Microsoft

Azure Verified Modules (AVM)

Community Call, 24th September 2024

Speakers: Máté Barabás, Erika Gressi, René Hézser, Jack Tracey, Jon Chancellor,
Jared Holgate, Chinedum Echeta, Nelly Kiboi-Mungo, Saverio Proto,
Pankaj Meshram, Jonathan D’Aloia

Meet the AVM Core Team

Technical SME's

Alex

Bilal

Chris

Erika

Jack

Jared

Jon

Matt

Predrag

Rainer

Sebastian

René

PM's

Charlie

Máté

Pankaj

Agenda

- Poll – How familiar are you with AVM?
- Bicep & Terraform Updates (15 mins)
    - Module development progress
    - Utility modules
    - Specification updates
    - Custom CI Secrets
    - Bicep CI bootstrap tool
    - WAF updates
- Showcasing pattern modules (20 mins)
- Guest speaker: Telefónica Tech (10 mins)
- Q & A

Azure Verified Modules Poll

- **Please answer the poll in Teams chat:**
    - What is your awareness level of Azure Verified Modules?
        - Level 100 – I have heard of AVM but never used it
        - Level 200 – I know about AVM and have used it in PoC
        - Level 300 – I used AVM all the time
        - Level 400 – I contribute to the AVM Libraries

Microsoft

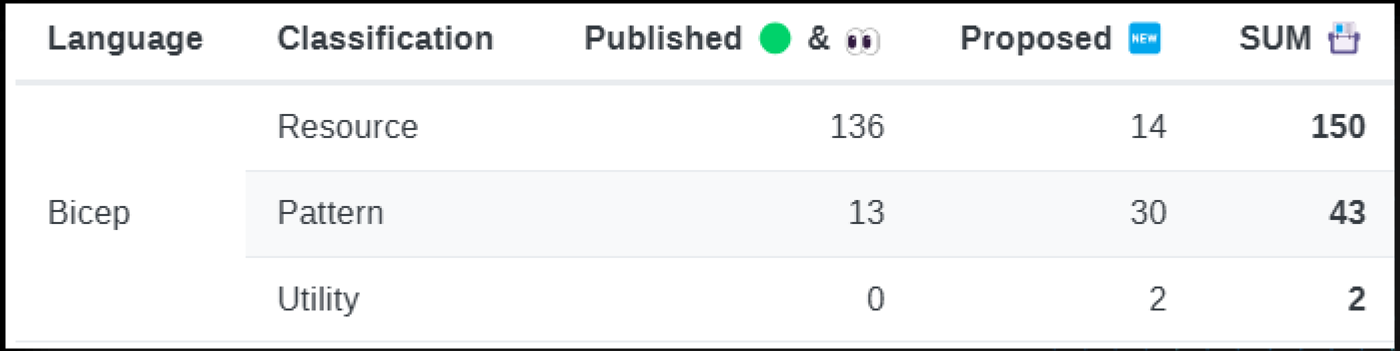
Bicep Updates

Erika Gressi, René Hézser, Jack Tracey

Module Updates

Pattern modules – 7 new

- avm/ptn/lz/sub-vending
- avm/ptn/network/private-link-private-dns-zones
- avm/ptn/deployment-script/import-image-to-acr
- avm/ptn/ai-platform/baseline
- avm/ptn/aca-lza/hosting-environment
- avm/ptn/azd/insights-dashboard
- avm/ptn/azd/apim-api



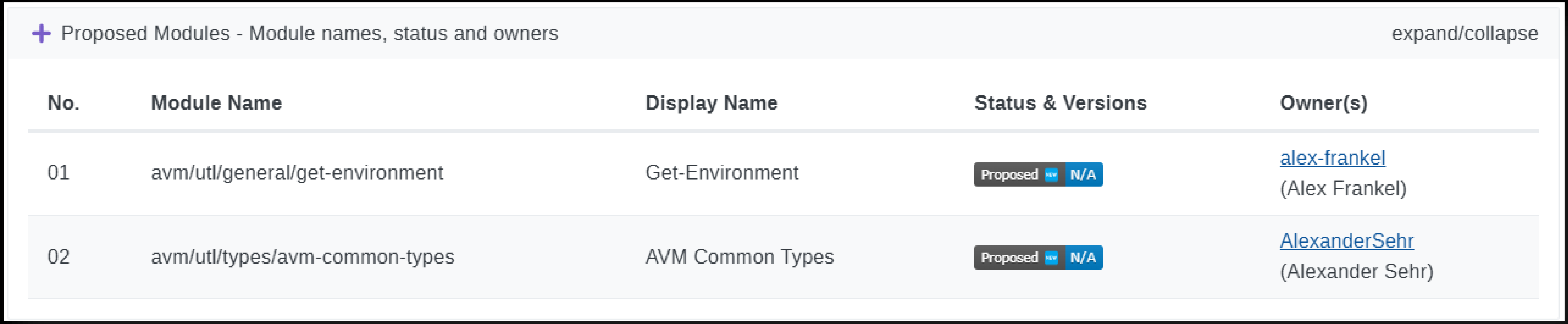
Language	Classification	Published 🟢 & 👀	Proposed 🆕	SUM 🗳️
Bicep	Resource	136	14	**150**
	Pattern	13	30	**43**
	Utility	0	2	**2**

