AZURE 104

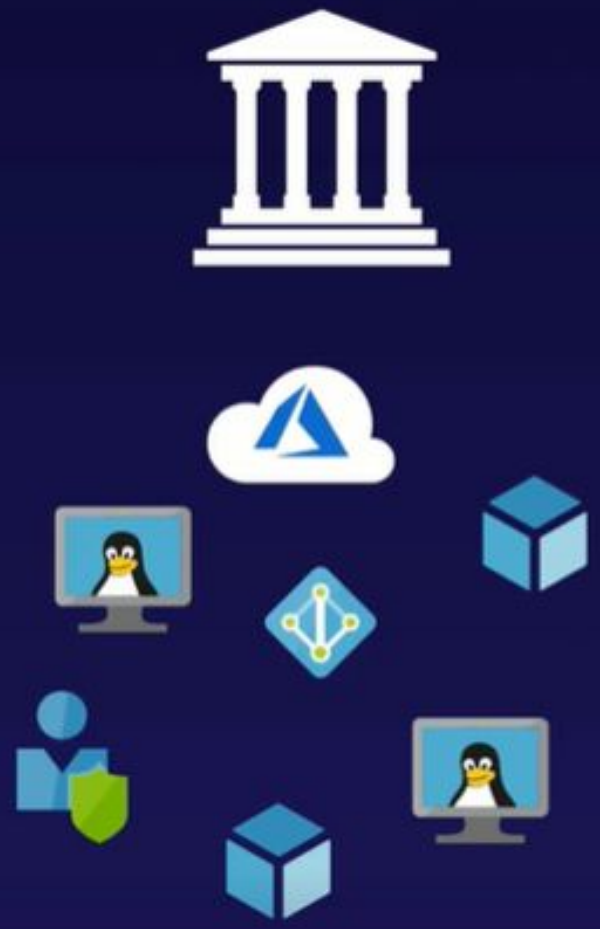
Azure Identities and Governance

Plan

1. Azure Management Groups
2. Role-Based Access Control
3. Azure Policy
4. Azure Blueprints
5. Azure AD Access Reviews
6. Virtual Network Security

Implementing and Managing Governance in Azure

Overview



Take Control of Your Environment

Cloud makes growth and change easy. Structure is important to help manage that growth and change, including items such as:

- Organizational policies and standards
- Security and access control
- Ownership and accountability
- Billing and cost management

Overview

Azure AD Tenant

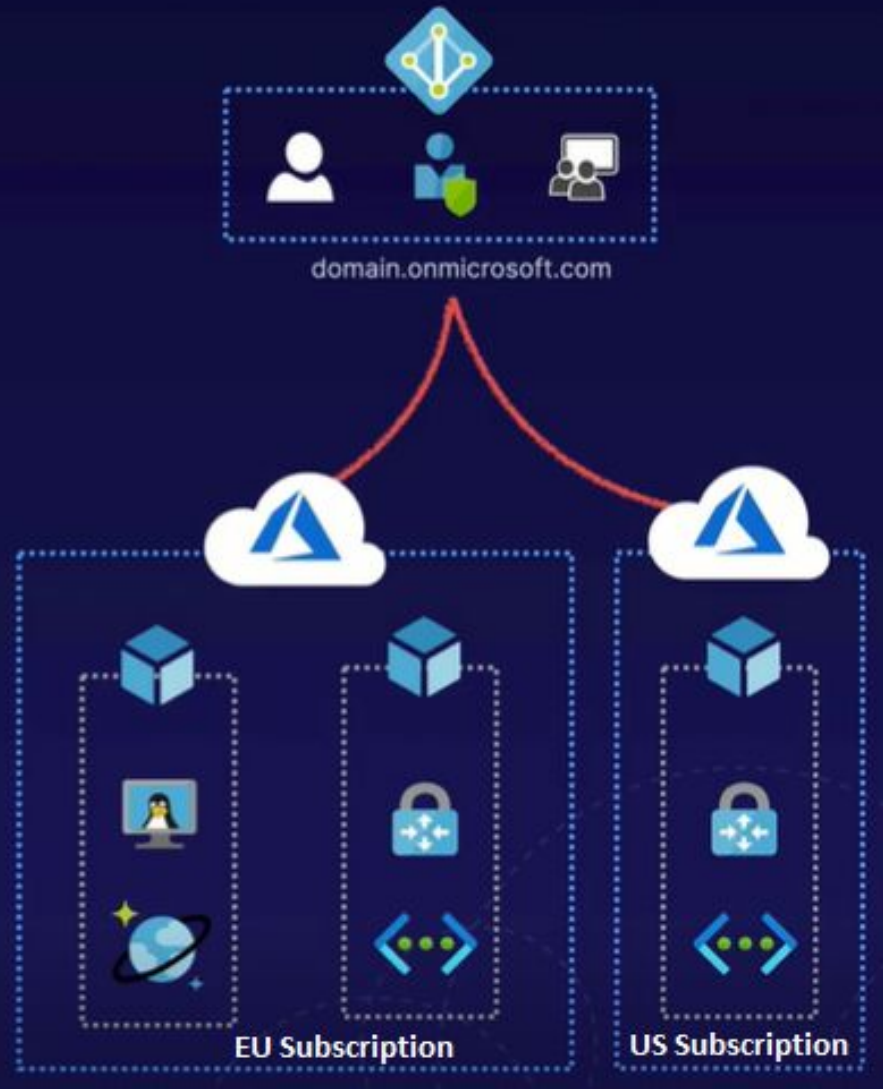
- Centralized identity and access management
- Often shared by multiple subscriptions
- E.g., yourdomain.onmicrosoft.com

Azure Subscription

- Defines important billing/pricing properties
- Multiple can be used by an organization
- E.g., environments, business units, geography

Resource Groups and Resources

- Resource Groups: a logical container for any resource we create (stores meta-data)
- Resources: what we build in Azure



Tagging

Custom Information

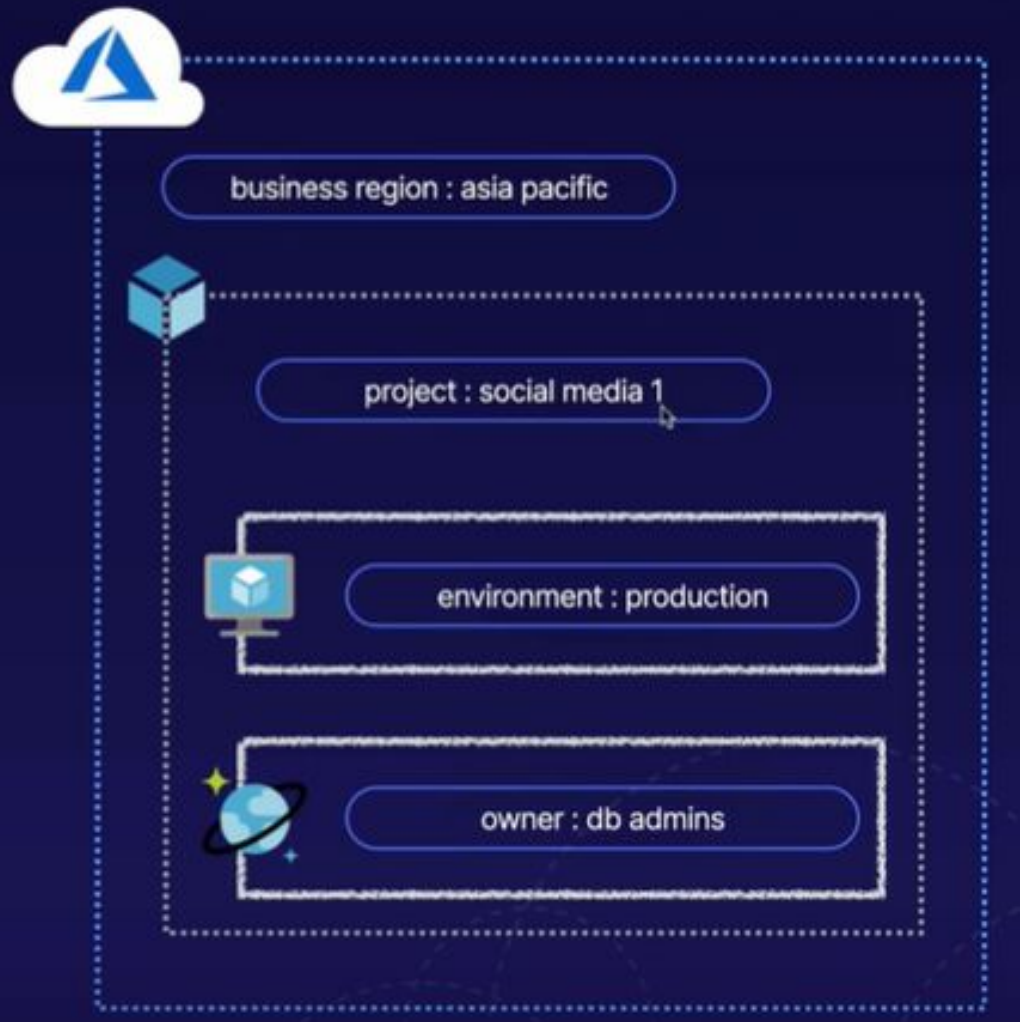
Tagging allows you to add name/value text pairs for storing additional information about your resources.

Applying Tags

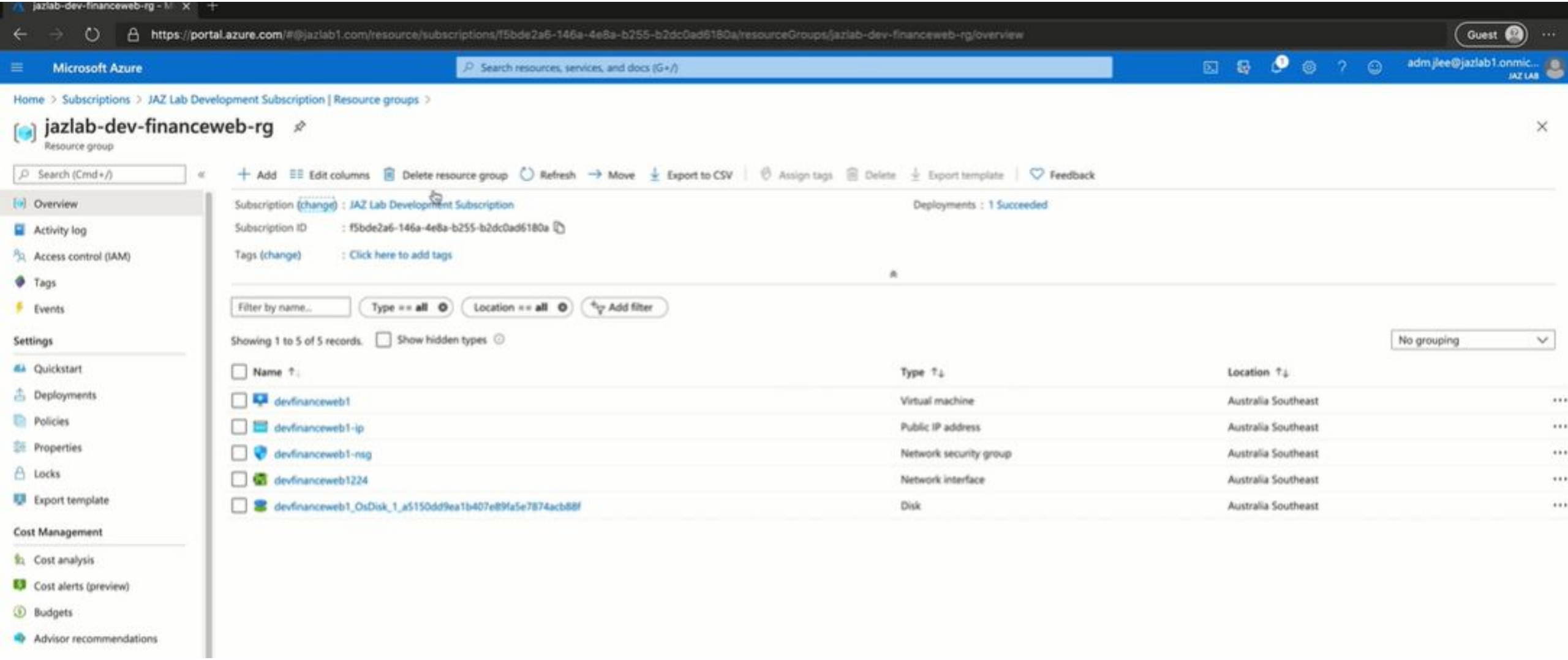
Tags can be applied to resources, resource groups, and subscriptions. Note: not all resources currently support tags.

Use Cases

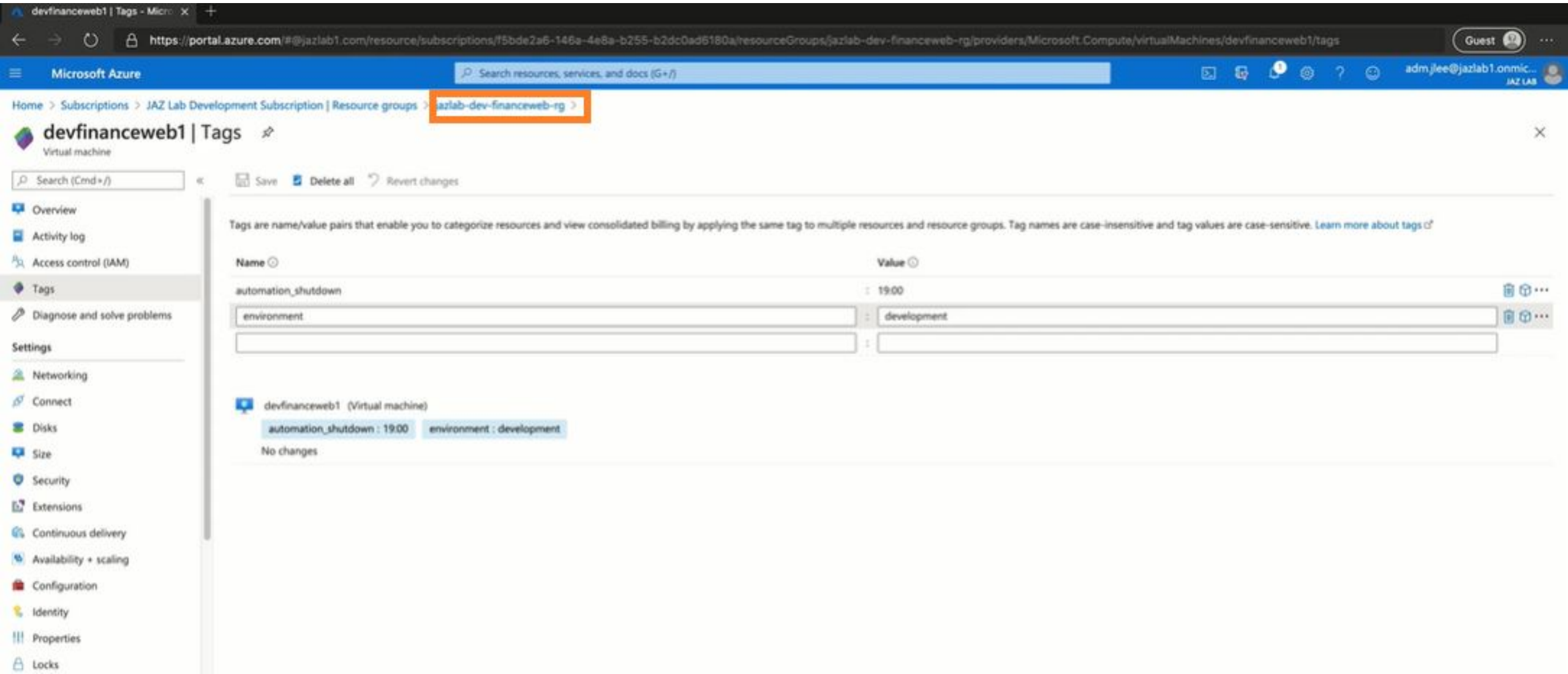
Tagging can be used in a variety of ways, including cost management, automation, monitoring and management, and much more.



Tagging


jazlab-dev-financeweb-rg - M
https://portal.azure.com/#@jazlab1.com/resource/subscriptions/f5bde2a6-146a-4e8a-b255-b2dc0ad6180a/resourceGroups/jazlab-dev-financeweb-rg/overview
Guest
Microsoft Azure
Search resources, services, and docs (G+/)
adm.jlee@jazlab1.onmic...
JAZ LAB
Home > Subscriptions > JAZ Lab Development Subscription | Resource groups >
jazlab-dev-financeweb-rg
Resource group
Search (Cmd+/)
Add
Edit columns
Delete resource group
Refresh
Move
Export to CSV
Assign tags
Delete
Export template
Feedback
Overview
Activity log
Access control (IAM)
Tags
Events
Settings
Quickstart
Deployments
Policies
Properties
Locks
Export template
Cost Management
Cost analysis
Cost alerts (preview)
Budgets
Advisor recommendations
Subscription (change) : JAZ Lab Development Subscription
Deployments : 1 Succeeded
Subscription ID : f5bde2a6-146a-4e8a-b255-b2dc0ad6180a
Tags (change) : Click here to add tags
Filter by name...
Type == all
Location == all
Add filter
Showing 1 to 5 of 5 records.
Show hidden types
No grouping
Name
Type
Location
devfinanceweb1
Virtual machine
Australia Southeast
devfinanceweb1-ip
Public IP address
Australia Southeast
devfinanceweb1-nsg
Network security group
Australia Southeast
devfinanceweb1224
Network interface
Australia Southeast
devfinanceweb1_OsDisk_1_a5150dd9ea1b407e89fa5e7874acb88f
Disk
Australia Southeast

Tagging


devfinanceweb1 | Tags - Micro
https://portal.azure.com/#@jazlab1.com/resource/subscriptions/f5bde2a6-146a-4e8a-b255-b2dc0ad6180a/resourceGroups/jazlab-dev-financeweb-rg/providers/Microsoft.Compute/virtualMachines/devfinanceweb1/tags
Guest
Microsoft Azure
Search resources, services, and docs (G+/)
adm.jlee@jazlab1.onmic...
JAZ LAB
Home > Subscriptions > JAZ Lab Development Subscription | Resource groups > jazlab-dev-financeweb-rg >
devfinanceweb1 | Tags
Virtual machine
Search (Cmd+/)
Save
Delete all
Revert changes
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
Size
Security
Extensions
Continuous delivery
Availability + scaling
Configuration
Identity
Properties
Locks
Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Tag names are case-insensitive and tag values are case-sensitive. Learn more about tags
Name
Value
automation_shutdown : 19:00
environment : development
devfinanceweb1 (Virtual machine)
automation_shutdown : 19:00
environment : development
No changes

Azure Management Groups

Efficiently Manage Subscriptions

Organizations will often use multiple subscriptions to segregate billing and responsibilities. Management Groups allow us to better manage these subscriptions.

