabilities.



Azure Verified Modules



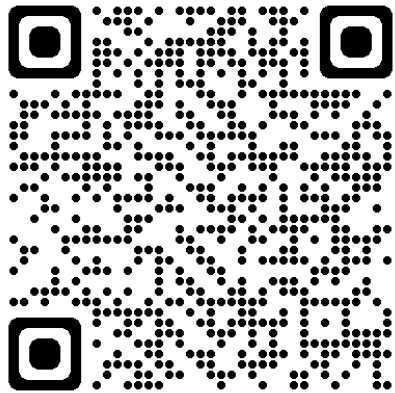
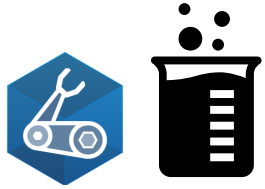
Azure Verified Modules – “Verified”

- Follows **clear specifications and naming standards**, defining what a good IaC module is:
 - How they should be constructed and built
 - How they are to be consumed
 - What they deliver for consumers in terms of resources deployed and configured
 - Where appropriate, aligned across IaC languages (e.g., Bicep, Terraform, etc.).
- **Codifies** current **best practices** guidelines, as per Microsoft Azure **Well-Architected Framework**
- Azure Verified **Modules just work** - enforcing consistency and testing where possible
- **Modules are maintained** – I can trust that modules follow available Azure capabilities over time
- **Microsoft supports it** – there’s a process with SLAs that guarantee that issues will be handled in a timely manner; related engineering team was consulted/asked to provide feedback/owns the module
- Provides a level of **documentation/examples** that make consumption **self-service**

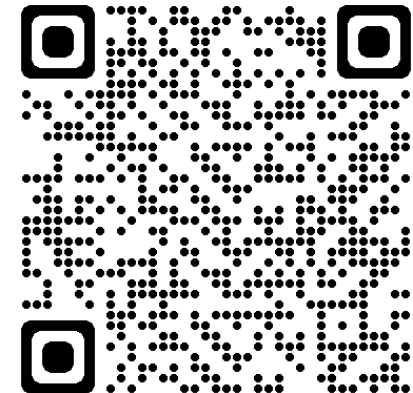
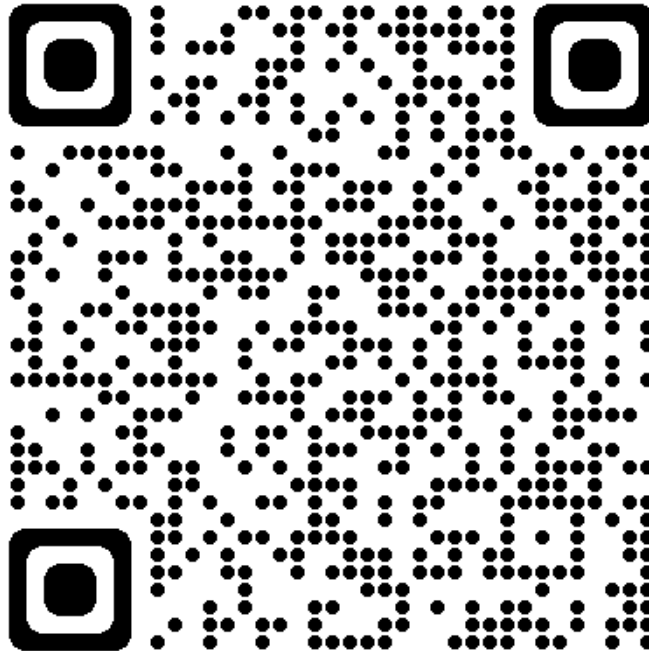


Azure Verified Modules – Where is it?