Resource modules – 5 new

- avm/res/portal/dashboard
- avm/res/kusto/cluster
- avm/res/hybrid-compute/machine
- avm/res/alerts-management/action-rule
- avm/res/dev-ops-infrastructure/pool

Utility Modules

Implements a function or routine that can be flexibly reused in resource or pattern modules and does not deploy any Azure resources.



+ Proposed Modules - Module names, status and owners

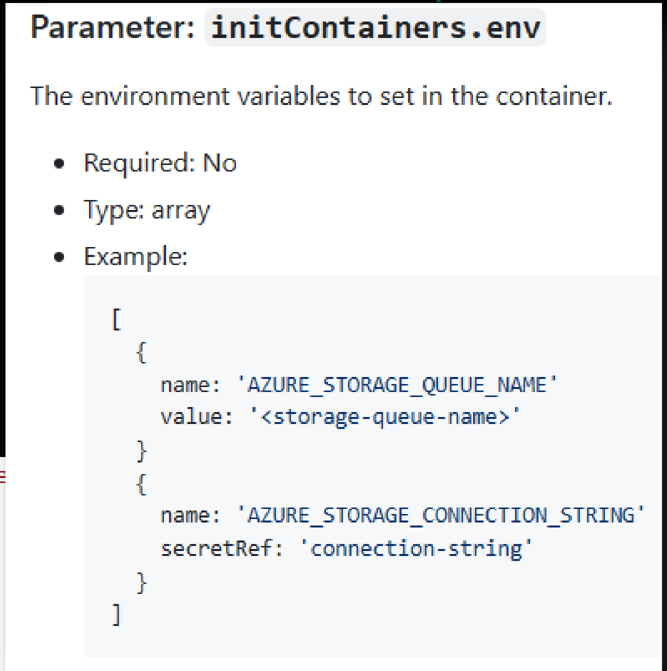
expand/collapse

No.	Module Name	Display Name	Status & Versions	Owner(s)
01	avm/utl/general/get-environment	Get-Environment	Proposed 🆕 N/A	alex-frankel (Alex Frankel)
02	avm/utl/types/avm-common-types	AVM Common Types	Proposed 🆕 N/A	AlexanderSehr (Alexander Sehr)

[Bicep Utility Modules | Azure Verified Modules]

New Features / specification updates

- PowerShell Helper Script To Setup Fork & CI Test Environment
  - Simplifies forking and setting up Azure for testing
- Documentation - Parameter Input Examples
  - Can be used as example for specific scenarios
- Improved versioning documentation
  - Semantic Versioning
  - < 1.0.0 guidance

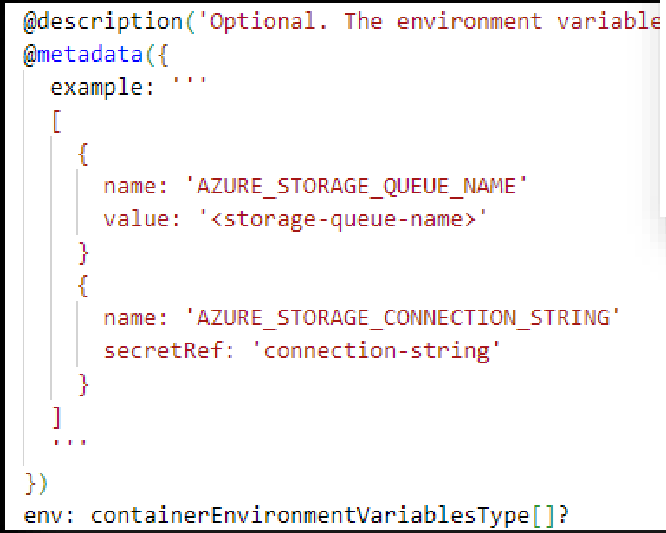


Parameter: `initContainers.env`

The environment variables to set in the container.