- Build a hierarchy that suits your organization
- Apply governance conditions to multiple subscriptions:
  - Enforce Policies
  - Enforce role-based access control

Azure Management Groups - Configuration

Root Management Group

- Top of the entire hierarchy
- Policies applied here are considered "global"
- Requires Azure AD Global Admin access

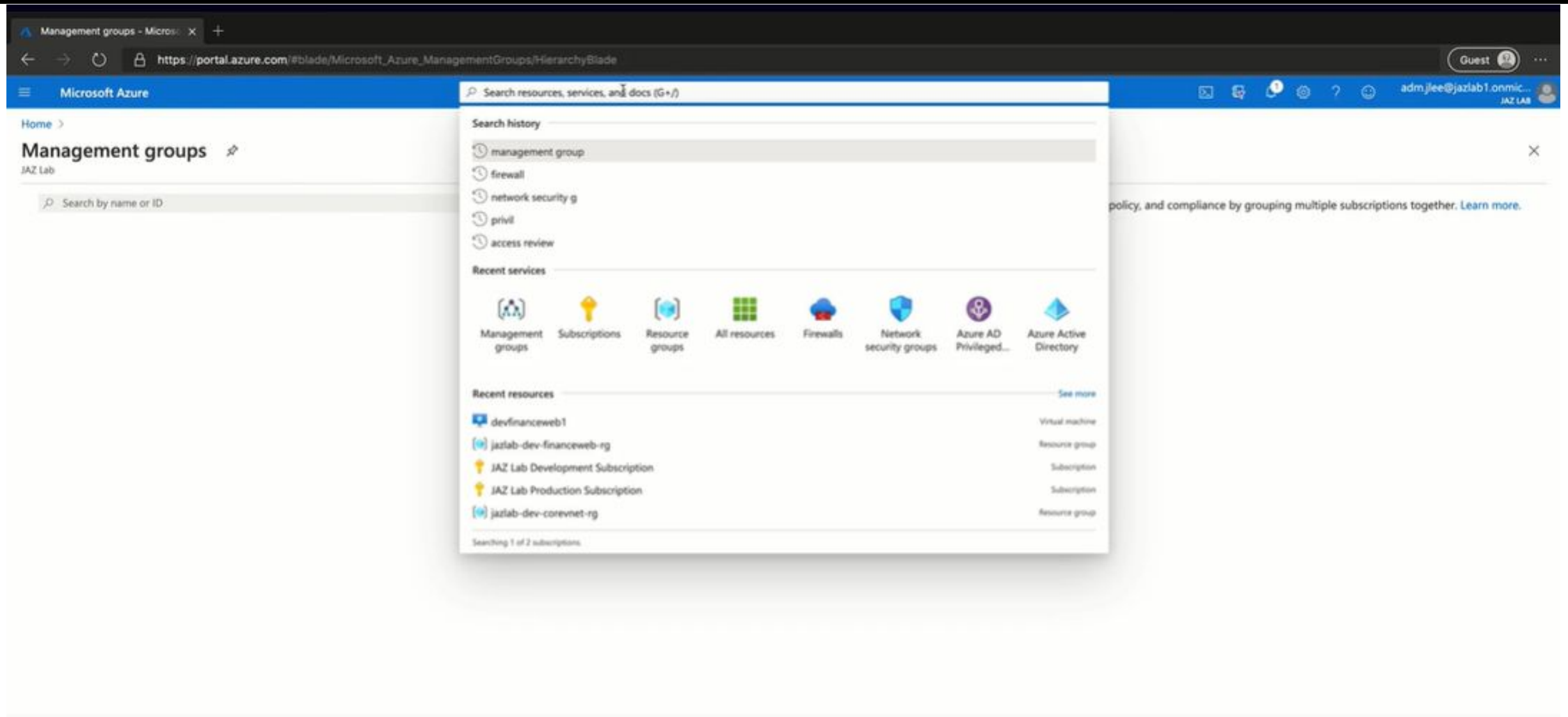
Management Group (MG) Hierarchy

- Up to six levels are supported
- One MG can have multiple children
- One subscription/MG can have only one parent

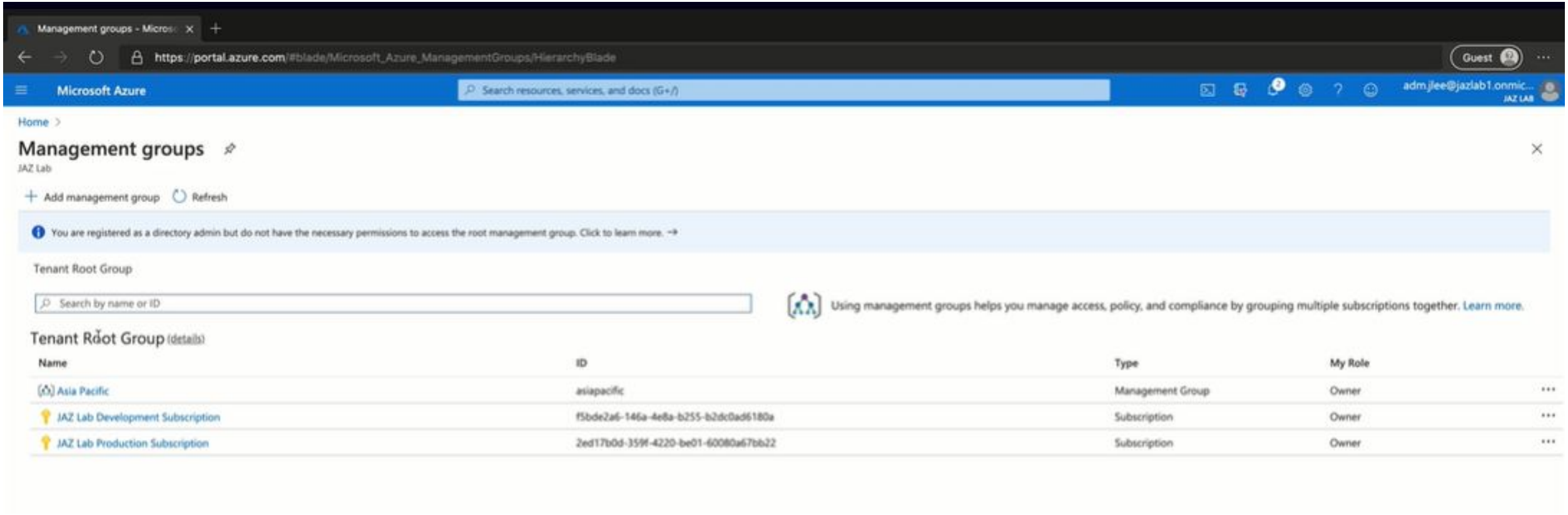
Compliance

- Supports Policies
- Supports RBAC (role-based access control)
- Supports auditing with Activity Logs

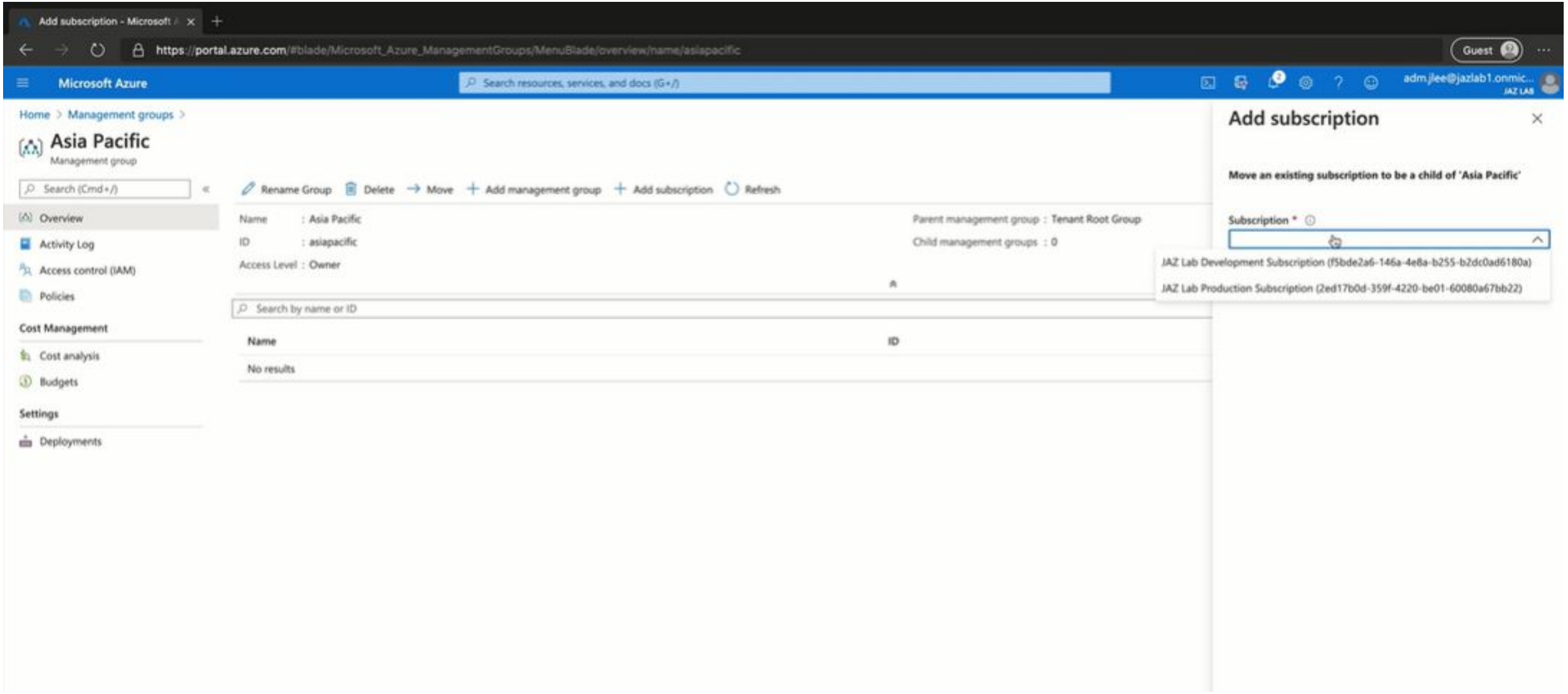
Azure Management Groups



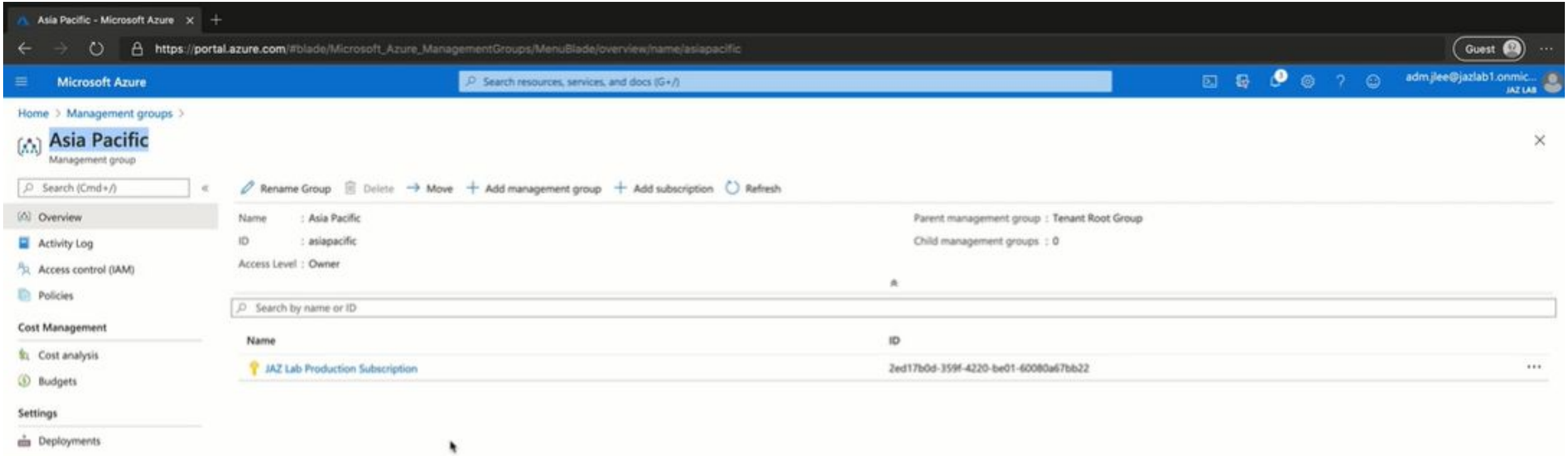
Azure Management Groups



Azure Management Groups



Azure Management Groups



Role-Based Access Control

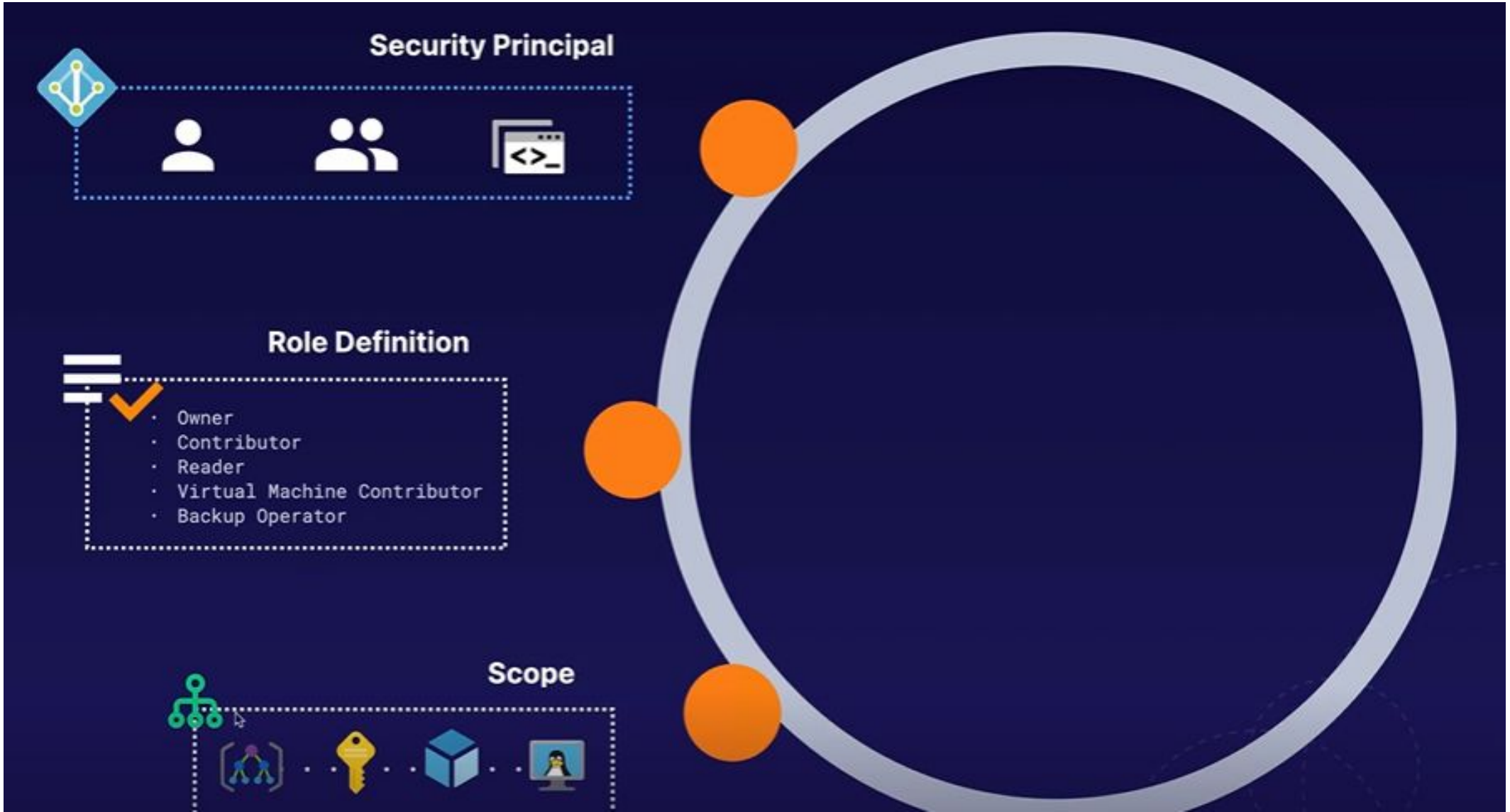
Secure Access to Azure Resources

Role-based access control (RBAC) allows us to implement secure access, following the principle of least privilege.

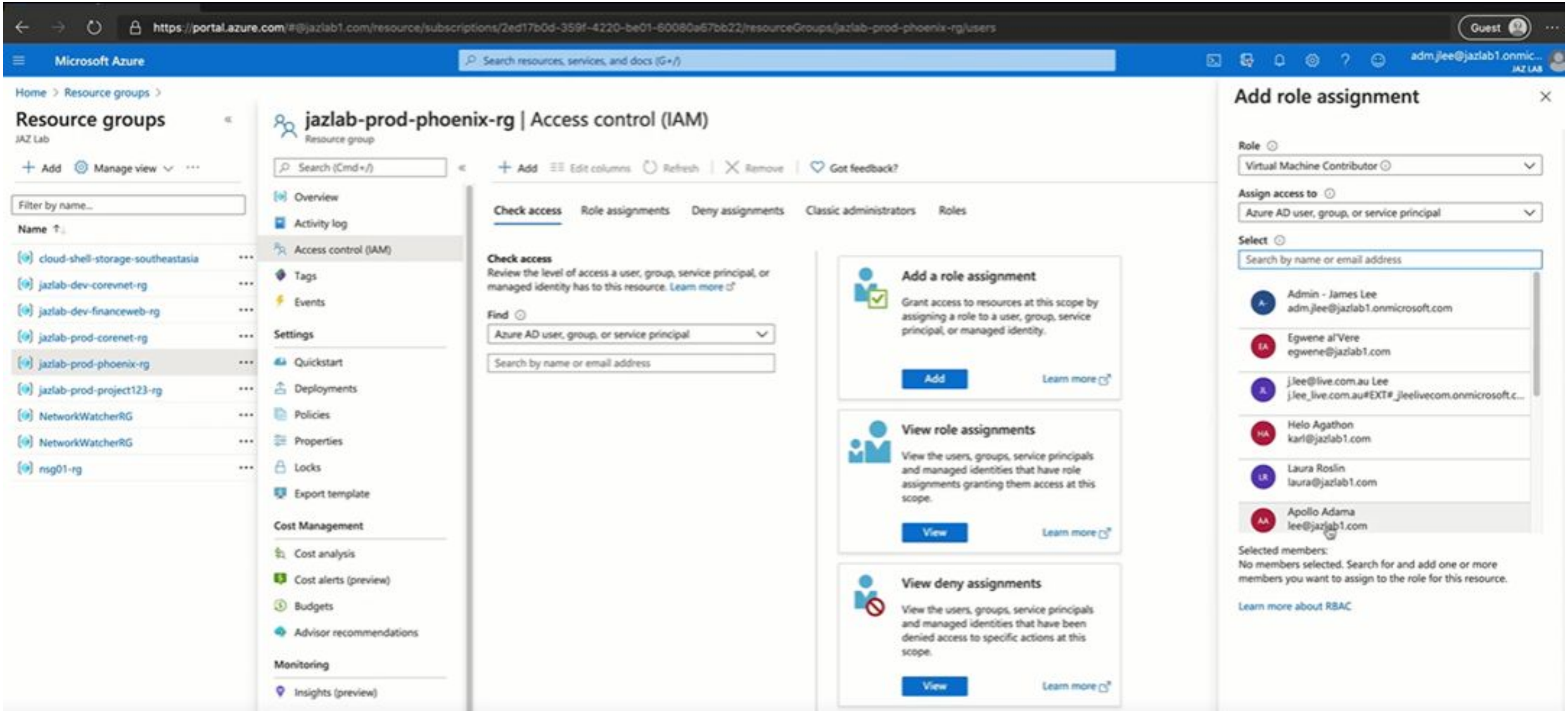
Through Azure RBAC, we can:

- Control access to Azure resources
- Configure permissions based on actual roles
- Define the permissions that are and are not allowed

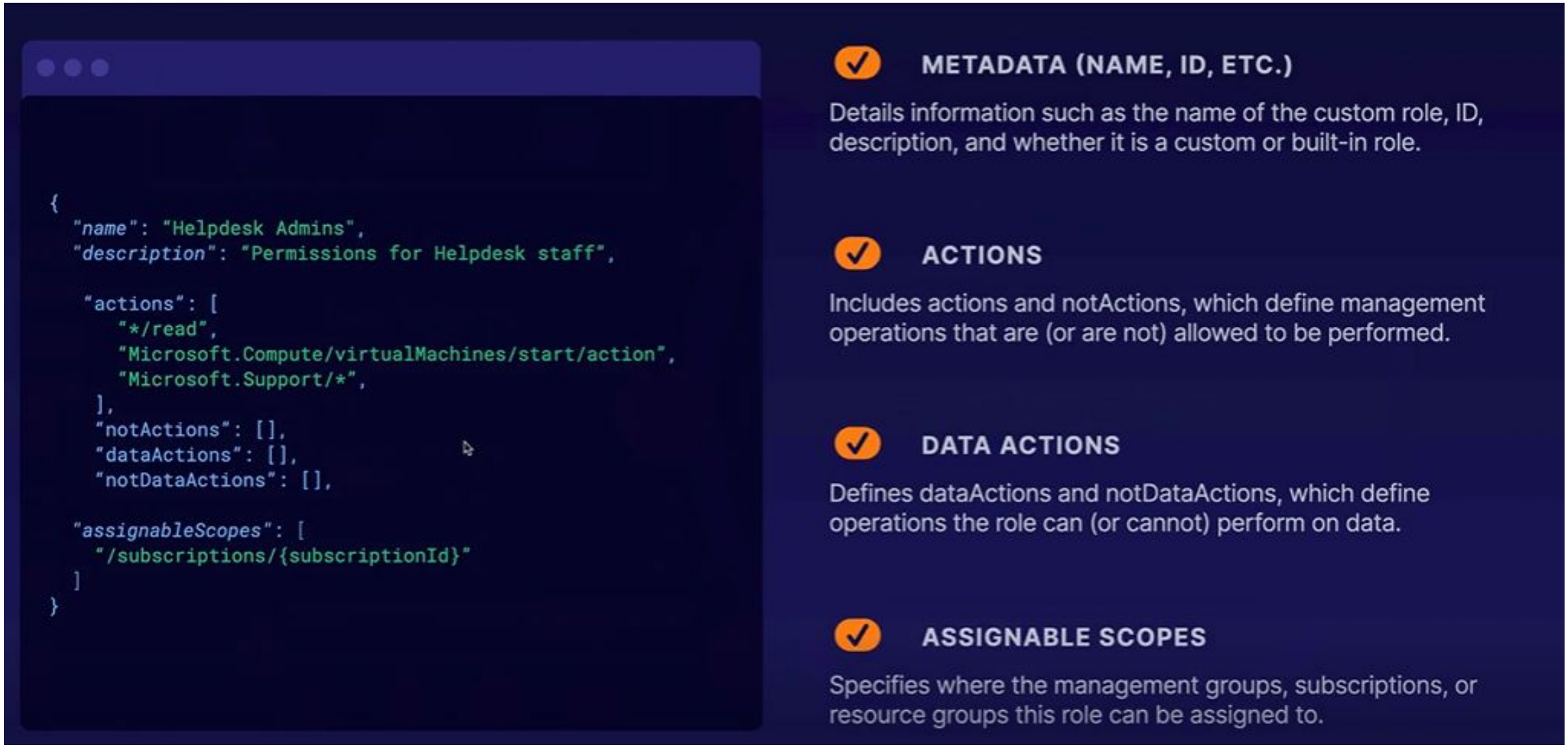
Role-Based Access Control – Key components