<https://aka.ms/AVM>



<https://aka.ms/avm/bicep/labs>



<https://aka.ms/avm/tf/labs>

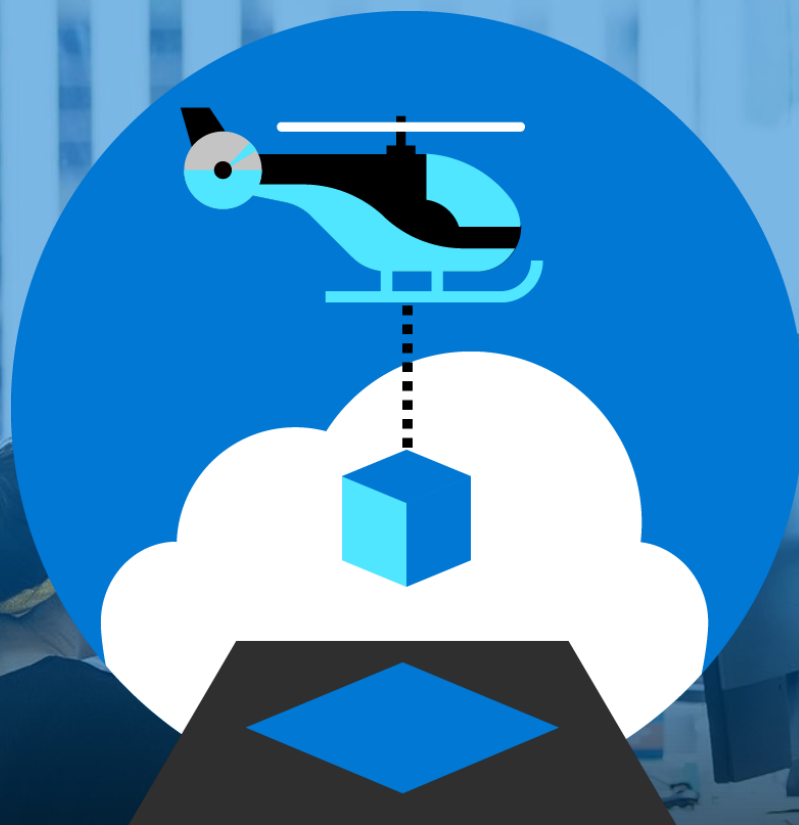


Azure Verified Modules – Contribute



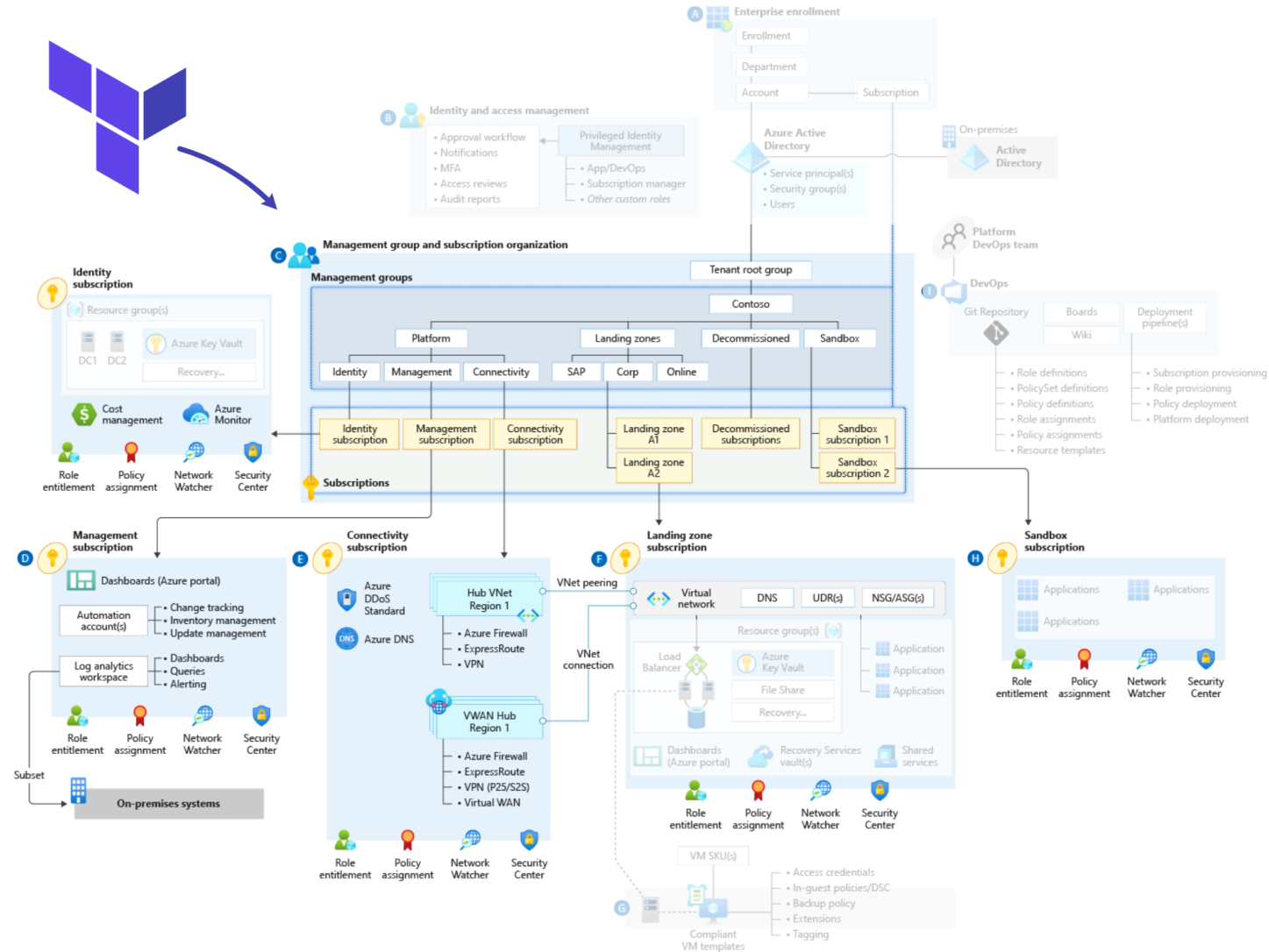
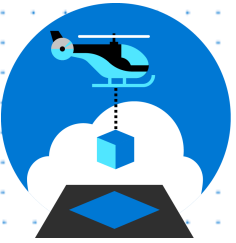
Propose new modules and contribute to modules.