- Required: No
- Type: array
- Example:

```
[
  {
    name: 'AZURE_STORAGE_QUEUE_NAME'
    value: '<storage-queue-name>'
  }
  {
    name: 'AZURE_STORAGE_CONNECTION_STRING'
    secretRef: 'connection-string'
  }
]
```



```
@description('Optional. The environment variable
@metadata({
  example: '''
  [
    {
      name: 'AZURE_STORAGE_QUEUE_NAME'
      value: '<storage-queue-name>'
    }
    {
      name: 'AZURE_STORAGE_CONNECTION_STRING'
      secretRef: 'connection-string'
    }
  ]
  '''
})
env: containerEnvironmentVariablesType[]?
```

Custom CI Secrets

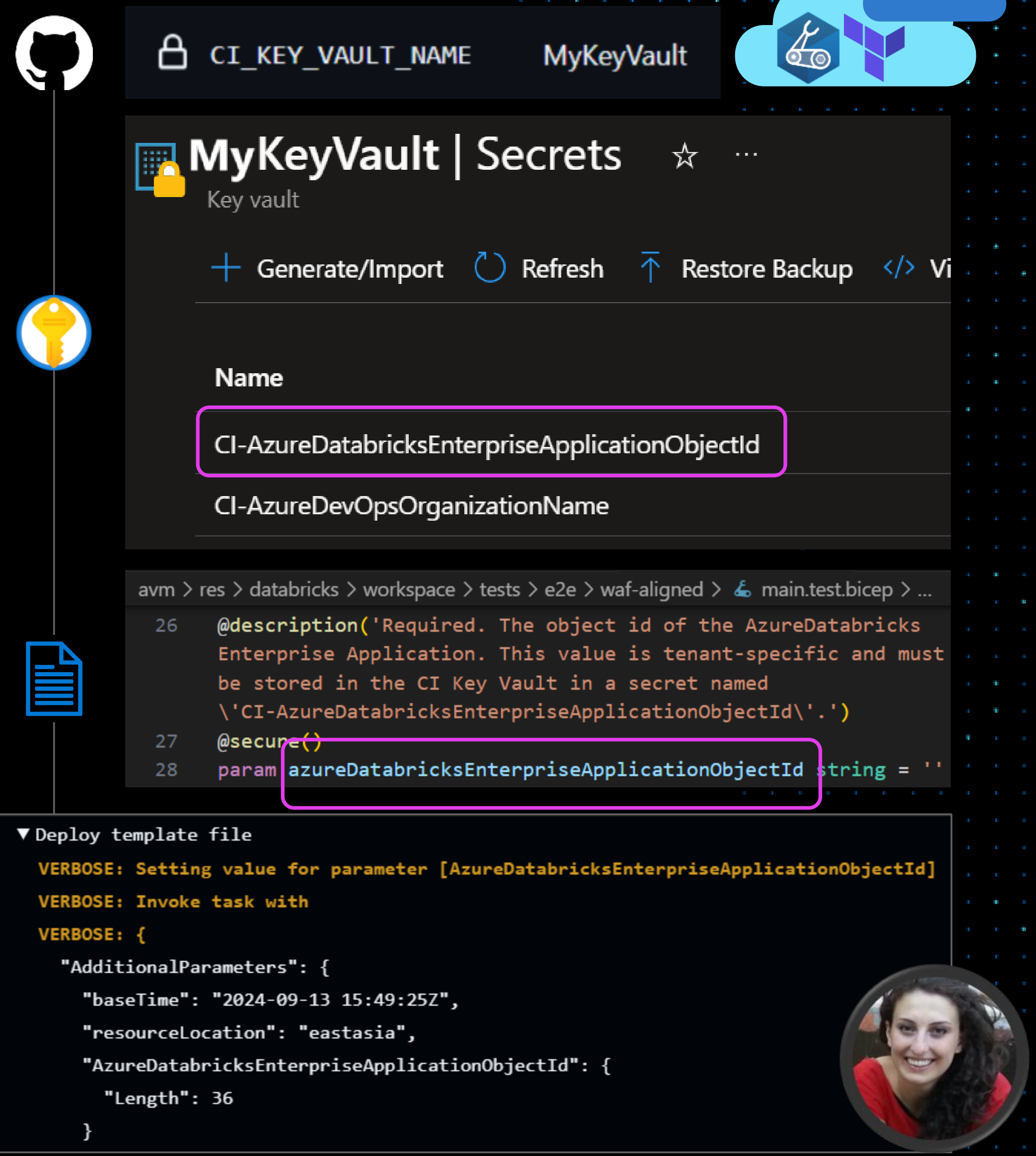
Parameterize **tenant specific values** in e2e deployment tests