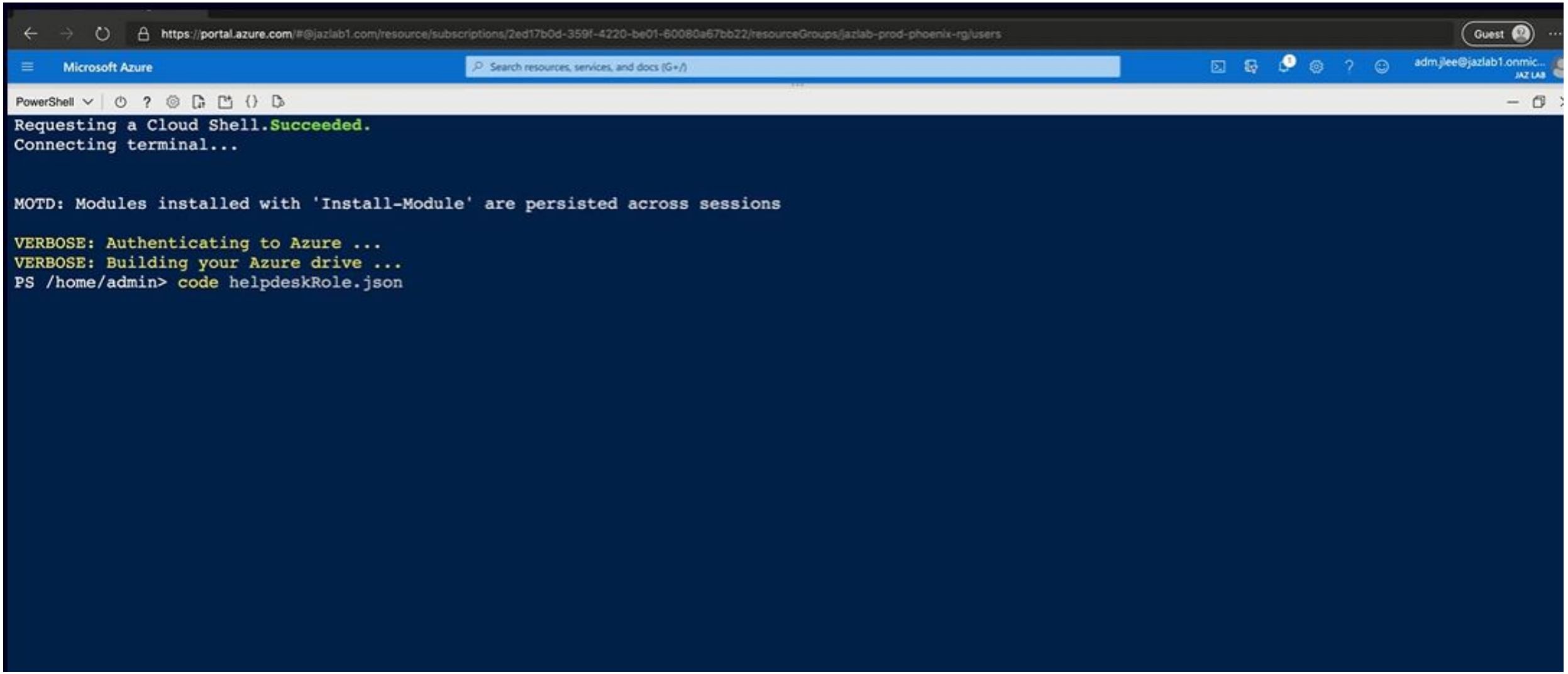
Role-Based Access Control



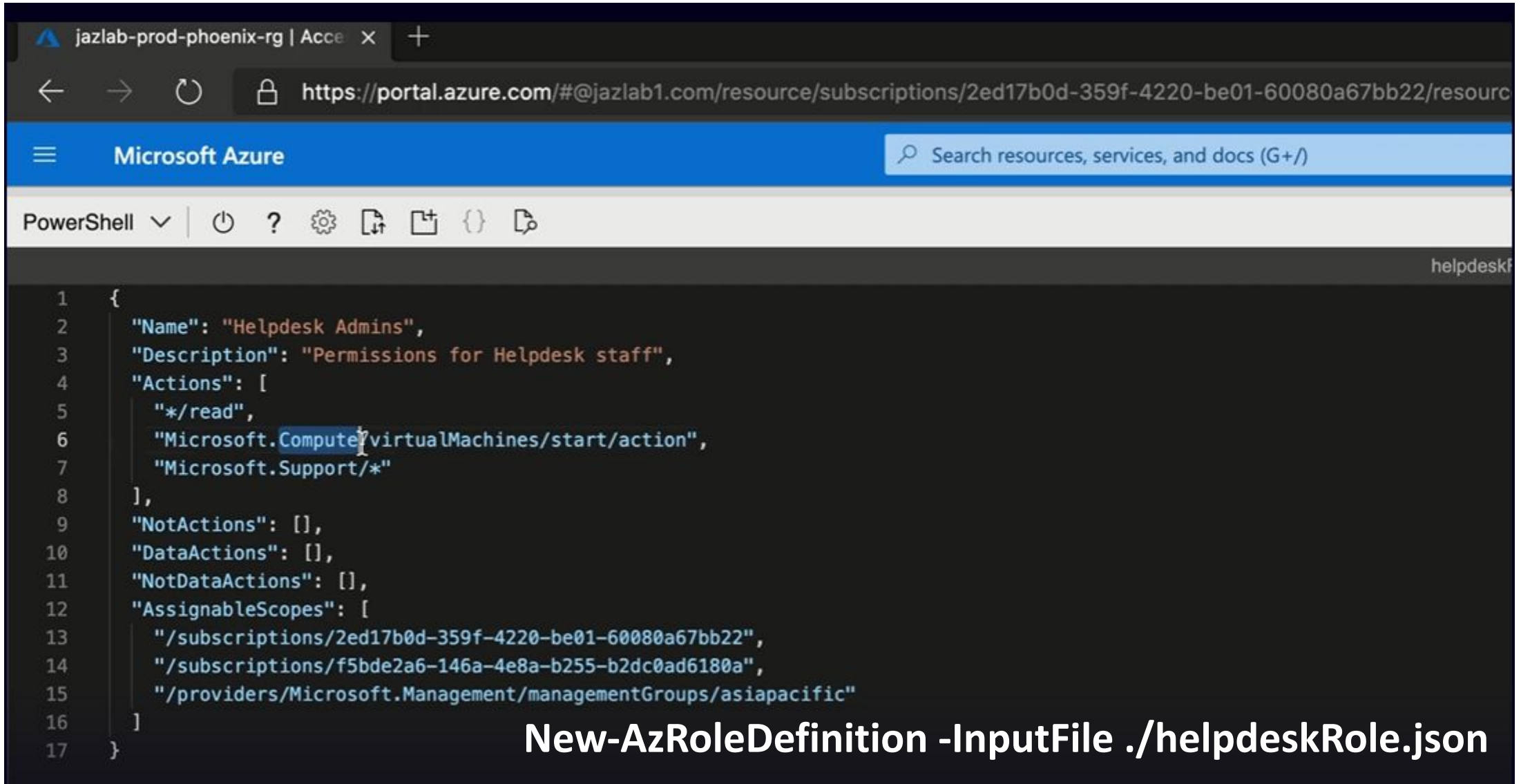
Role-Based Access Control – Custom RBAC Roles



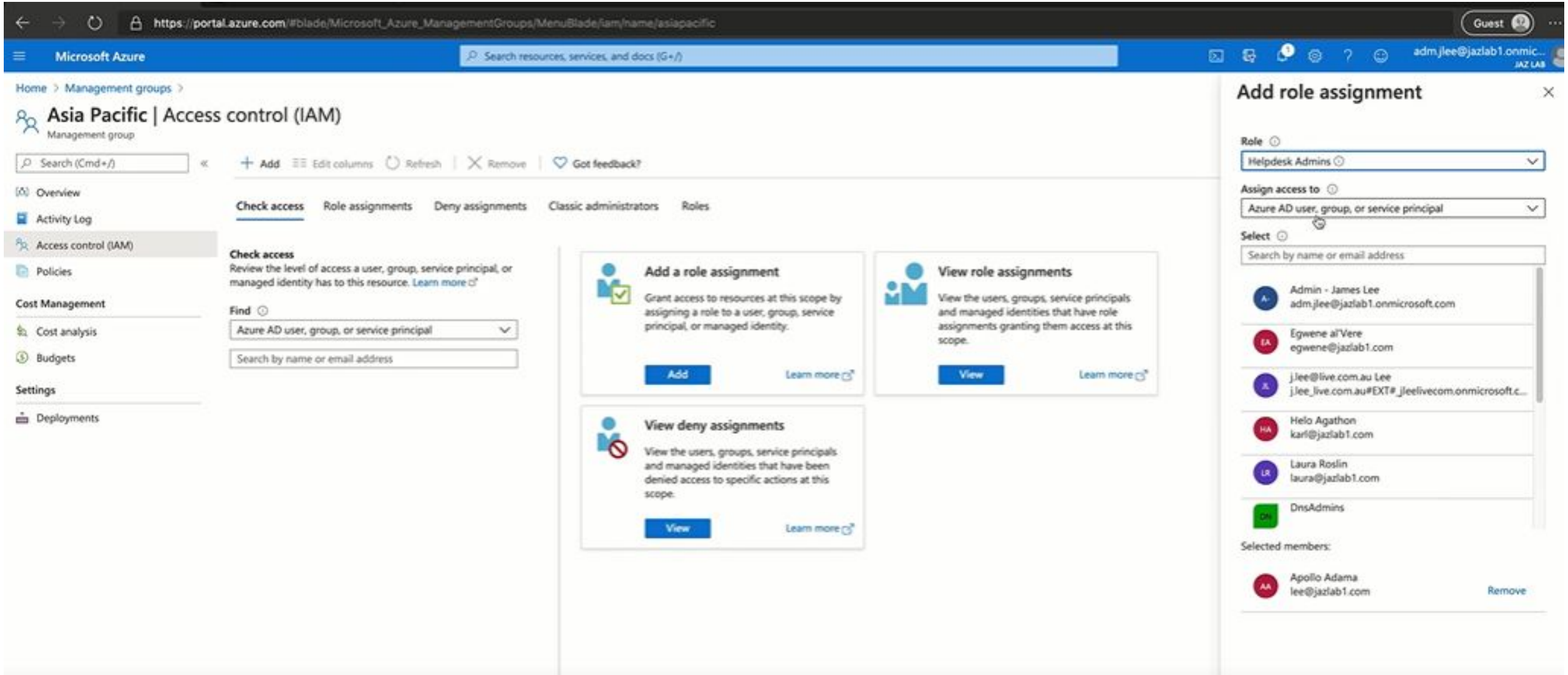
Role-Based Access Control



Role-Based Access Control



Role-Based Access Control



Azure Policy

Enforce and Audit Conventions for Azure Resources

Azure Policy helps to provide some much-needed control over an otherwise unlimited service - Azure.

Policies can help to:

- Enforce behavior, standards, and compliance
- Prevent (or audit) creation of non-compliant resources
- For example: restrict the allowed virtual machine sizes

Azure Policy – How it works

Monitor for a Condition

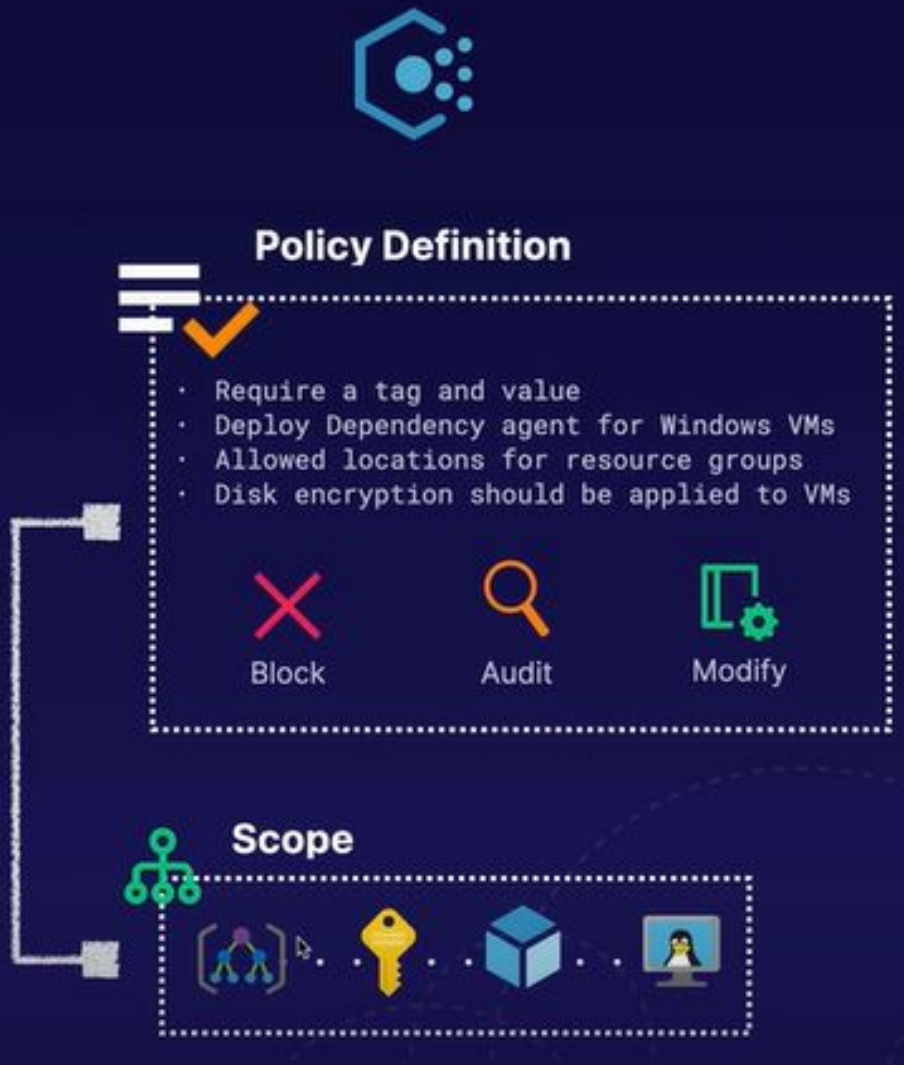
- Look at a resource property for a given value
- Specified within a Policy Definition
- E.g., does the resource "location" = "US West"

Trigger an Effect

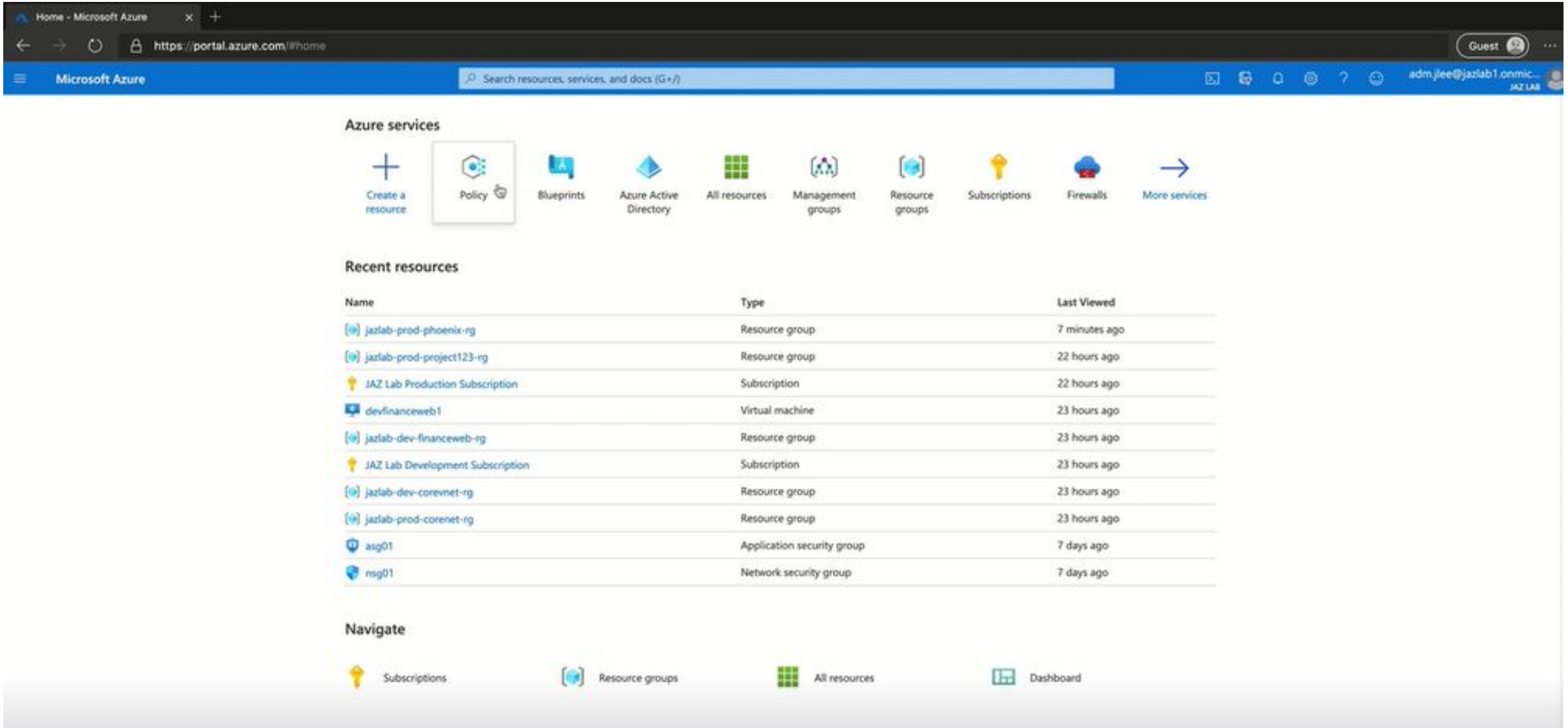
- Action to occur if the condition is met
- Azure Policy supports a range of effects, for example: append, audit, deny, modify

Assignment

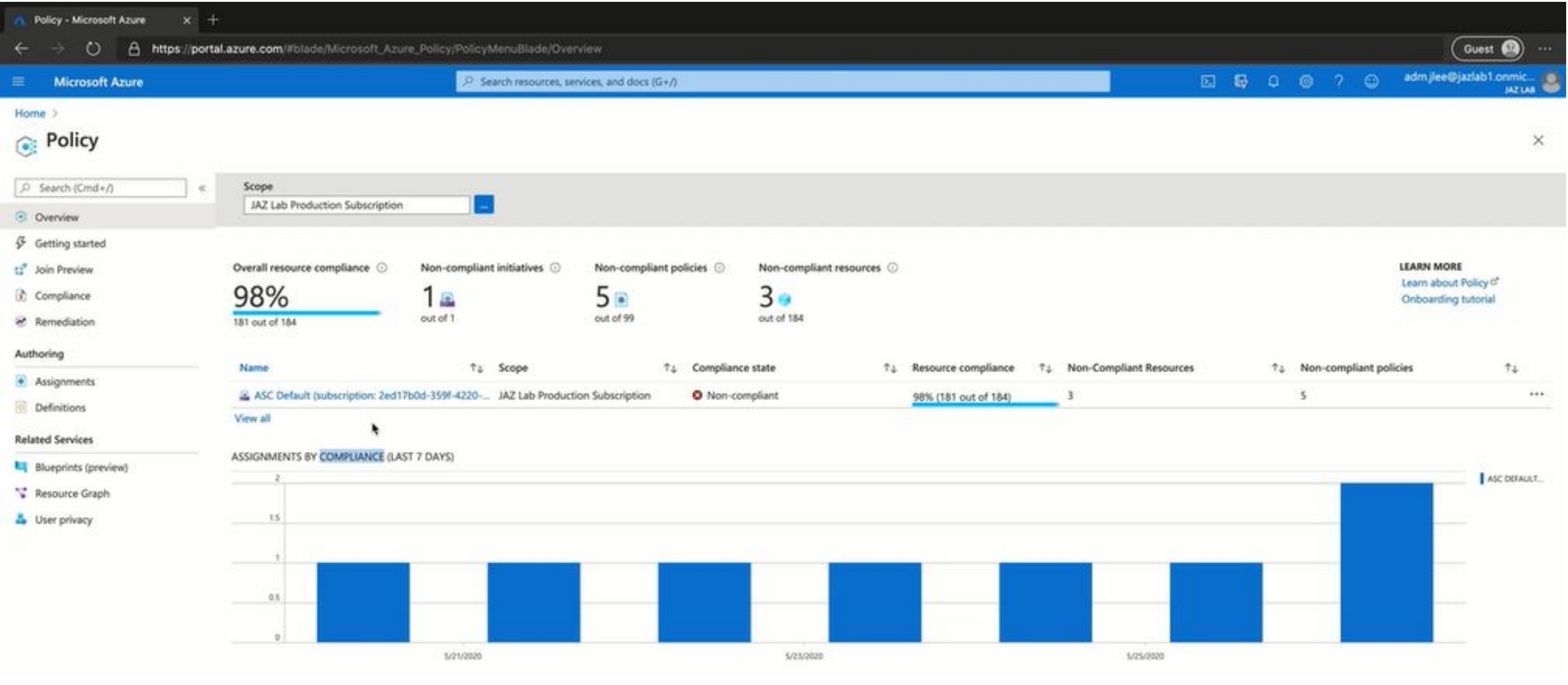
- Policies must be assigned to a scope
- Scopes can include a resource, resource group, subscription, or management group