Module owner(s) must be a Microsoft FTE, but you can contribute the code.



Azure Landing Zones Modules vNext

Azure Landing Zones Modules – What is it?



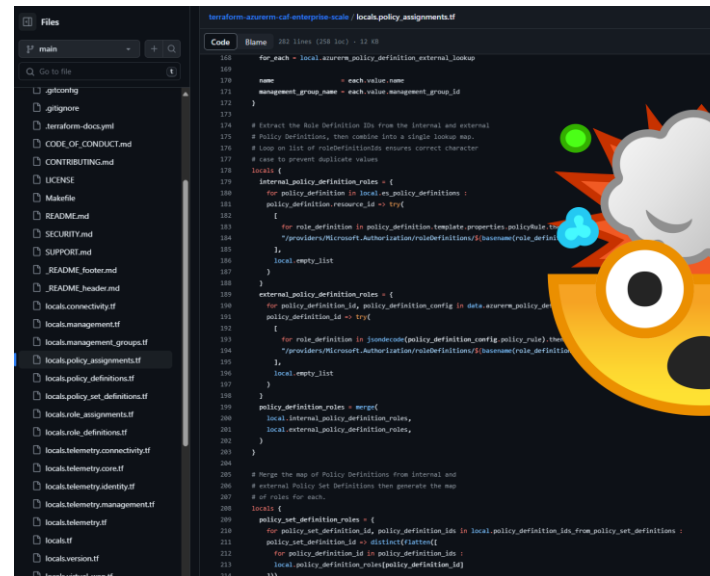


Azure Landing Zones Modules – Current State

[terraform-azurerm-caf-enterprise-scale](#) monolithic module that deploys everything.