Requires to be set up in both the upstream and the contributors environment

- GitHub repository variable
- Key vault secret
- Test input parameter

Secret - parameter match → Pull value

Ref Custom CI Secrets documentation



CI-AzureDatabricksEnterpriseApplicationObjectId

CI-AzureDevOpsOrganizationName

avm > res > databricks > workspace > tests > e2e > waf-aligned > main.test.bicep > ...

```
@description('Required. The object id of the AzureDatabricks Enterprise Application. This value is tenant-specific and must be stored in the CI Key Vault in a secret named \'CI-AzureDatabricksEnterpriseApplicationObjectId\'.')
@secure()
param azureDatabricksEnterpriseApplicationObjectId string = ''
```

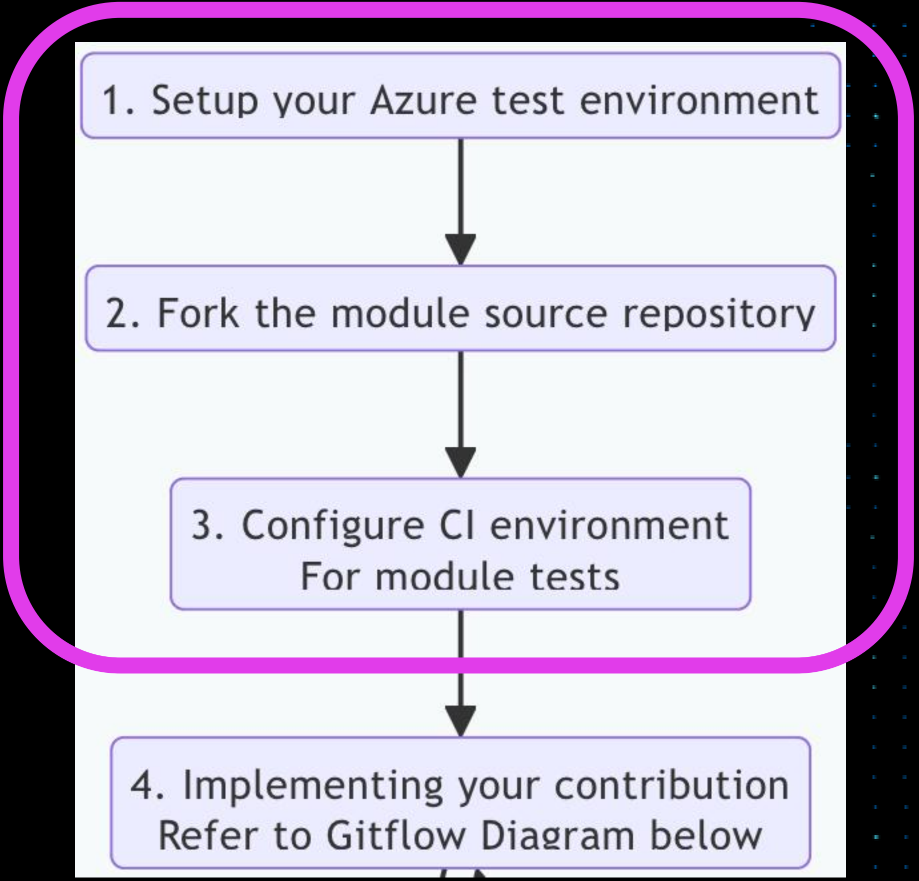
```
▼ Deploy template file
  VERBOSE: Setting value for parameter [AzureDatabricksEnterpriseApplicationObjectId]
  VERBOSE: Invoke task with
  VERBOSE: {
    "AdditionalParameters": {
      "baseTime": "2024-09-13 15:49:25Z",
      "resourceLocation": "eastasia",
      "AzureDatabricksEnterpriseApplicationObjectId": {
        "Length": 36
      }
```