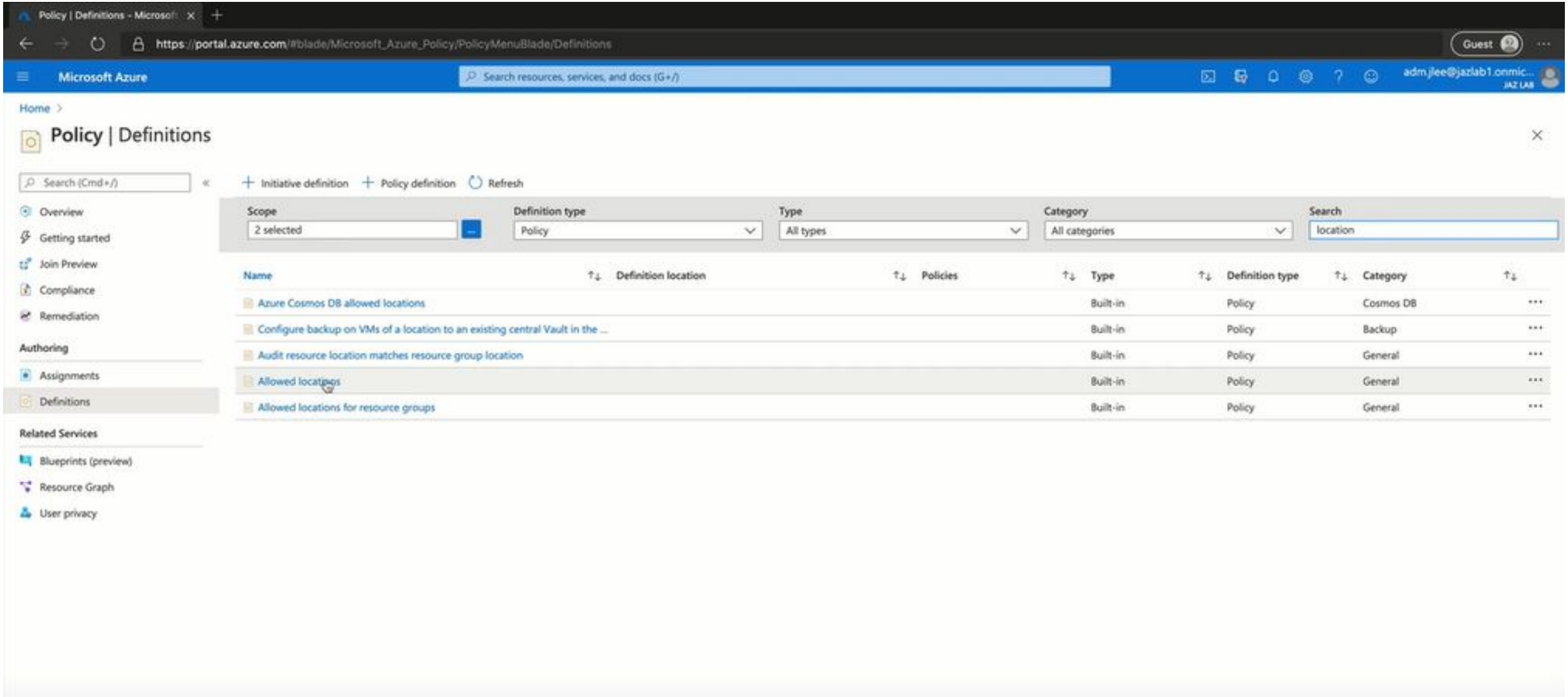
Azure Policy – How it works



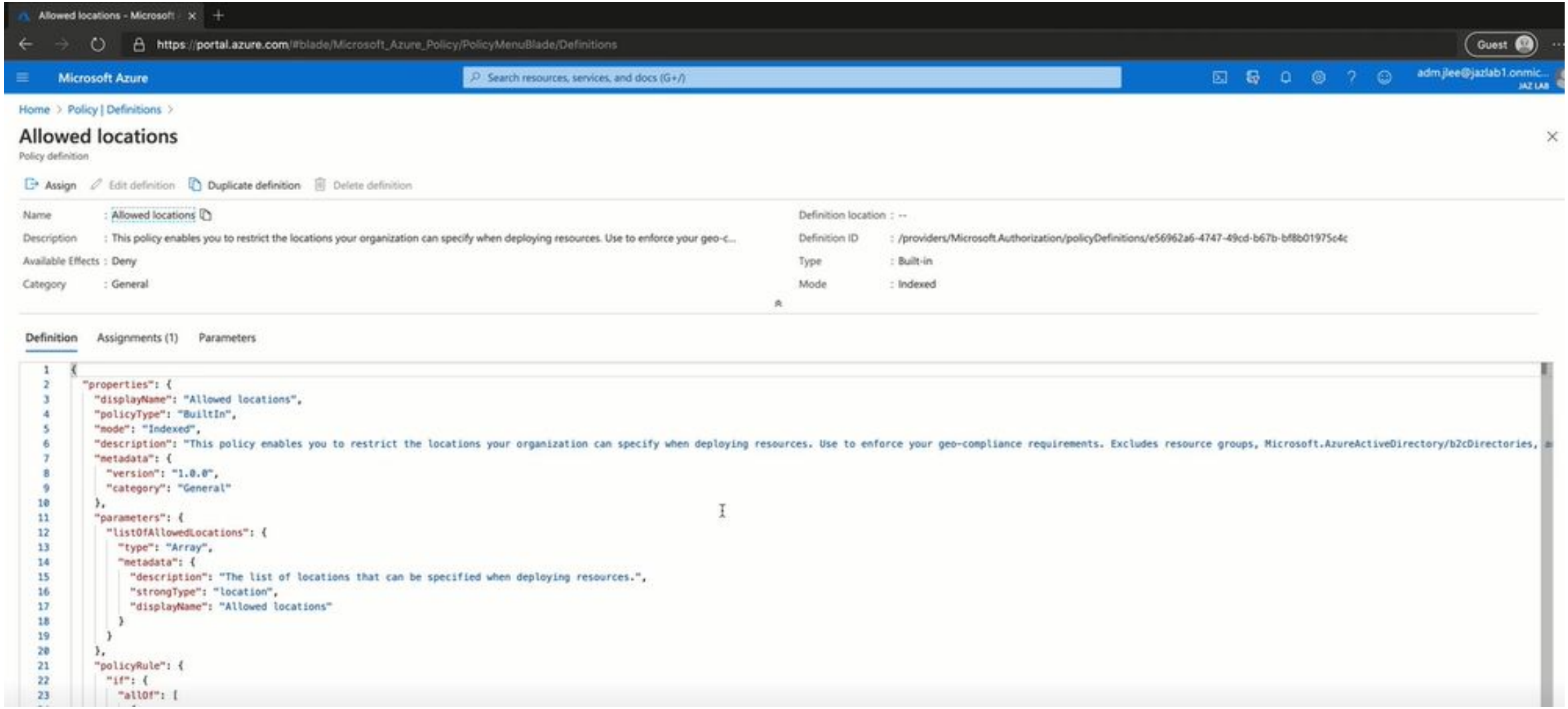
Azure Policy – How it works



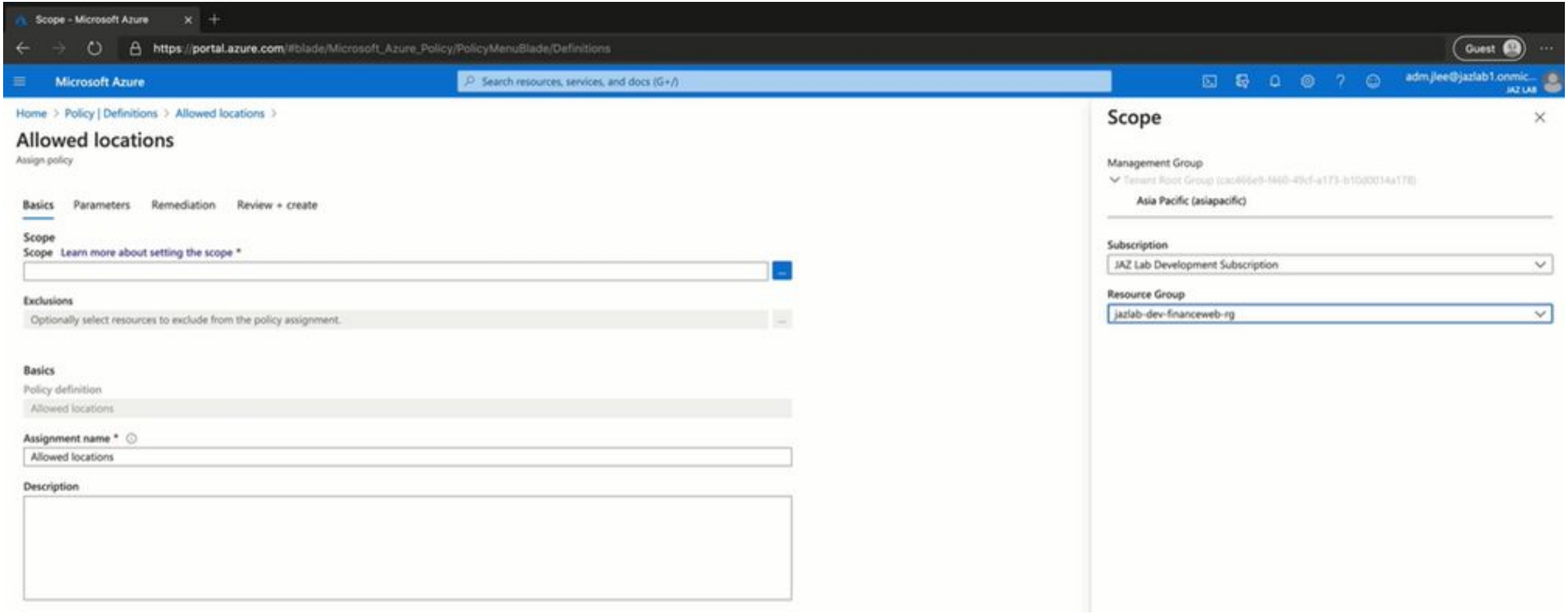
Azure Policy – How it works



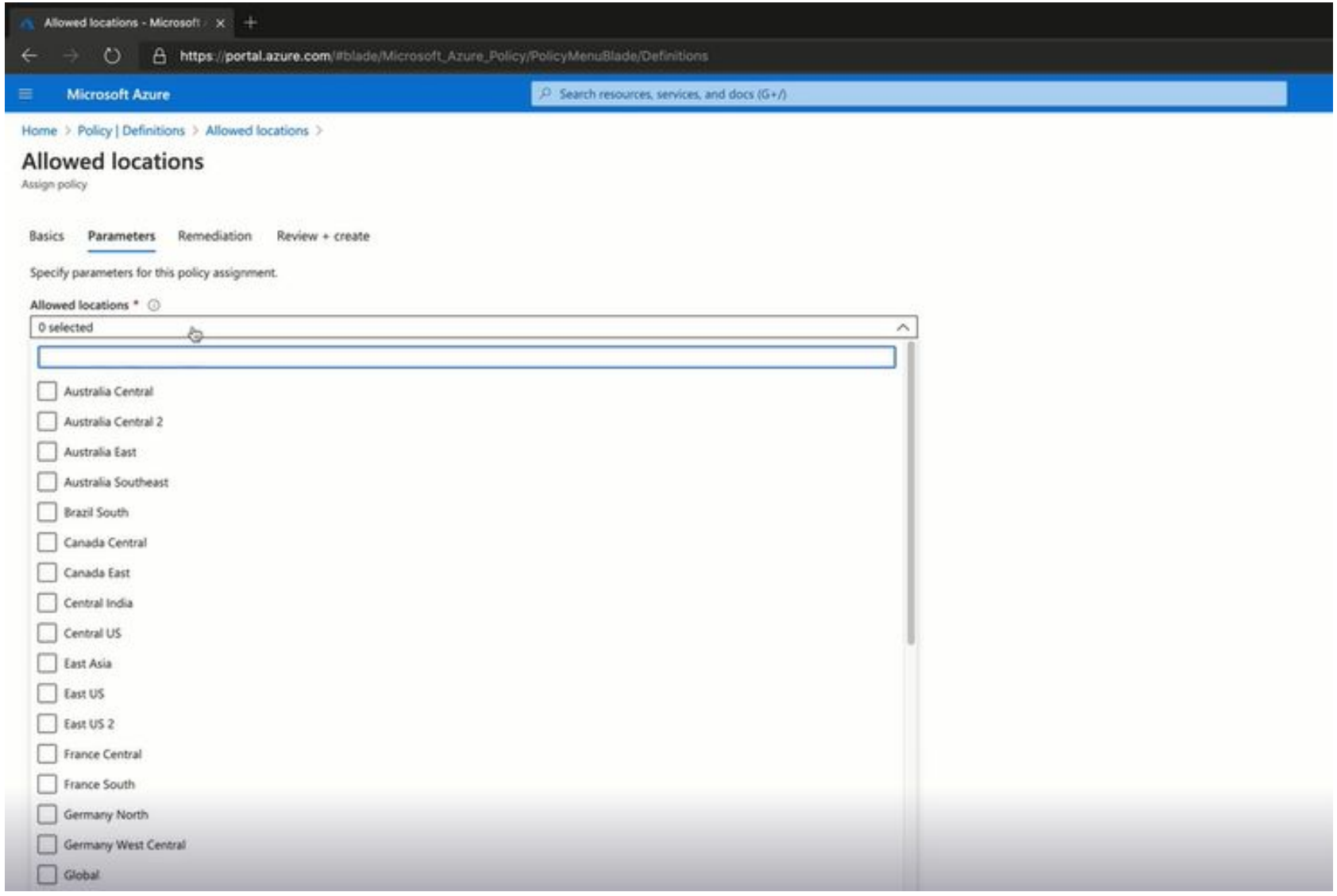
Azure Policy – How it works



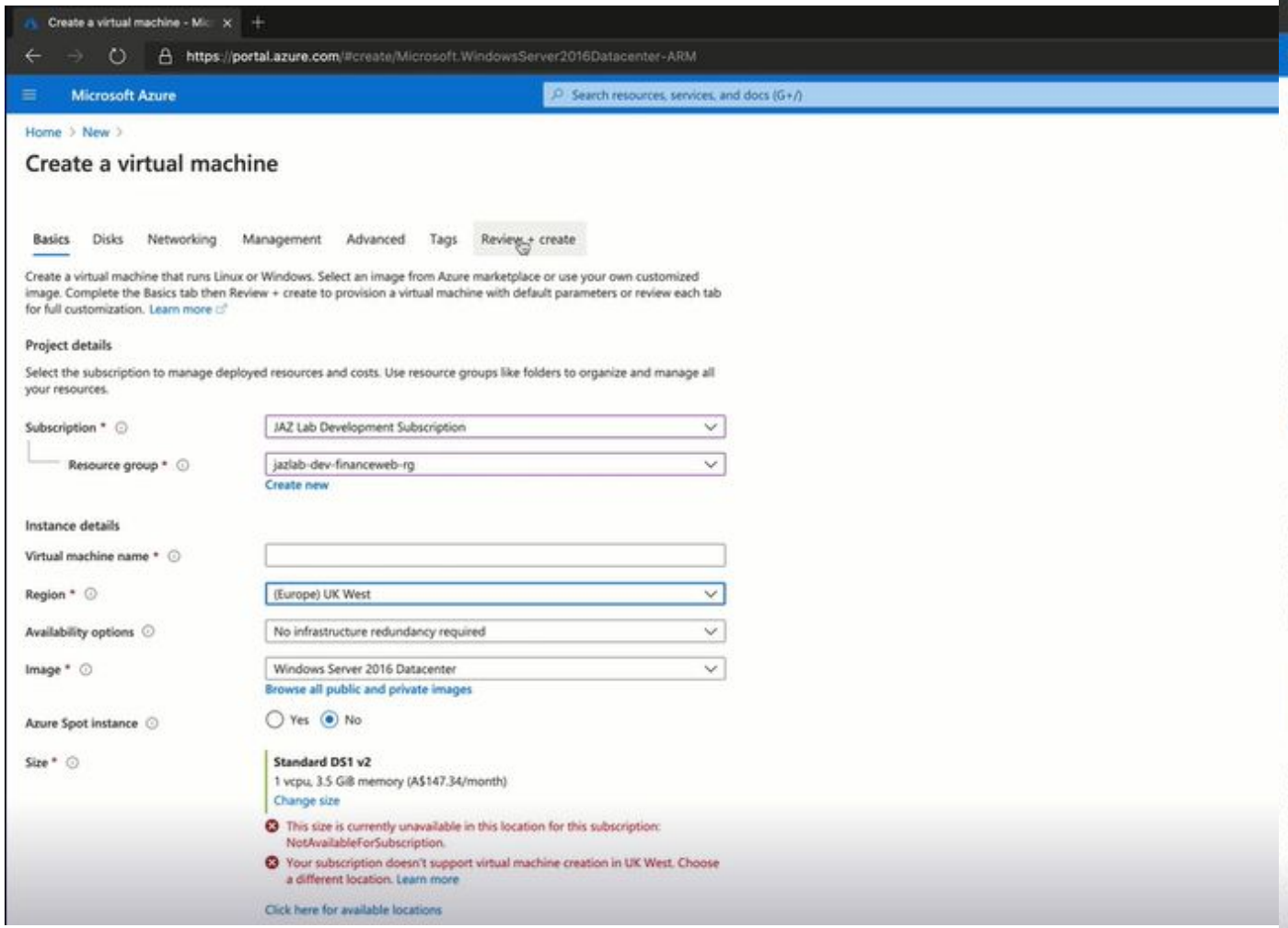
Azure Policy – How it works

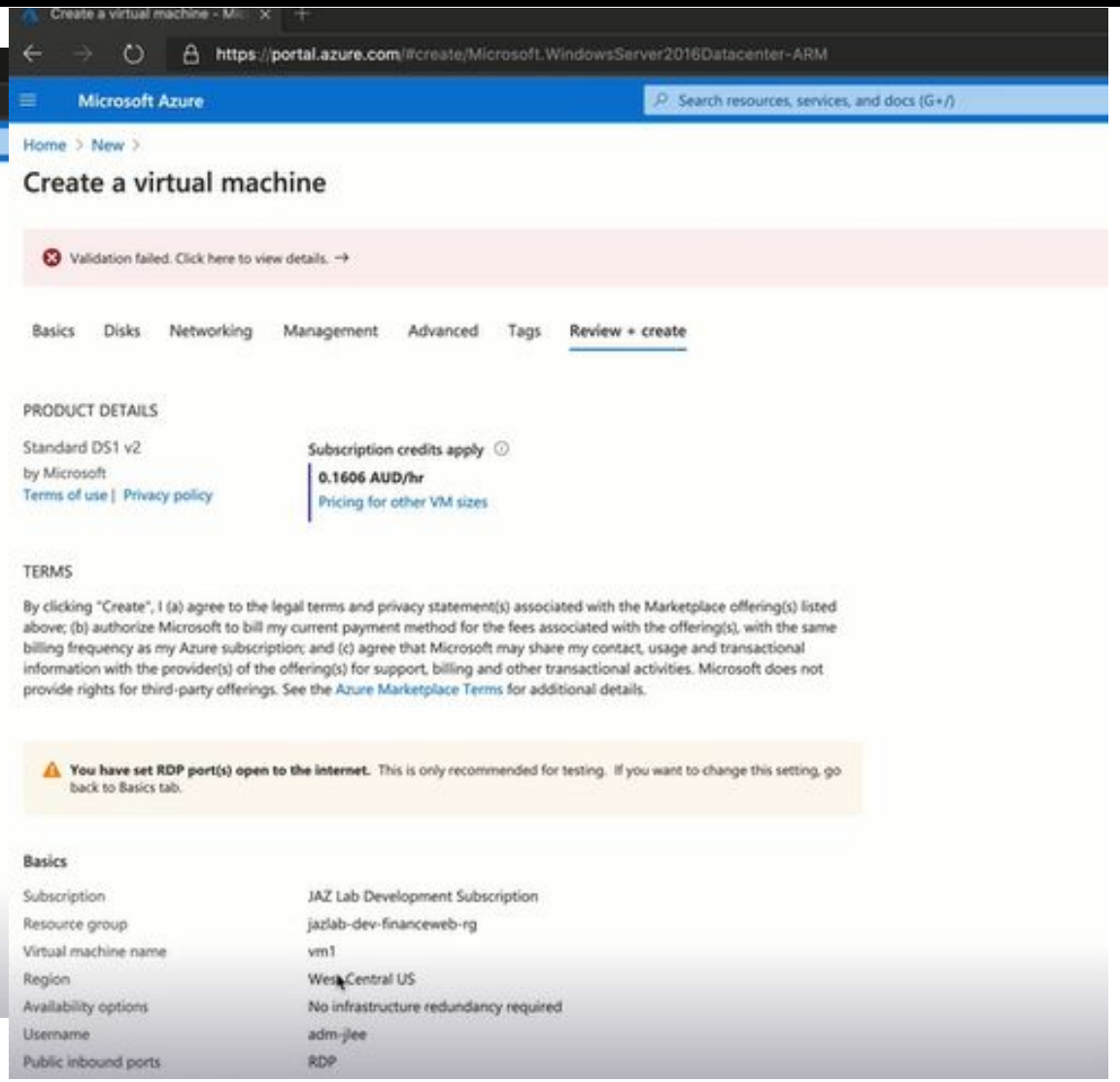


Azure Policy – How it works

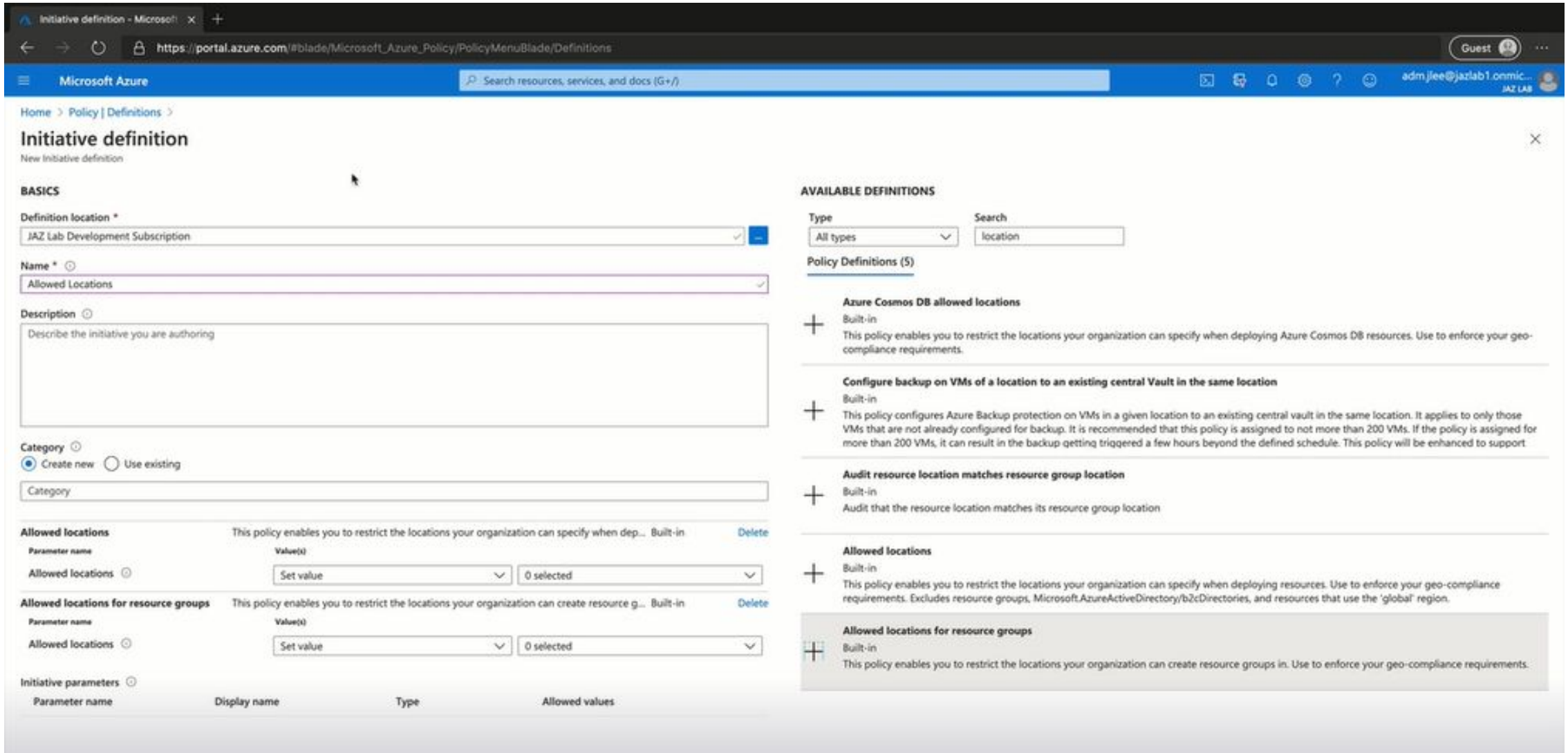


Azure Policy – How it works

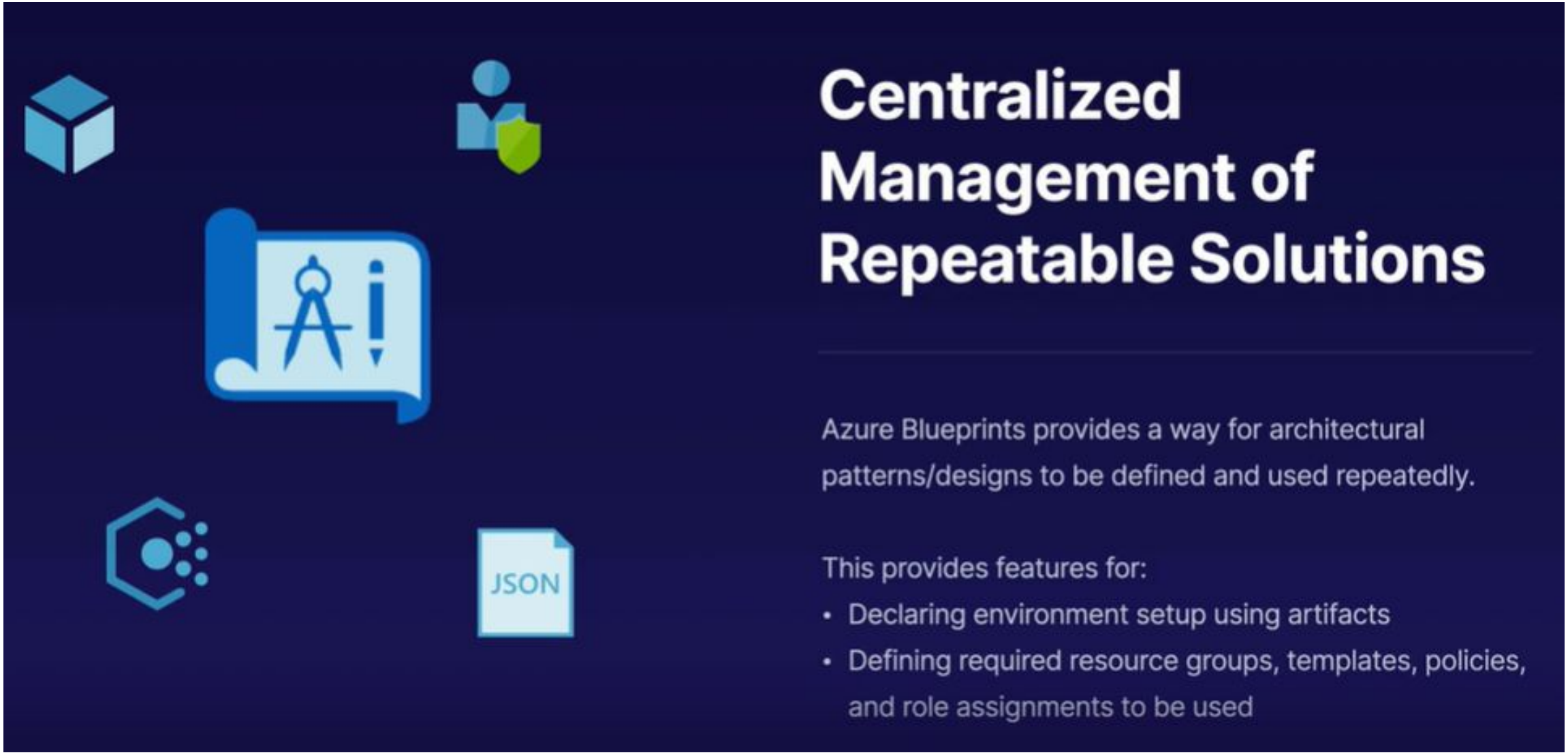




Azure Policy – How it works



Azure Blueprints



Centralized Management of Repeatable Solutions

Azure Blueprints provides a way for architectural patterns/designs to be defined and used repeatedly.