Feedback:

- Customers: want to pick and choose parts to deploy to compose their Azure Landing Zone
- Module Maintainers:





Azure Landing Zones Modules – vNext

Compose the modules together

[Azure/avm-ptn-alz](#): Management groups and policy

[Azure/avm-ptn-alz-management](#): Management resources

[Azure/avm-ptn-hubnetworking](#): Hub networking with vNet

[Azure/avm-ptn-virtualwan](#): Virtual WAN

[Azure/avm-ptn-vnetgateway](#): vNet gateways

Etc...

```
10 module "alz_management_resources" {
11   source = "Azure/alz-management/azurerm"
12   version = "~> 0.1.0"
13
14   automation_account_name = module.naming.automation_account.name_unique
15   location                = local.default_location
16   log_analytics_workspace_name = module.naming.log_analytics_workspace.name_unique
17   resource_group_name      = module.naming.resource_group.name_unique
18 }
19
20 # This allows us to get the tenant id
21 data "azurerm_client_config" "current" {}
22
23 module "alz_archetype_root" {
24   source = "Azure/avm-ptn-alz/azurerm"
25   id     = "${random_pet.this.id}-alz-root"
26   display_name = "${random_pet.this.id}-alz-root"
27   parent_id   = data.azurerm_client_config.current.tenant_id
28   base_archetype = "root"
29   default_location = local.default_location
30   default_log_analytics_workspace_id = module.alz_management_resources.log_analytics_workspace.id
31   delays = {
32     before_management_group_creation = {
33       create = "0s"
34     }
35   }
36 }
37
38 module "alz_archetype_landing_zones" {
39   source = "Azure/avm-ptn-alz/azurerm"
40   id     = "${random_pet.this.id}-landing-zones"
41   display_name = "${random_pet.this.id}-landing-zones"
42   parent_id   = module.alz_archetype_root.management_group_name
43   base_archetype = "landing_zones"
44   default_location = local.default_location
45   default_log_analytics_workspace_id = module.alz_management_resources.log_analytics_workspace.id
46 }
47
48 module "alz_archetype_platform" {
49   source = "Azure/avm-ptn-alz/azurerm"
50   id     = "${random_pet.this.id}-platform"
51   display_name = "${random_pet.this.id}-platform"
52   parent_id   = module.alz_archetype_root.management_group_name
53 }
```

End to end examples:

- [complete vnext in Accelerator](#)
- [examples in ALZ module](#)

Subscription Vending: <https://github.com/Azure/terraform-azurerm-lz-vending>



Azure Landing Zones Modules – vNext

Pattern Module:

<https://registry.terraform.io/modules/Azure/avm-ptn-alz>

Backed by the ALZ Terraform Provider:

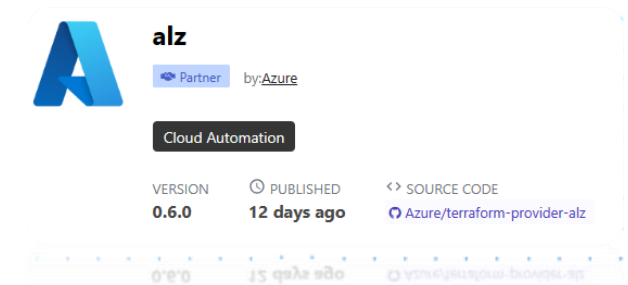
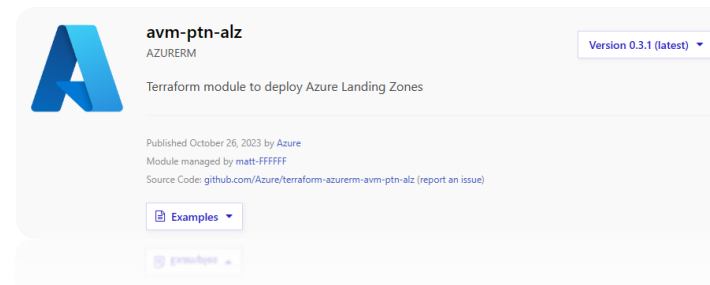
<https://registry.terraform.io/providers/Azure/alz>

Scope of the new module

Management groups

Policy

Role Assignments





Azure Landing Zones Modules



Try out the new modules.

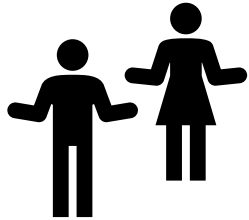
Raise issues and contribute code.