AVM Bicep CI pre-reqs bootstrap tool

We've heard loud and clear that getting started contributing to AVM Bicep modules with all of the CI pre-requisites was complicated 😭

Well, we listened and have good news… 🥁

New-AVMBicepBRMForkSetup.ps1 is now available to help you get started 🥳



1. Setup your Azure test environment

2. Fork the module source repository

3. Configure CI environment
For module tests

4. Implementing your contribution
Refer to Gitflow Diagram below

WAF Updates

- We are making good progress towards completing **high-impact Reliability recommendations** for the top 20 Azure services in both languages

- We are now starting the assessment phase for **high-impact Security recommendations** for the same top 20 services
  - Utilising the MDfC recommendations as per our FAQ
  - ⁉️ ***Are there other sources of truth we should be using?*** ⁉️

- We are taking the stance of we MUST be able to test, and have the test written and available, for us to be able to enforce the recommendation in both:
  - PSRule for Azure == Bicep
  - TFLint (AVM Ruleset) == Terraform

Microsoft

Terraform Updates

Jon Chancellor, Jared Holgate

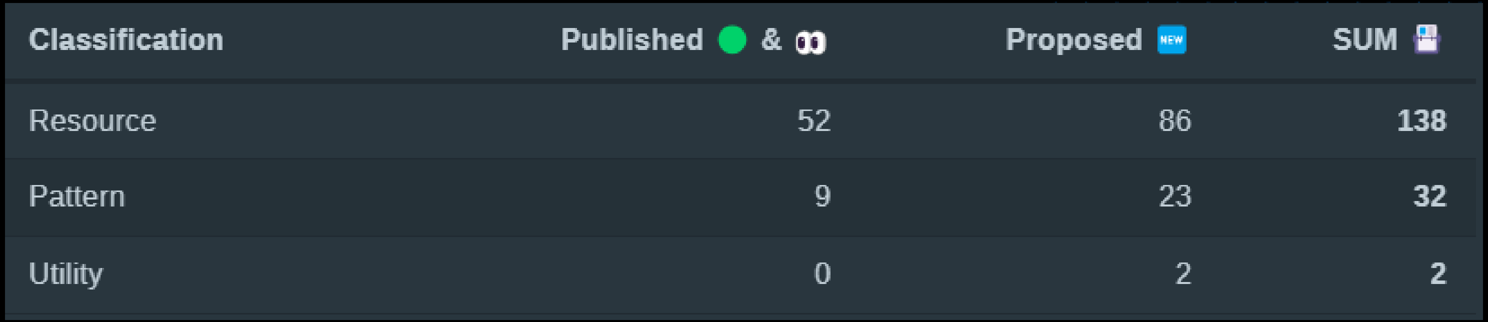
Module Updates

Pattern modules –

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

Resource modules –

- avm-res-cache-redis
- avm-res-logic-workflow
- avm-res-web-hostingenvironment
- avm-res-app-containerapp
- avm-res-containerinstance-containergroup
- avm-res-machinelearningservices-workspace
- avm-res-network-networkwatcher
- avm-res-compute-hostgroup
- avm-res-documentdb-databaseaccount
- avm-res-edge-site
- avm-res-hybridcontainerservice-provisionedclusterinstance
- avm-res-insights-component
- avm-res-network-applicationgateway
- avm-res-resources-resourcegroup
- avm-res-search-searchservice



Classification	Published 🟢 & 👀	Proposed 🆕	SUM 💾
Resource	52	86	**138**
Pattern	9	23	**32**
Utility	0	2	**2**

New Features / Specification Updates

Module Reviews

- Review of Terraform Modules | Azure Verified Modules

Output Spec Updates

- Terraform Specific Specification - Outputs | Azure Verified Modules

Telemetry Updates

- Using modtm to improve the overall telemetry implementation

AzureRM 4.0

Guidance Summary

- All modules using AzureRM must support v4.x by end of Jan 2025
- Before January 2025, module authors should update modules following demand and/or release of new features in 4.0 and release a new version
- Backward compatibility should be maintained with v3 until this is no longer possible
- Newly released modules should support both v3 and v4 unless feature or resource support mandates v4 only until January 2025
- Any referenced module versions should be pinned as per spec