This provides features for:

- Declaring environment setup using artifacts
- Defining required resource groups, templates, policies, and role assignments to be used

Azure Blueprints

Blueprint Definition

- A definition of a given environment/solution
- Includes artifacts (ARM templates, Azure Policy, RBAC, resource groups)

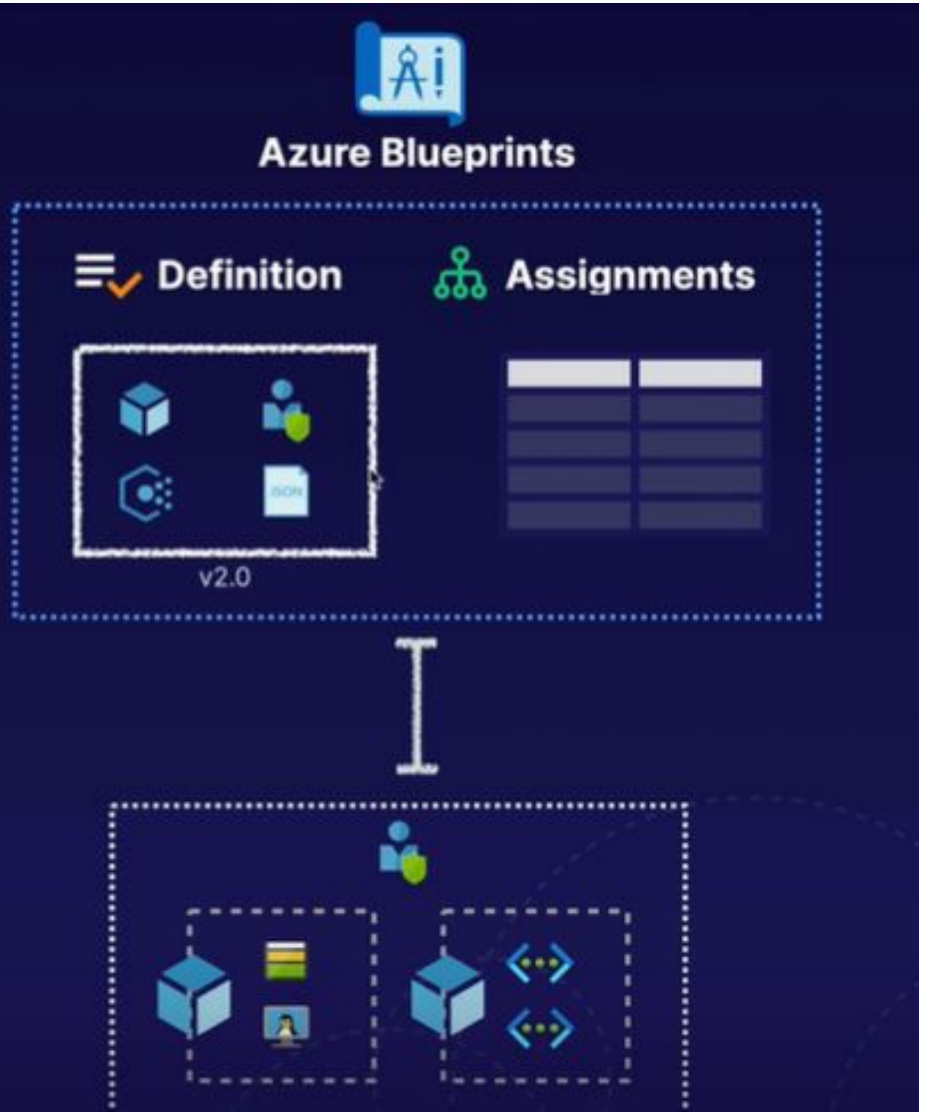
Publishing and Version Control

v2.0

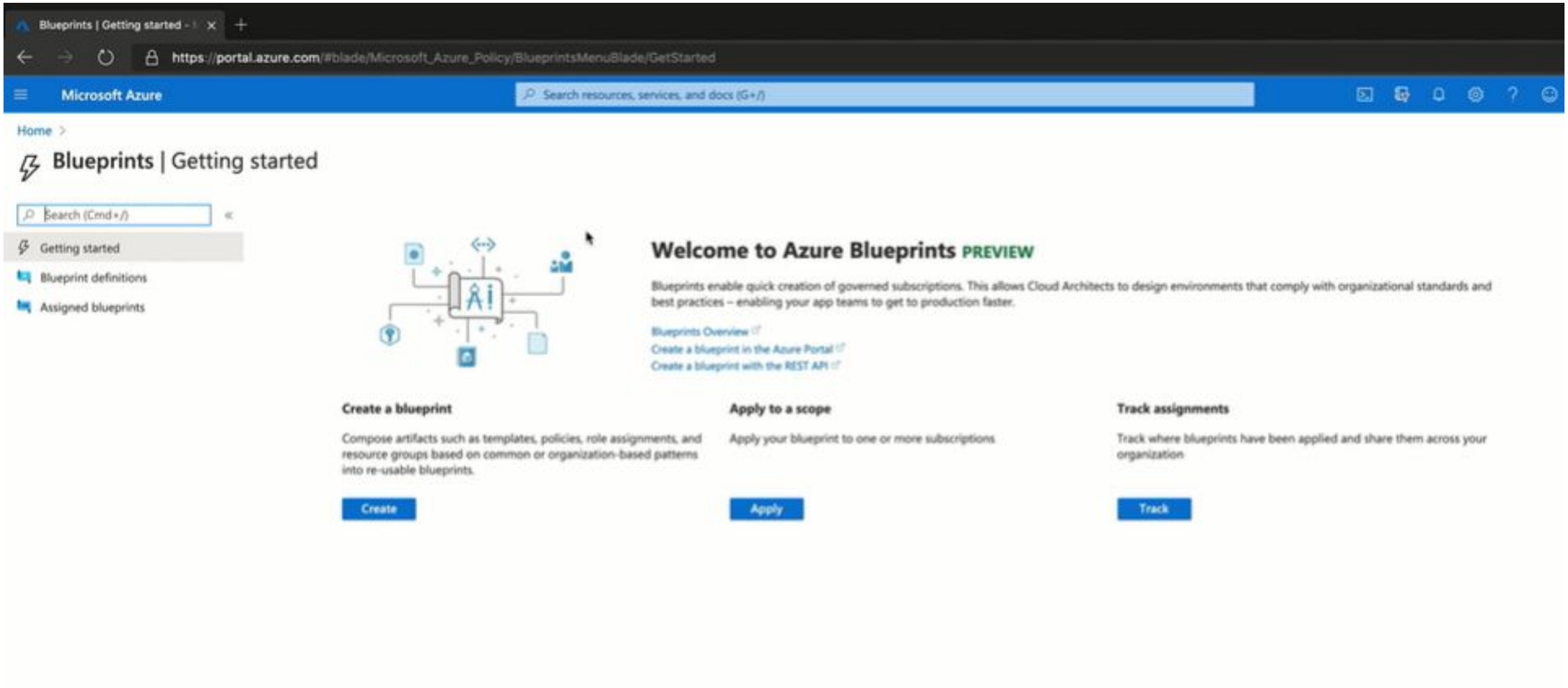
- For a Blueprint to be used, it must be published
- Publishing supports the use of version control to better manage artifacts and definitions

Assignments

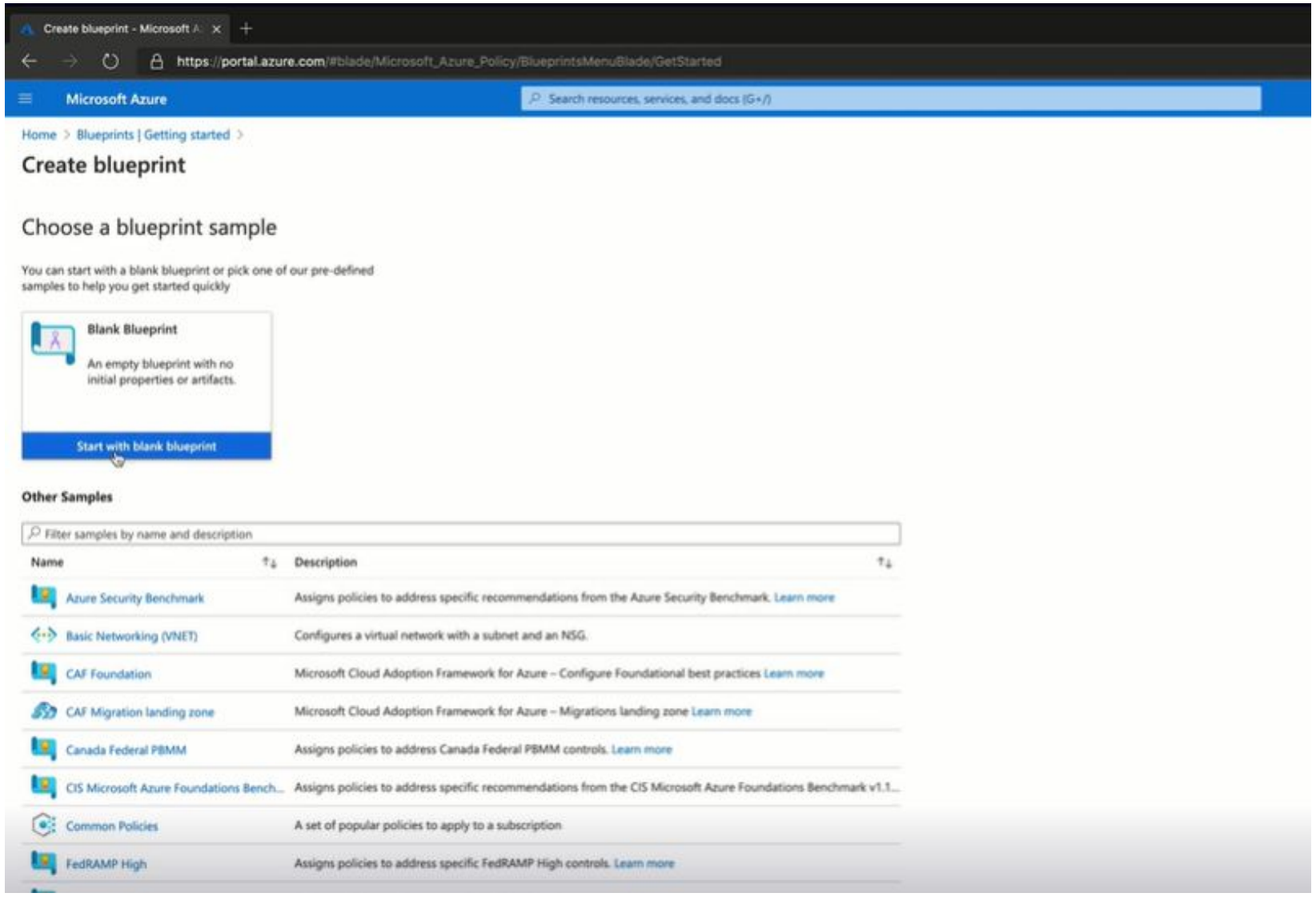
- Building something with a Blueprint creates an "assignment"
- Assignments provide an audit trail