Azure Landing Zones Accelerators

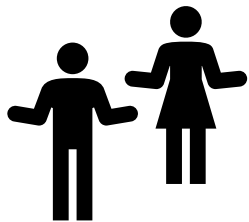


Azure Landing Zones Accelerators – Why



Microsoft

Helping my customers with ALZ deployments is hard, can we make it easier?

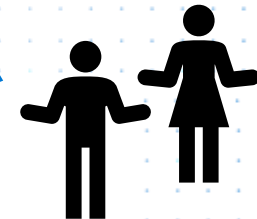


Partner

We need a best practice repeatable process and we don't want to invent it ourselves.

I'm new to IaC, where do I start?

I just want Microsoft to tell me what to do. I don't want to have to figure it out from scratch.



Customer



Azure Landing Zones Accelerators – What

- An **opinionated** quick start **guide** and **automation** to fulfil those asks
- The accelerator **scope** is the **Azure Landing Zone** (management groups, policy, hub networking, etc)

Azure Landing Zones Accelerators – How



Repository

Accelerator

Documentation

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

Pre-requisite Scripts

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

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



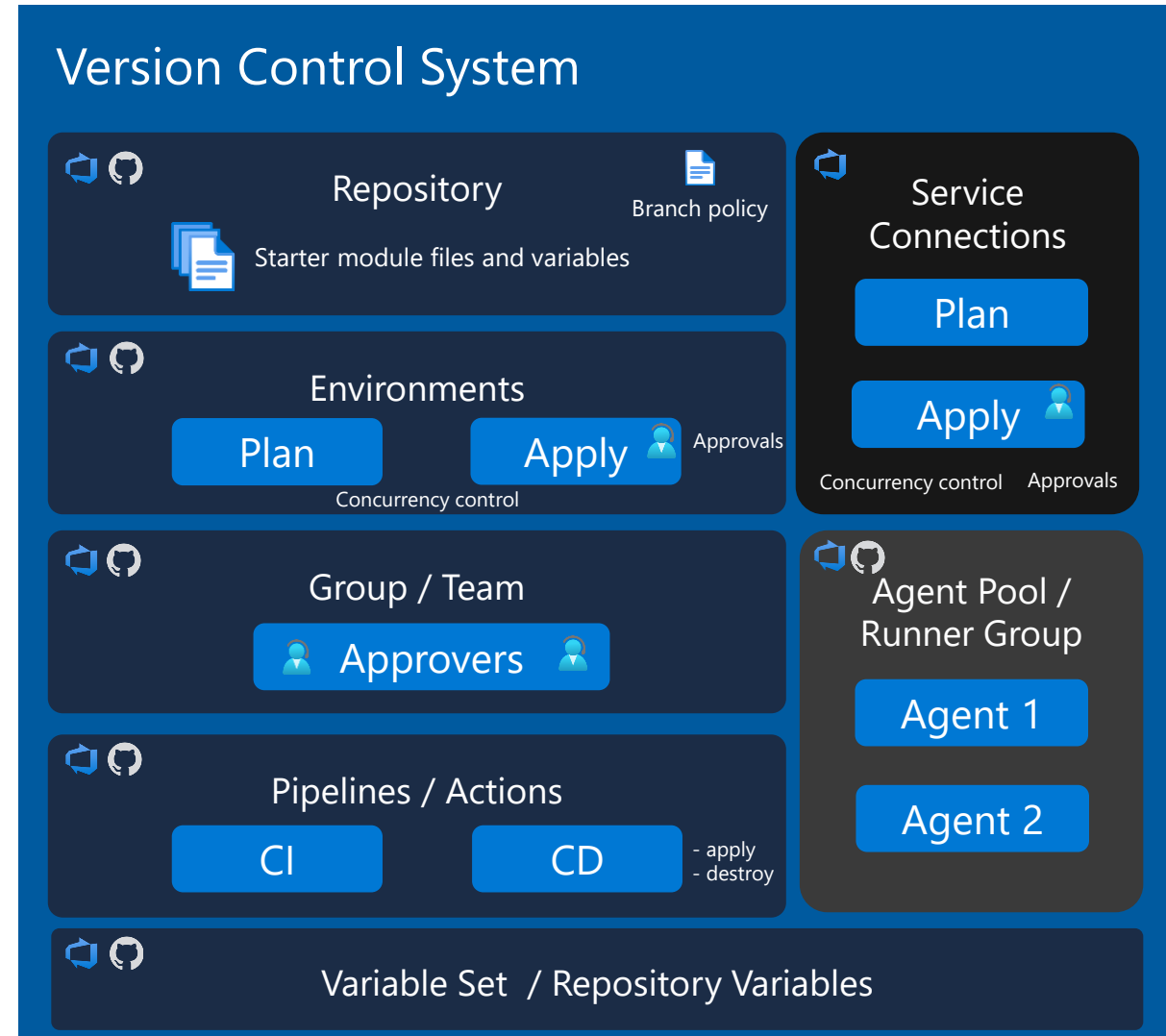
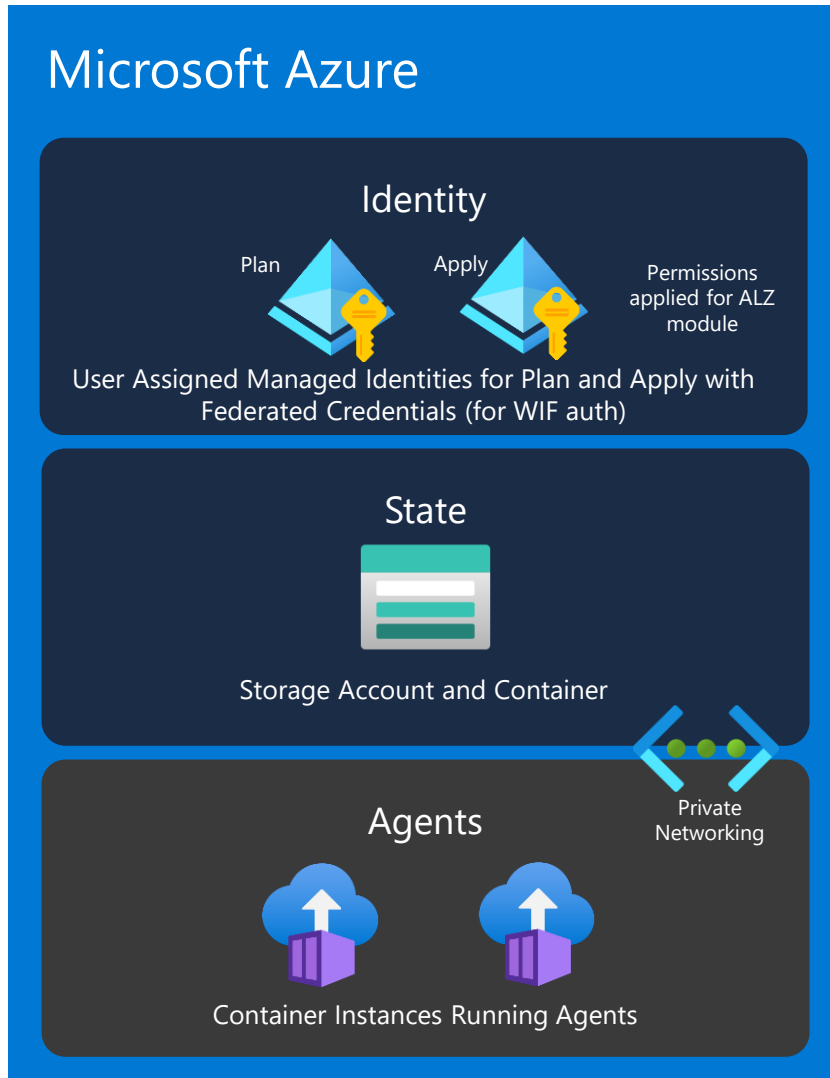
Azure Landing Zones Accelerators – Options

What options do we support now for Terraform? (Bicep coming soon!)

| Version Control System | Agents / Runners | Networking | Authentication |
|------------------------|--------------------|----------------|-------------------------------------|
| GitHub | Microsoft Hosted | Public | Workload identity federation |
| GitHub | Self Hosted | Public | Workload identity federation |
| GitHub | Self Hosted | Private | Workload identity federation |
| Azure DevOps | Microsoft Hosted | Public | Workload identity federation |
| Azure DevOps | Self Hosted | Public | Workload identity federation |
| Azure DevOps | Self Hosted | Private | Workload identity federation |
| Azure DevOps | Self Hosted | Public | Managed identity |
| Azure DevOps | Self Hosted | Private | Managed identity |