Comments and Discussion

- AzureRM v4.0 thread · Azure/Azure-Verified-Modules · Discussion #1338 (github.com)

CD Security and Efficiency updates

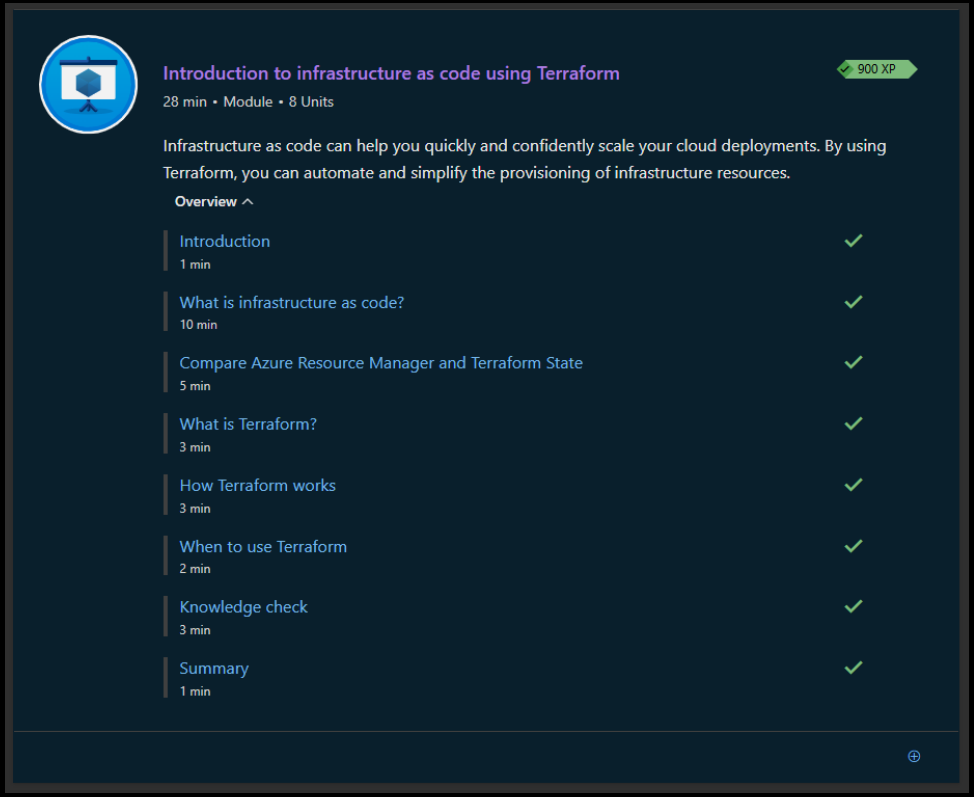
Configuration	Previous Solution	New Solution	Benefits
Runners	1ES Self-hosted pool	Microsoft-hosted	Faster start up, remove parallel run limit
Identity	Compute Managed Identity	User Assigned Managed Identity with OIDC	Granular per repo, per environment. Lower blast radius.
Governed / required workflow	Not possible	Coming soon with centralised template	Workflow cannot be run without the template
Secrets	Not required	Required on environment (automated)	Flexibility to switch tenant / subscription moving forward
Override for edge cases	Difficult and hard coded	Built in override capability	Easily target another tenant and subscription if needed
Git workflow for e2e tests	Could be run from a fork*	Cannot be run from a fork and requires a release branch workflow	Improved security, albeit with a bit of overhead.

* Major driver for making these changes urgently

Repository creation and configuration will be fully automated in the next few weeks.

Terraform on Azure Learning Path

- First module released: Introduction to Infrastructure as code using Terraform: aka.ms/tf/fundamentals
- More modules coming soon!



Introduction to infrastructure as code using Terraform

28 min • Module • 8 Units

Infrastructure as code can help you quickly and confidently scale your cloud deployments. By using Terraform, you can automate and simplify the provisioning of infrastructure resources.