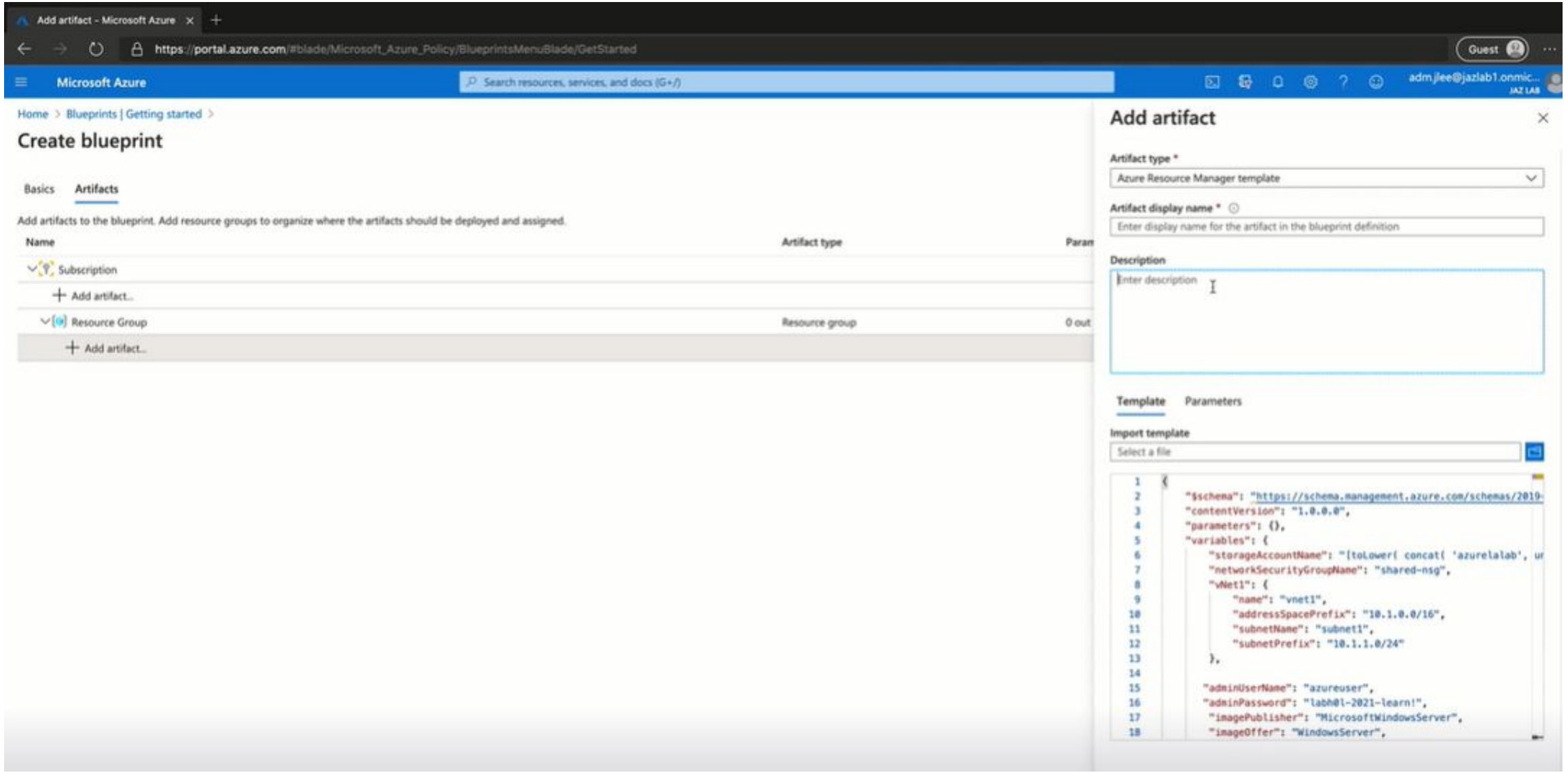
Azure Blueprints



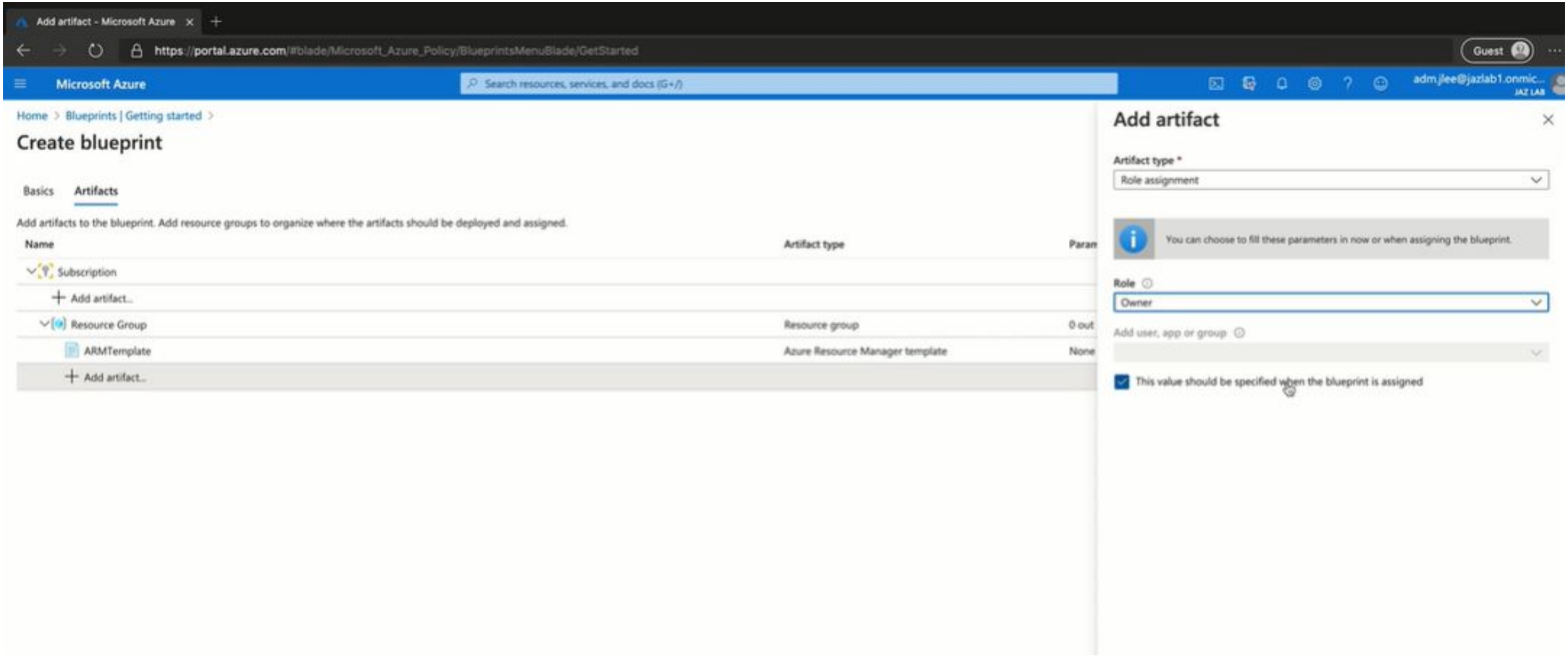
Azure Blueprints



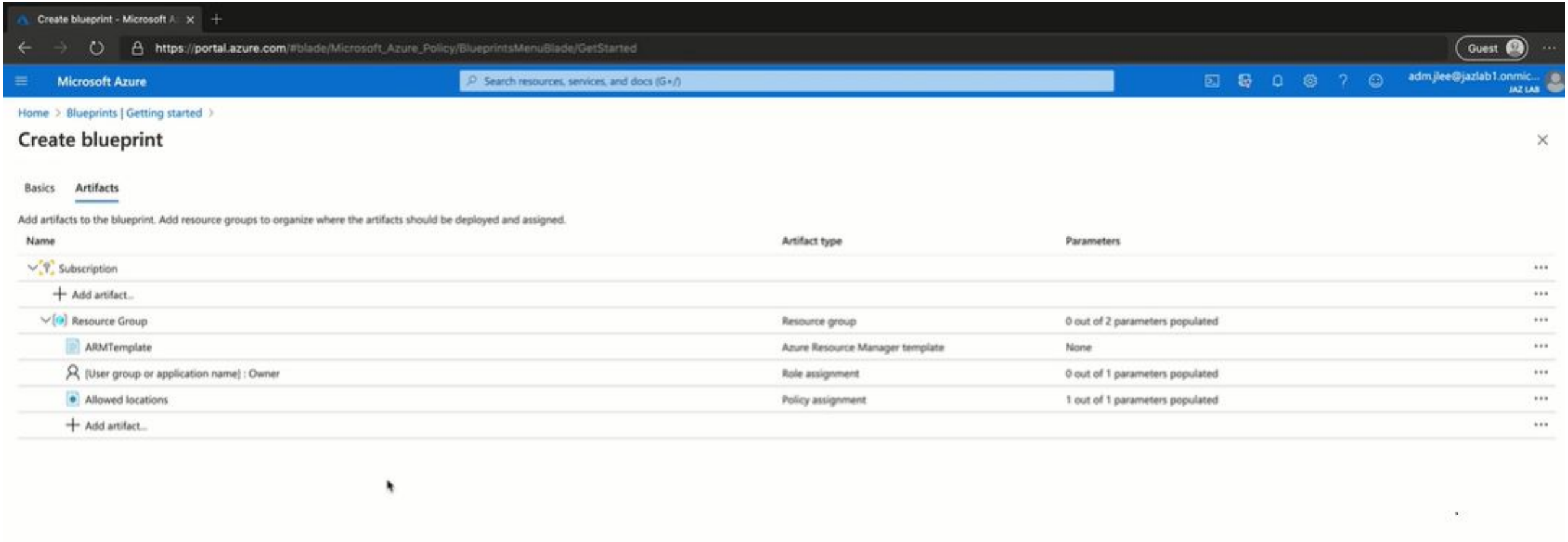
Azure Blueprints



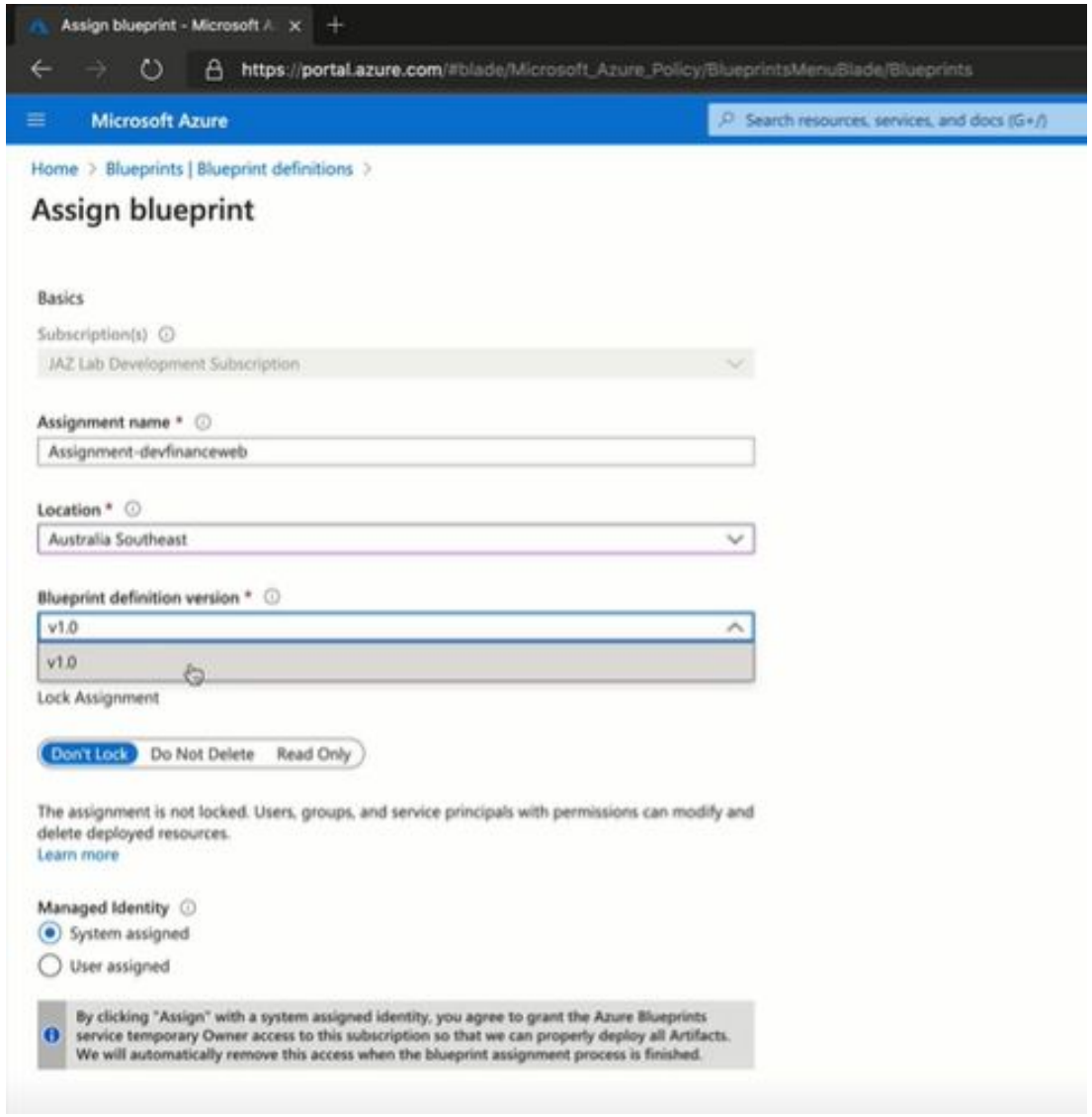
Azure Blueprints



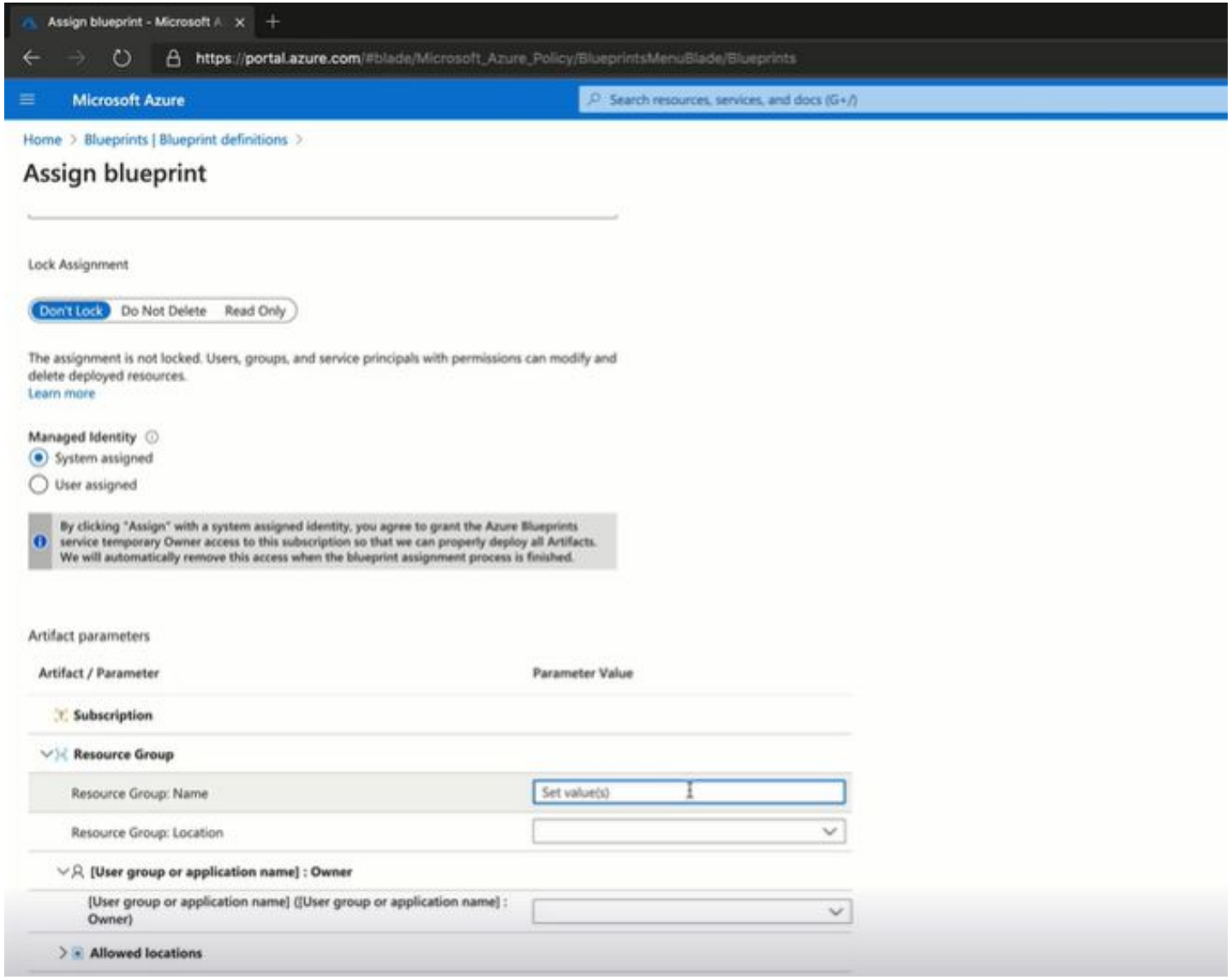
Azure Blueprints



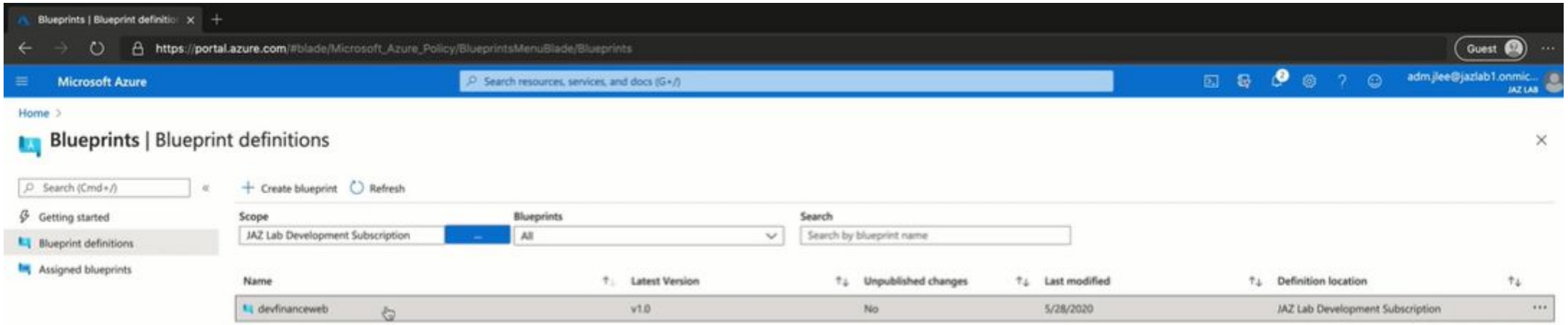
Azure Blueprints

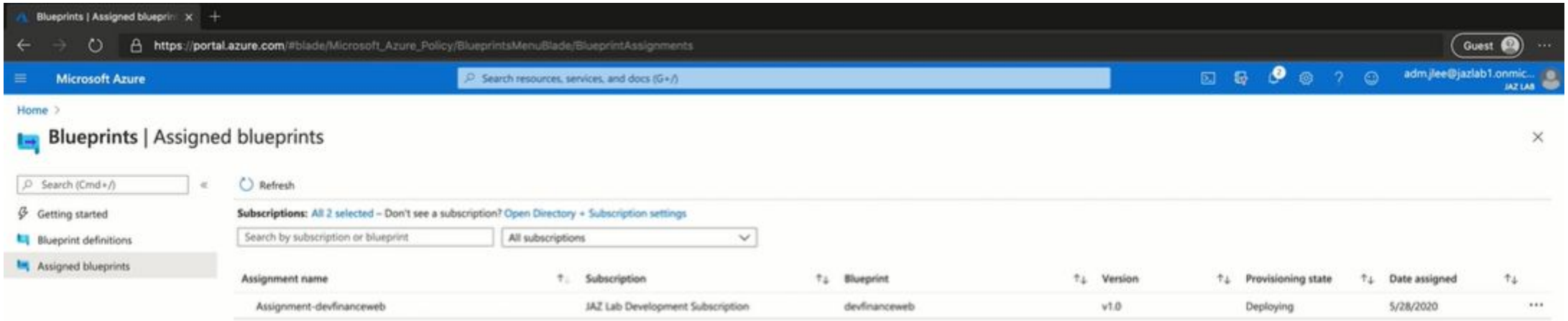


Azure Blueprints



Azure Blueprints





Azure AD Access Reviews

Streamlined Access Management and Monitoring

Azure Active Directory (AD) Access Reviews provide a simplified approach to manage ongoing access.

The key features include:

- Removing access which is no longer required
- Self-service to reduce IT admin workloads
- Management of Azure AD and Azure resource access

Azure AD Access Reviews - Implementation

Onboard the Azure AD Tenant

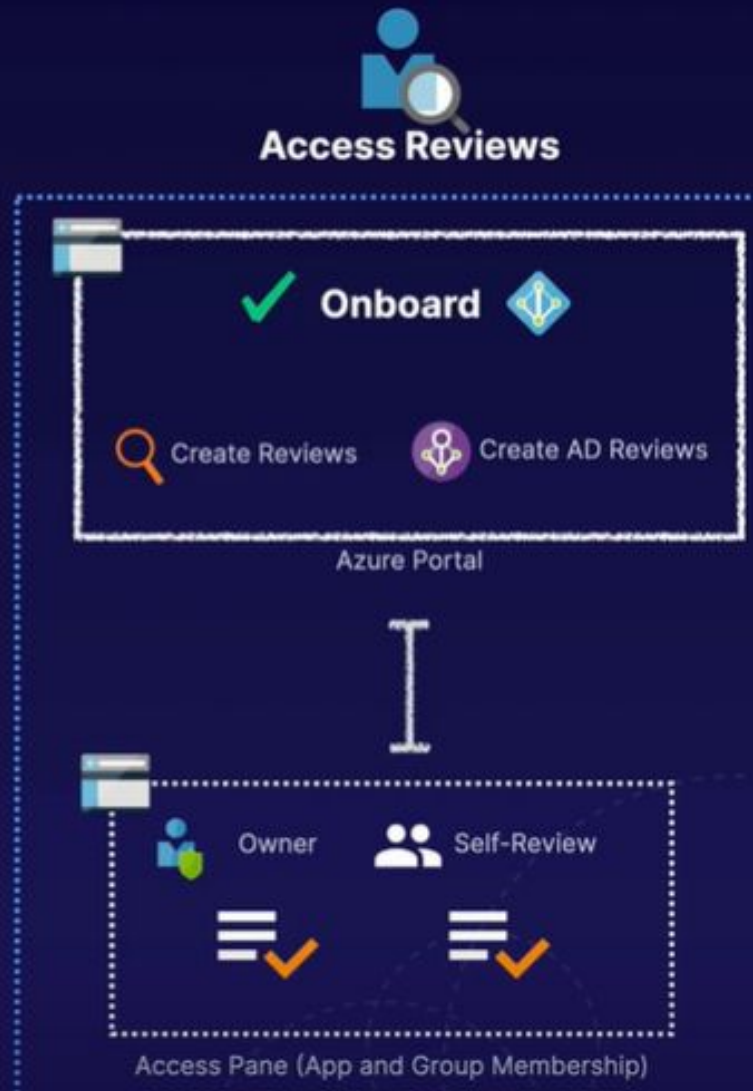
- Onboarding provides administrator consent for the use of Access Reviews, per tenant
- Azure AD P2 licensing is required

Access Reviews

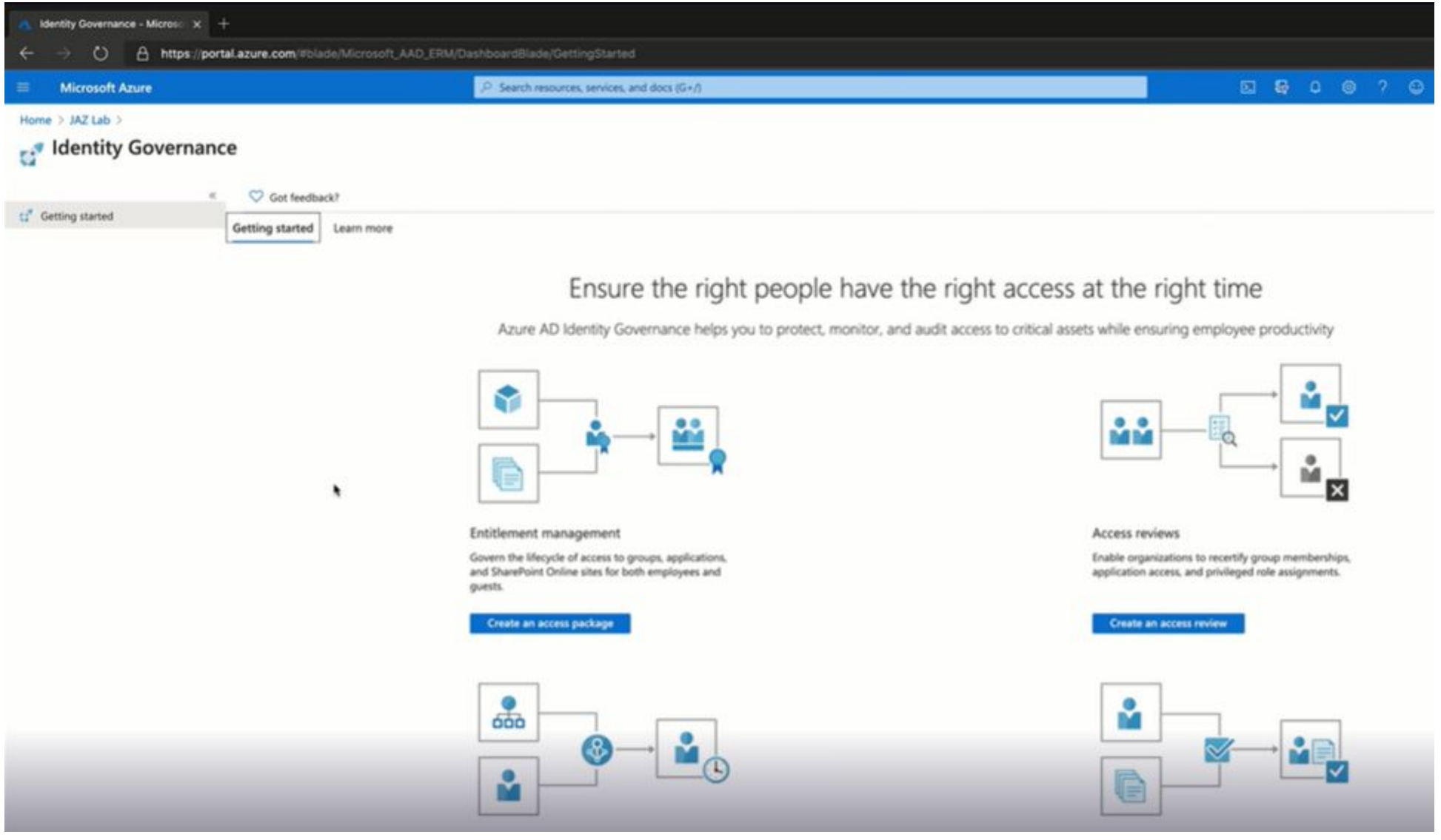
- Supports security group and app reviews
- Supports reviewers such as self, owner, etc.
- Access is reviewed through the Access Pane