Azure Landing Zones Accelerators – Bootstrap





Azure Landing Zones Accelerators – Usage

```
# Install the PowerShell Module
```

```
Install-Module -Name ALZ
```

```
# Deploy the Bootstrap for Bicep and GitHub
```

```
Deploy-Accelerator -i "bicep" -b "alz_github"
```

```
# Deploy the Bootstrap for Bicep and Azure DevOps
```

```
Deploy-Accelerator -i "bicep" -b "alz_azuredevops"
```

```
# Deploy the Bootstrap for Terraform and GitHub
```

```
Deploy-Accelerator -i "terraform" -b "alz_github"
```

```
# Deploy the Bootstrap for Terraform and Azure DevOps
```

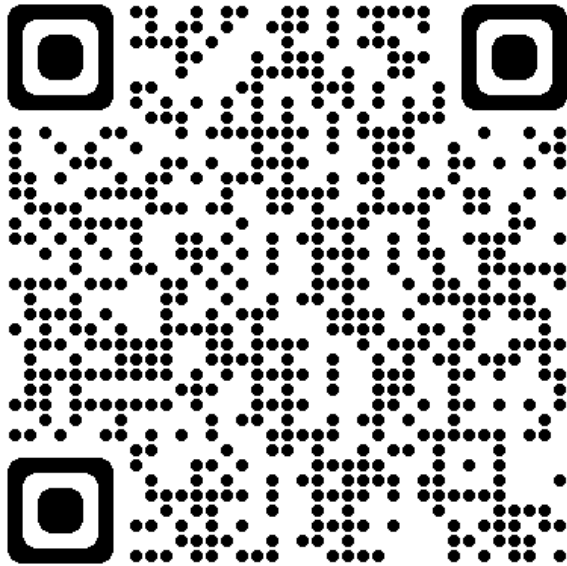
```
Deploy-Accelerator -i "terraform" -b "alz_azuredevops"
```



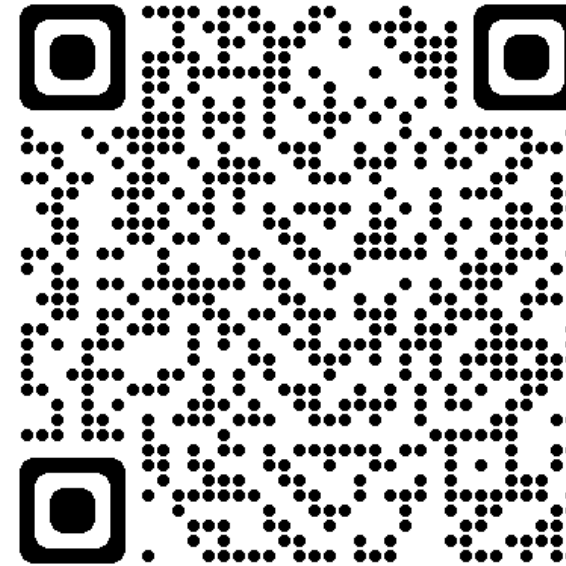
Azure Landing Zone Accelerators – Where is it?



<https://aka.ms/alz-tf-acc>



<https://aka.ms/alz-bcp-acc>



★ <https://aka.ms/alz-tf-acc-blog> ★



Azure Landing Zones Accelerators



Try out the Accelerators.

Raise issues and contribute code.



DEMO

- Fingers crossed!

We need

YOU!



Help Wanted!

Have Global Impact and Earn Recognition



Badges!

Have Global Impact and Earn Recognition

Contribute

- AVM – Pick up issues for Docs or Code Fixes
- AVM – Propose modules
- ALZ Modules – Pick up issues for Docs or Code Fixes
- ALZ Accelerators – Pick up issues for Docs or Code Fixes

Raise Issues

- Improvements
- Bugs





Thank you