Overview ^

- Introduction 1 min ✓
- What is infrastructure as code? 10 min ✓
- Compare Azure Resource Manager and Terraform State 5 min ✓
- What is Terraform? 3 min ✓
- How Terraform works 3 min ✓
- When to use Terraform 2 min ✓
- Knowledge check 3 min ✓
- Summary 1 min ✓

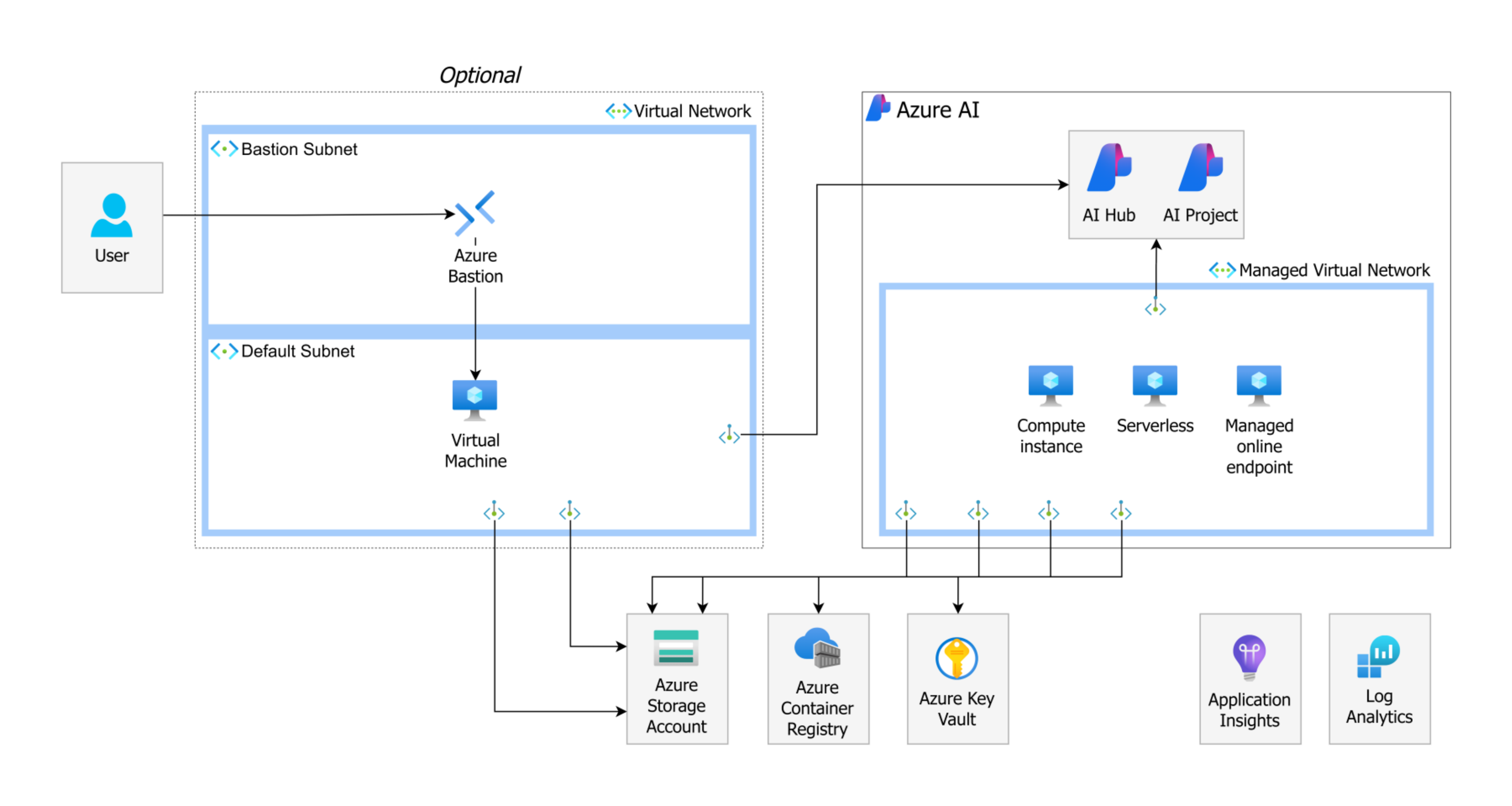
Microsoft

Pattern Modules

Chinedum Echeta, Nelly Kiboi-Mungo, Saverio Proto

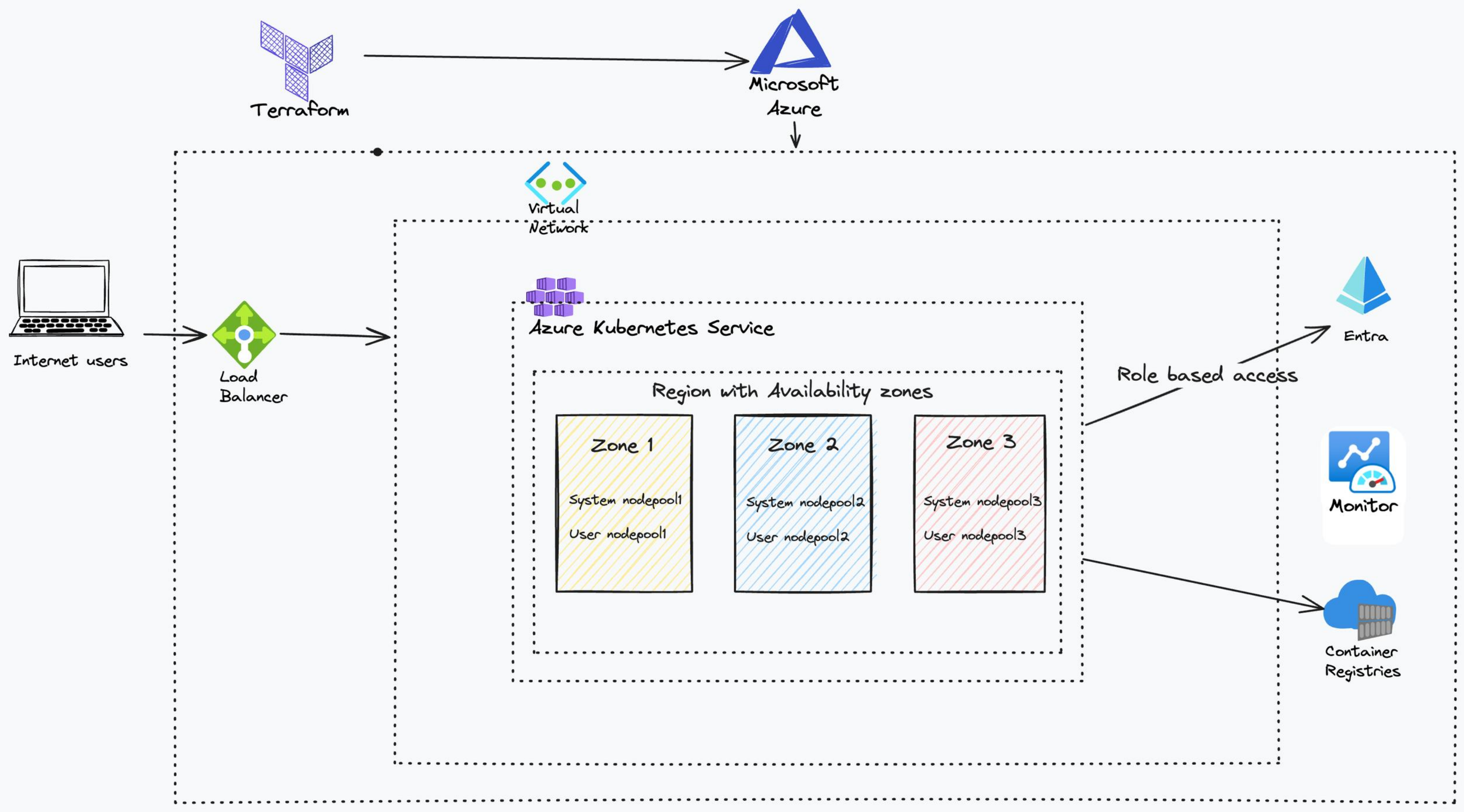
Showcasing Pattern Modules (Bicep)

- **AI Platform Baseline**



Showcasing Pattern Modules (Terraform)

Avm-ptn-aks-production - Simplify Creation Of A Production Ready Aks Cluster



- AKS Cluster
- Virtual Network
- Azure Container Registry

Showcasing Pattern Modules (Terraform)

- ○ User Zonal Node Pools in All Availability Zones(automatically set depending on region)
- ○ Use Azure CNI Overlay for optimal and simple IP address space management
- ○ Leverage AKS automatic upgrades to keep the cluster secure and supported
- ○ Bring your own network and force a User Assigned identity
- ○ Use Private Kubernetes API endpoint and Microsoft Entra authentication for enhanced security
- ○ Don't use any preview features

[How to deploy a production-ready AKS cluster]

Microsoft

Guest Speaker

Jonathan D’Aloia (Telefónica Tech), Pankaj Meshram

Services Partner

Pankaj Meshram

Jonathan D'Aloia
Telefónica Tech

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