Azure AD Privileged Role Reviews

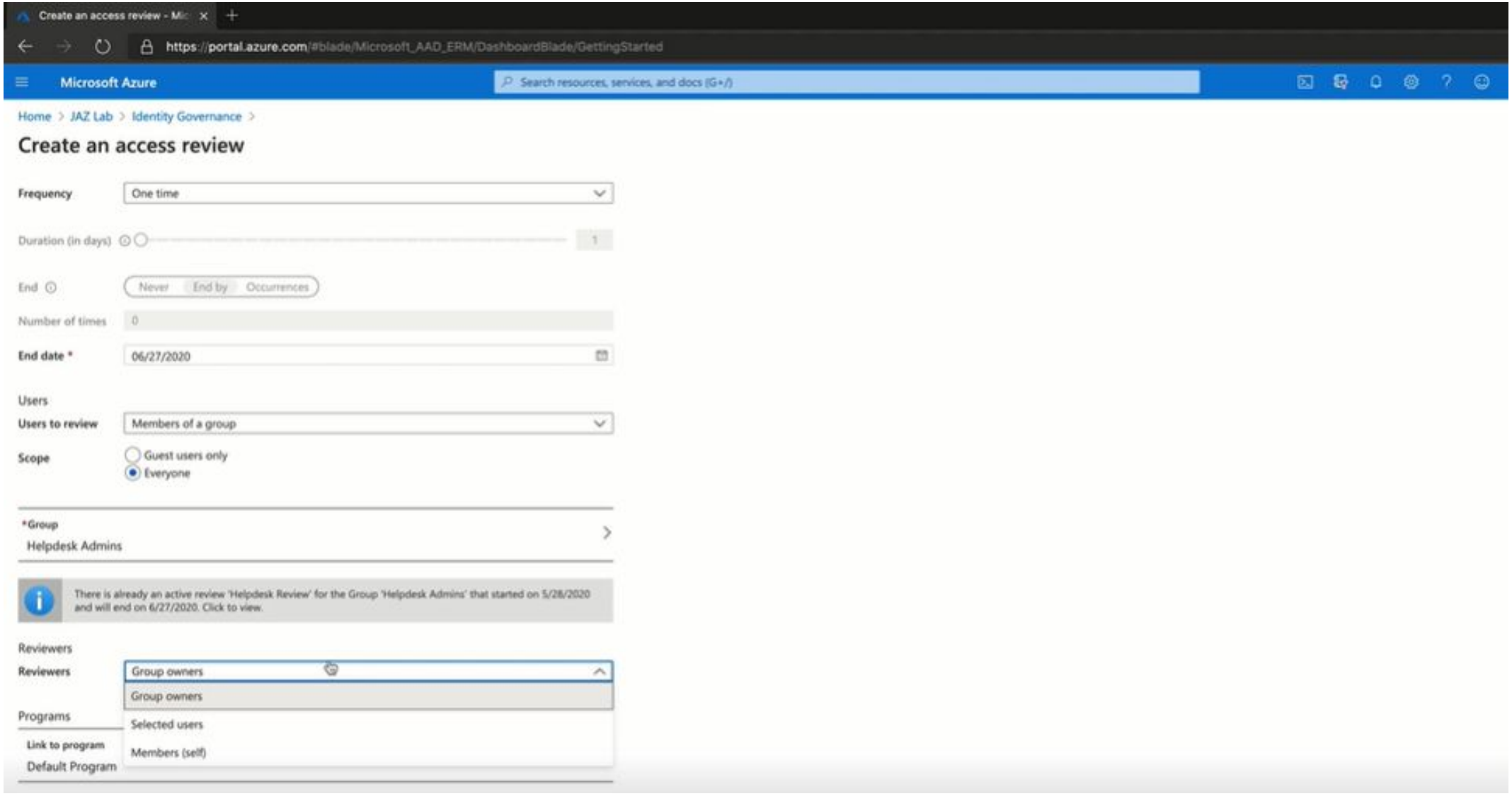
- Supports Azure AD role reviews
- Currently managed through Azure AD PIM
- Access is reviewed through the Azure Portal



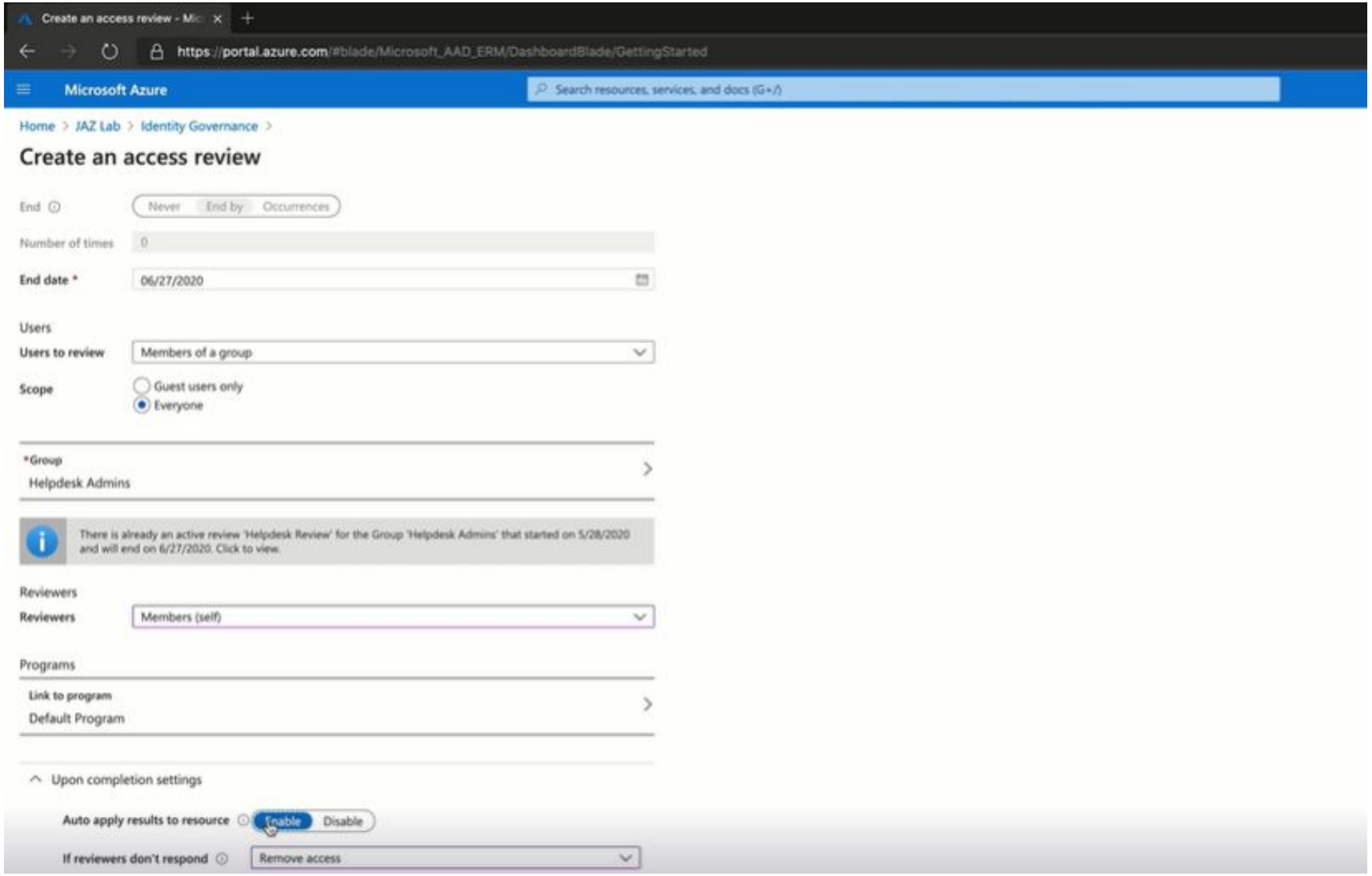
Azure AD Access Reviews - Implementation



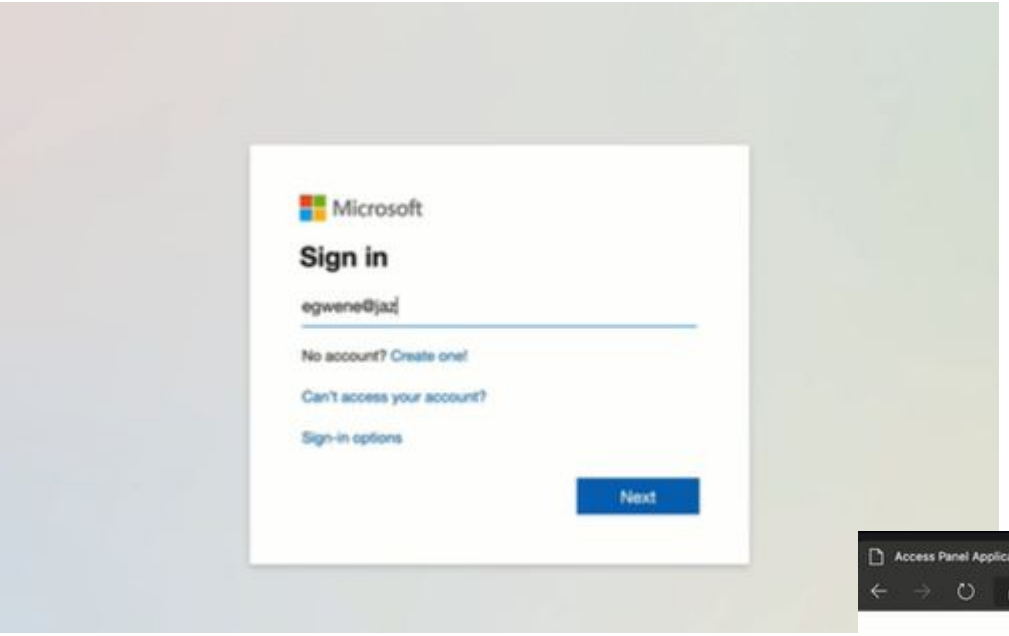
Azure AD Access Reviews - Implementation

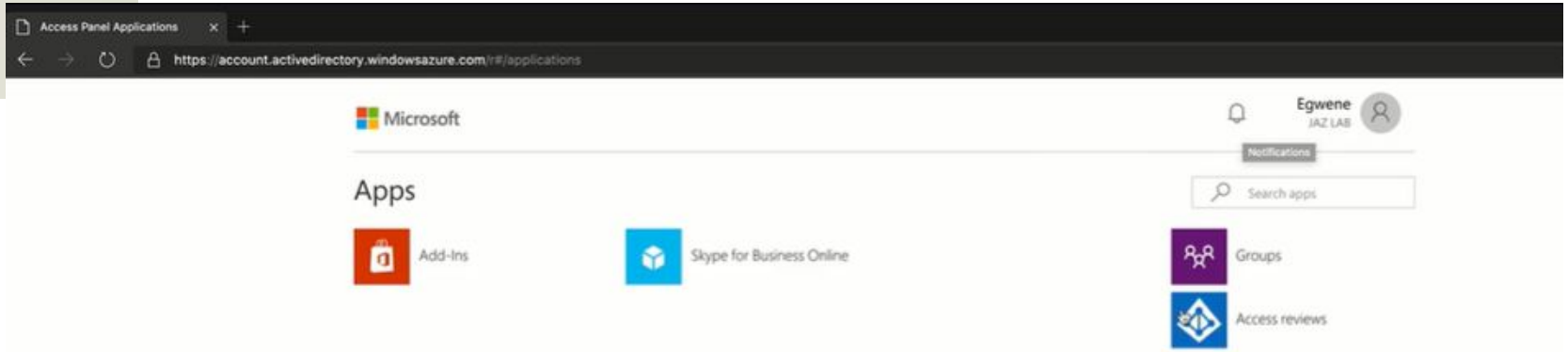


Azure AD Access Reviews - Implementation

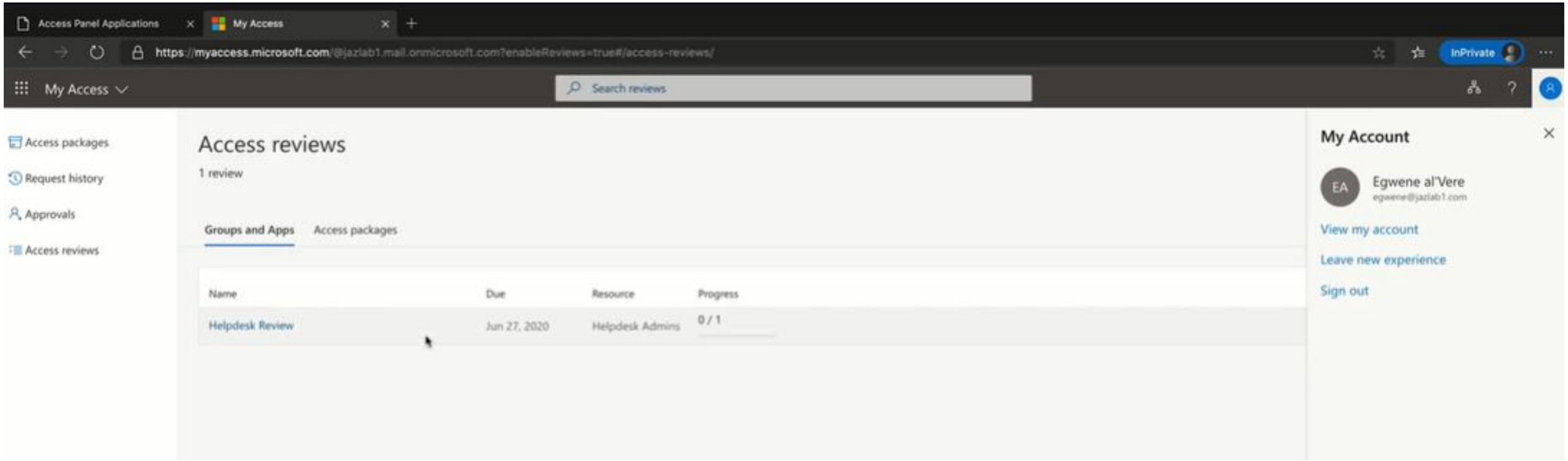


Azure AD Access Reviews - Implementation

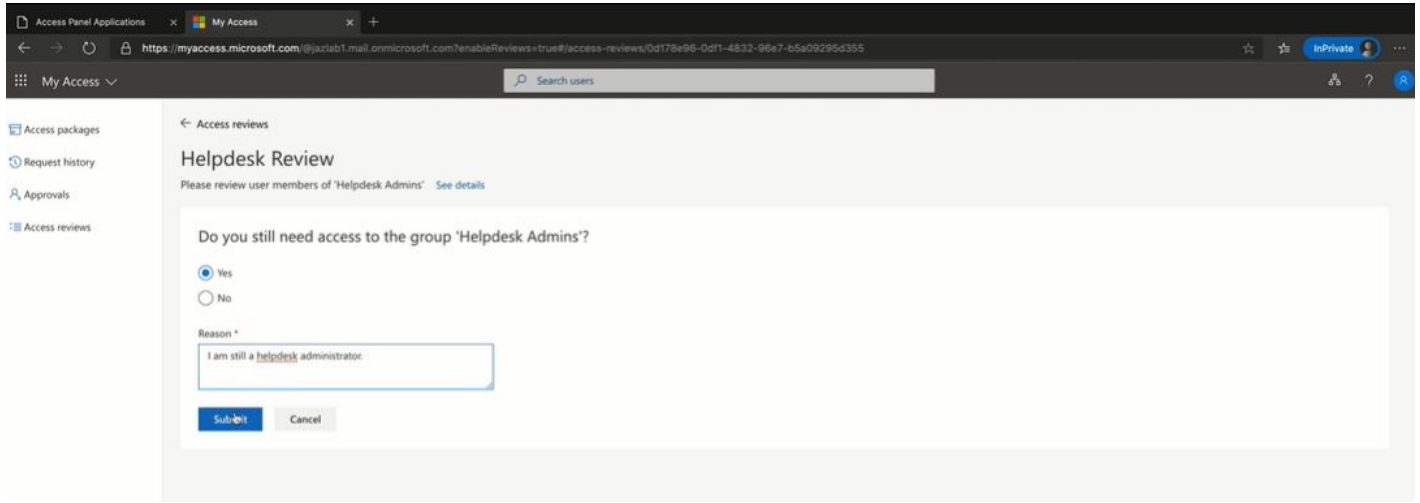


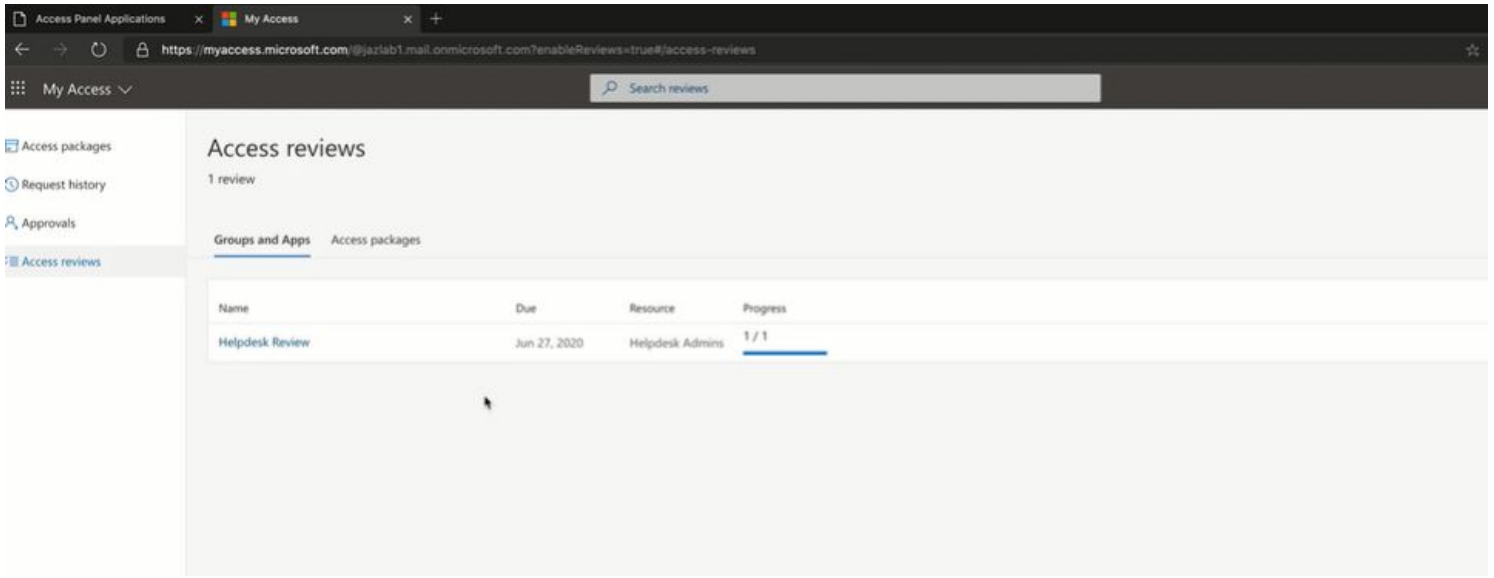


Azure AD Access Reviews - Implementation

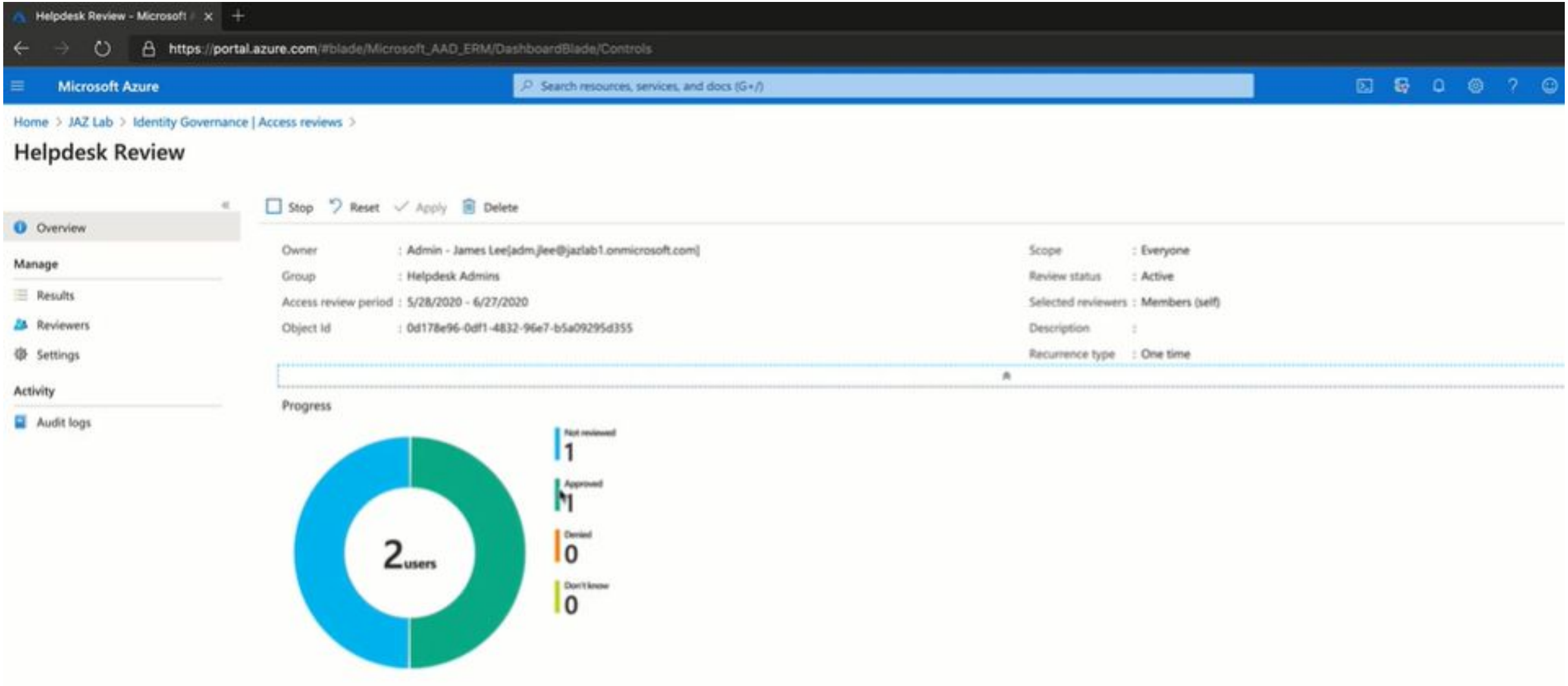


Azure AD Access Reviews - Implementation

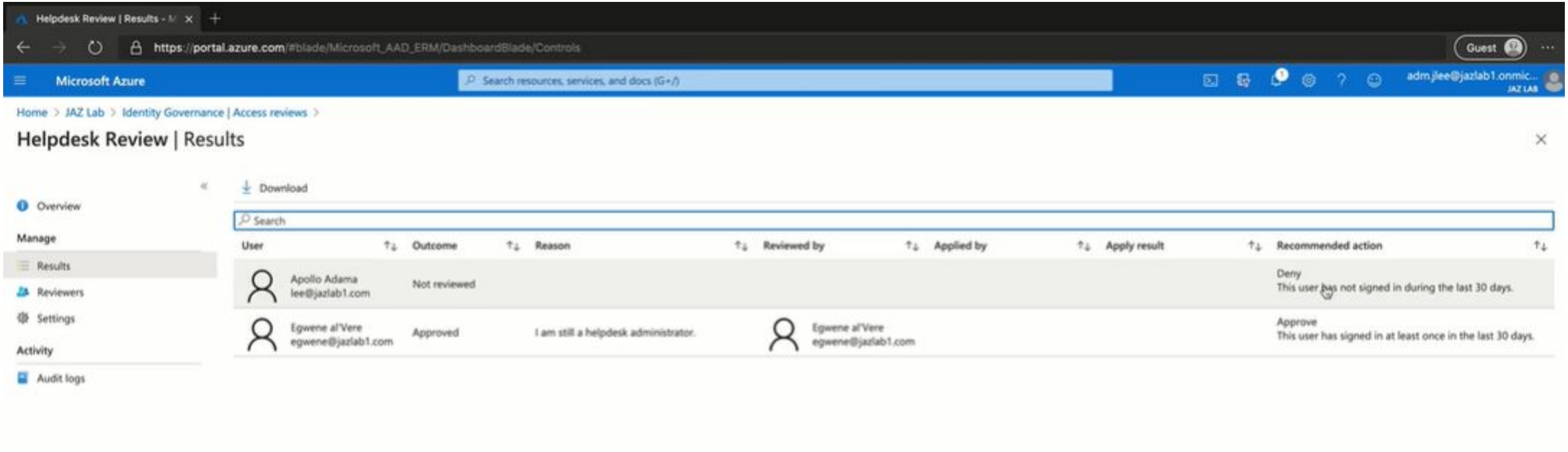




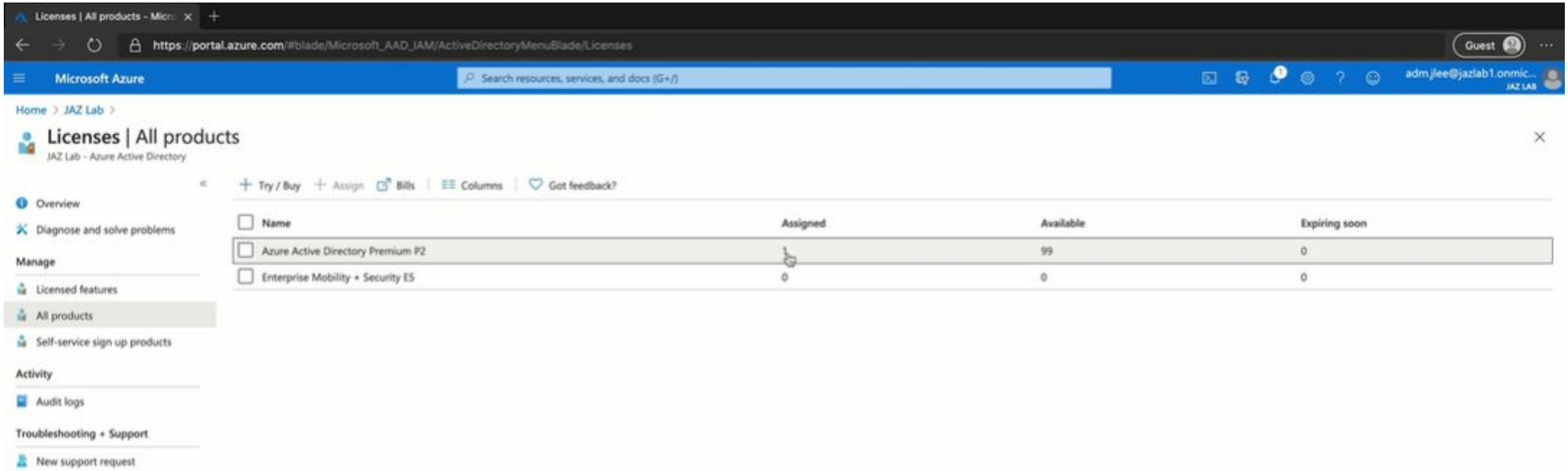
Azure AD Access Reviews - Implementation



Azure AD Access Reviews - Implementation

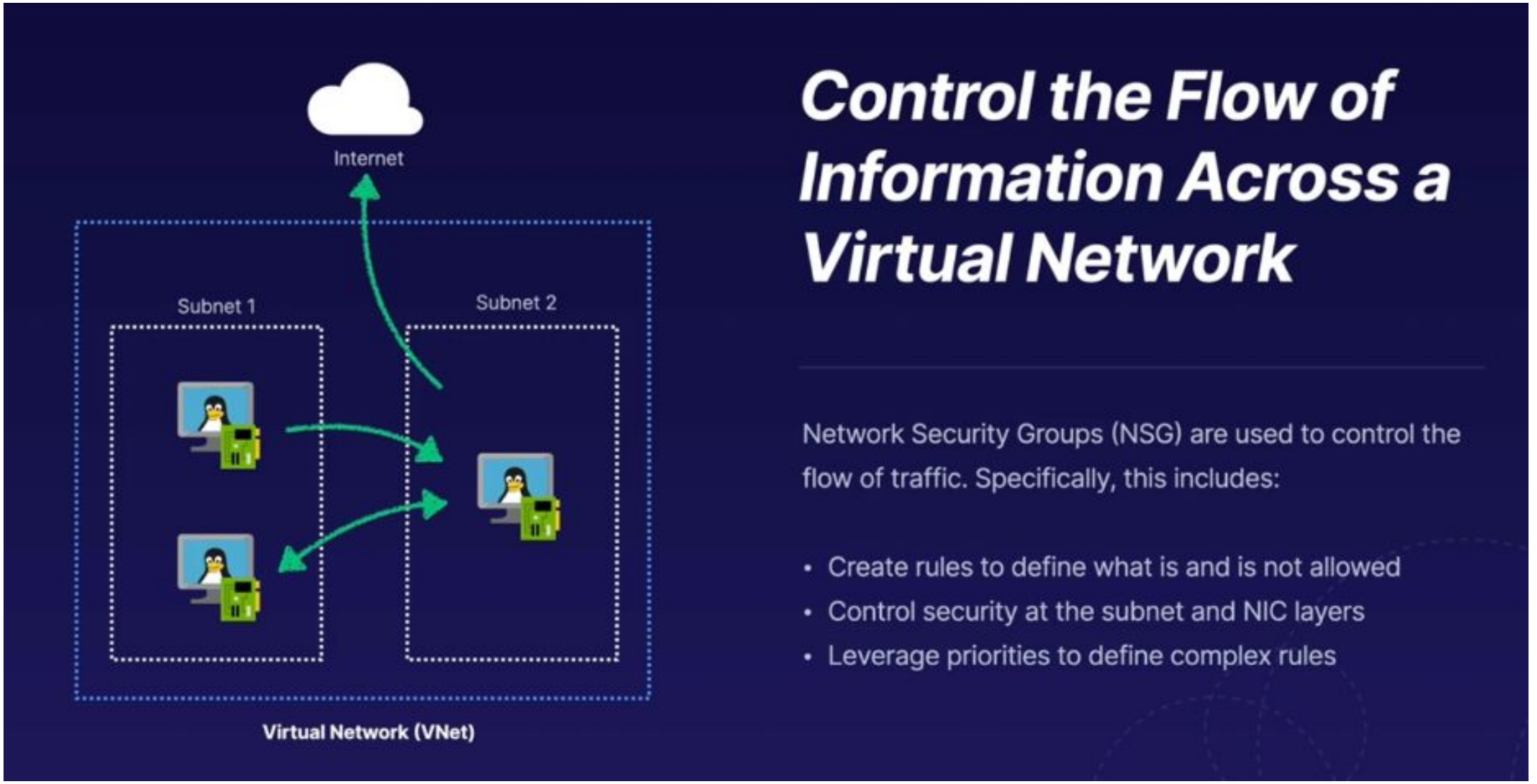


Azure AD Access Reviews - Implementation



Virtual Network Security

Network Security Groups



Network Security Groups Rules

Filtering Traffic

What traffic will we allow or deny? This includes source, source port, destination, destination port, and protocol.

Default Rules

NSG rules include several default rules such as "DenyAllInbound". These cannot be deleted, but can be overridden.

Priority

To support different scenarios, we must define priorities for a rules. The lower the number, the higher the priority.

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBou...	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Network Security Groups Assignments

Assign to an NIC

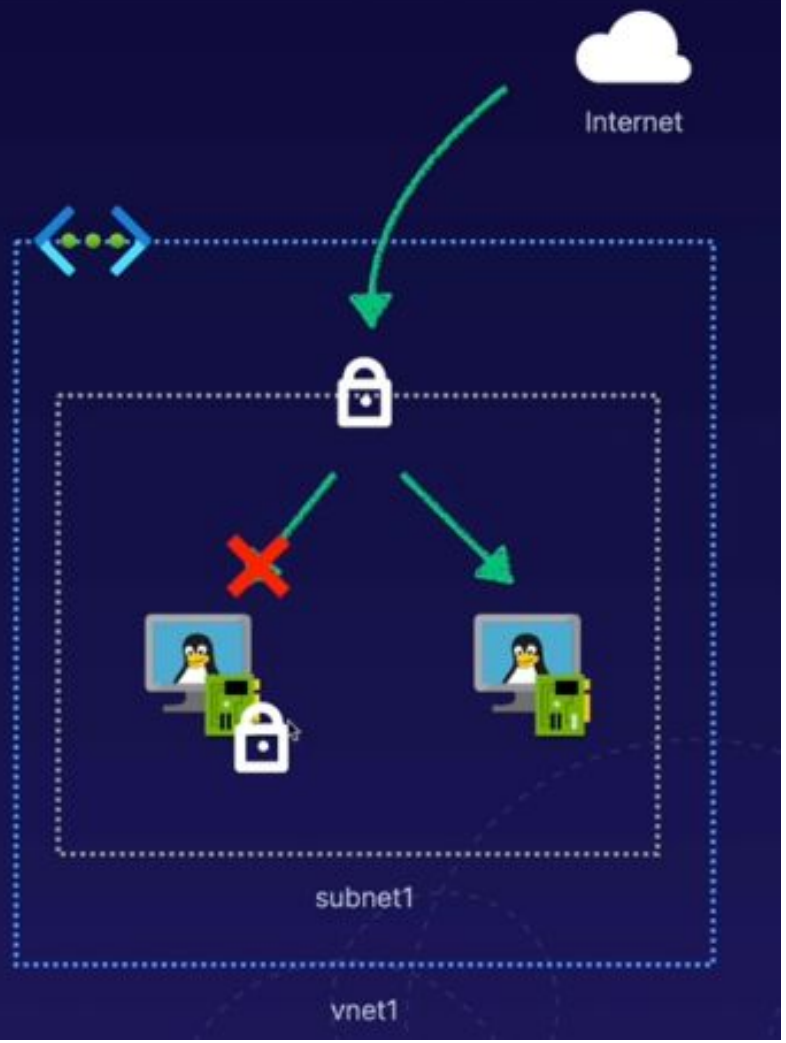
An NSG has no affect unless it is assigned. NSGs can be associated directly with an NIC on a virtual machine.

Assign to a Subnet

NSGs can also be associated with a subnet, meaning the rules apply to all resources within the subnet.

Precedence and Processing

"Follow the traffic" to see which rules will take effect. Once a rule is matched, no further rules will be processed.



Augmented Security Rules | Application Security Groups

Represent Customer Solutions

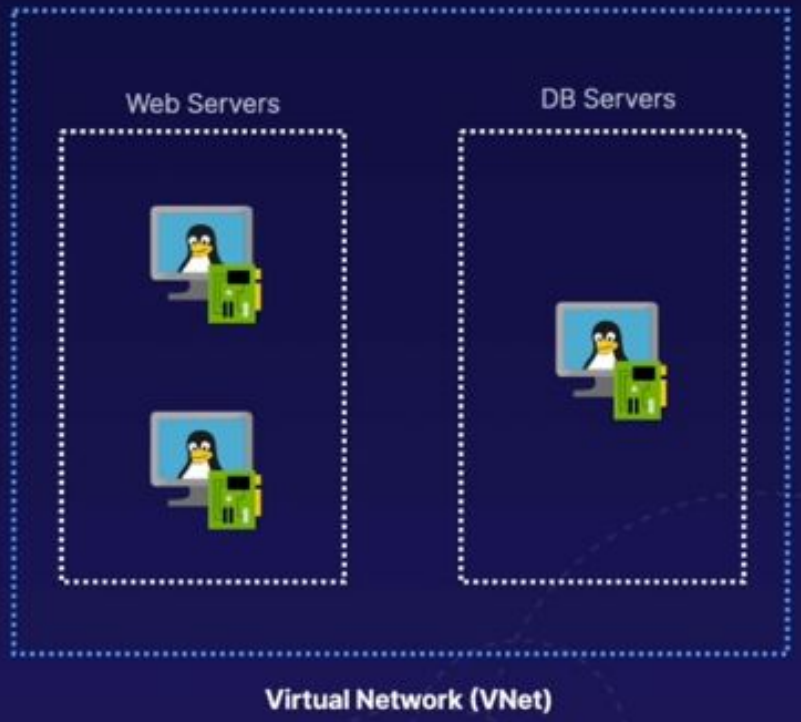
Application Security Groups (ASG) are logical containers for the network interfaces used in your solution.

Simplified Network Security Groups

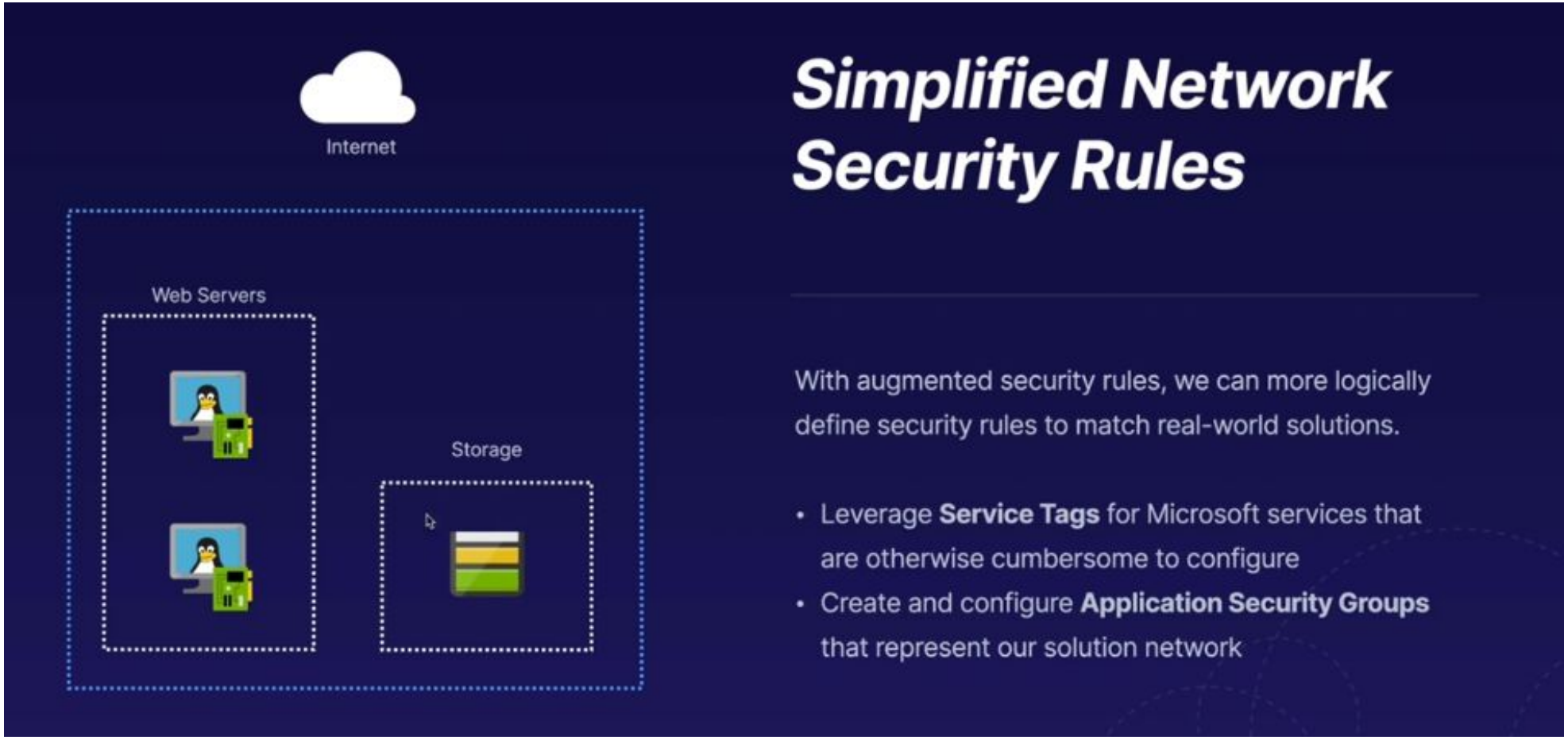
An ASG can be used easily within NSG rules, to simplify the management of security rules for a solution.

Virtual Network (VNet) Limitation

All NICs for an ASG must exist in the same VNet. This is also true when an ASG is used in a rule for both source and destination.



Augmented Security Rules | Overview



Augmented Security Rules | Service Tags

MS

Represent Microsoft Services

Service Tags are a collection of IP address prefixes that correspond to a specific Azure service.

Microsoft Managed

Microsoft manages the associated IP addresses of service tags, as Azure services can regularly change.

Easy to Leverage

Service Tags can be used within both Network Security Groups and the Azure Firewall.

Tag	Purpose	Can use inbound or outbound?	Can be regional?	Can use with Azure Firewall?
ActionGroup	Action Group	Inbound	No	No
ApiManagement	Management traffic for Azure API Management-dedicated deployments. Note: This tag represents the Azure API Management service endpoint for control plane per region. This enables customers to perform management operations on the APIs, Operations, Policies, NamedValues configured on the API Management service.	Inbound	Yes	Yes

Augmented Security Rules | Application Security Groups

Represent Customer Solutions

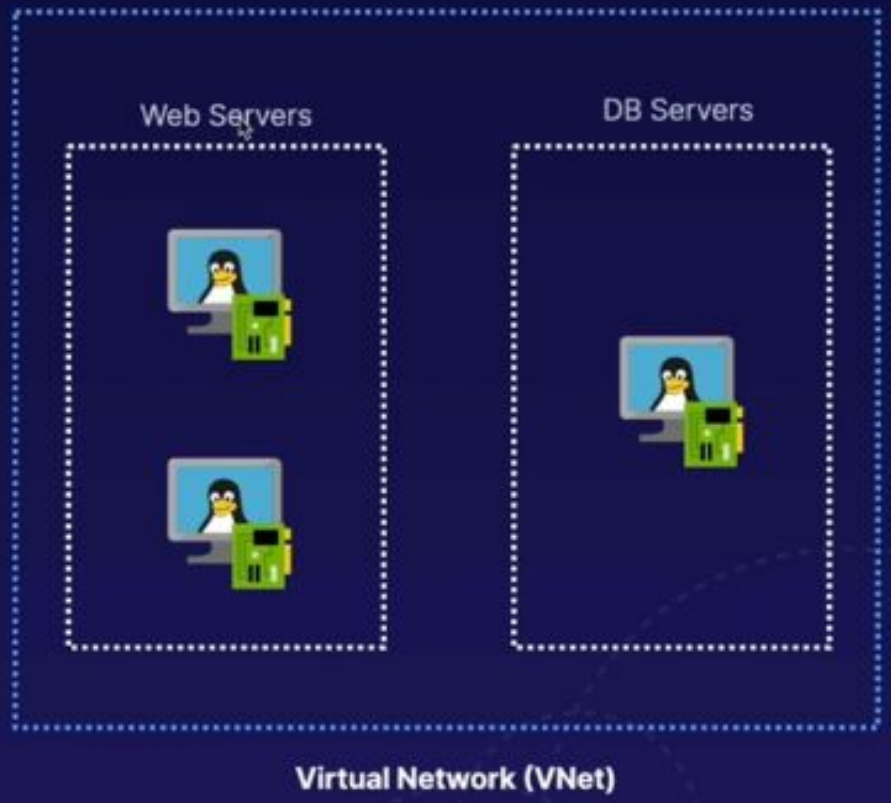
Application Security Groups (ASG) are logical containers for the network interfaces used in your solution.

Simplified Network Security Groups

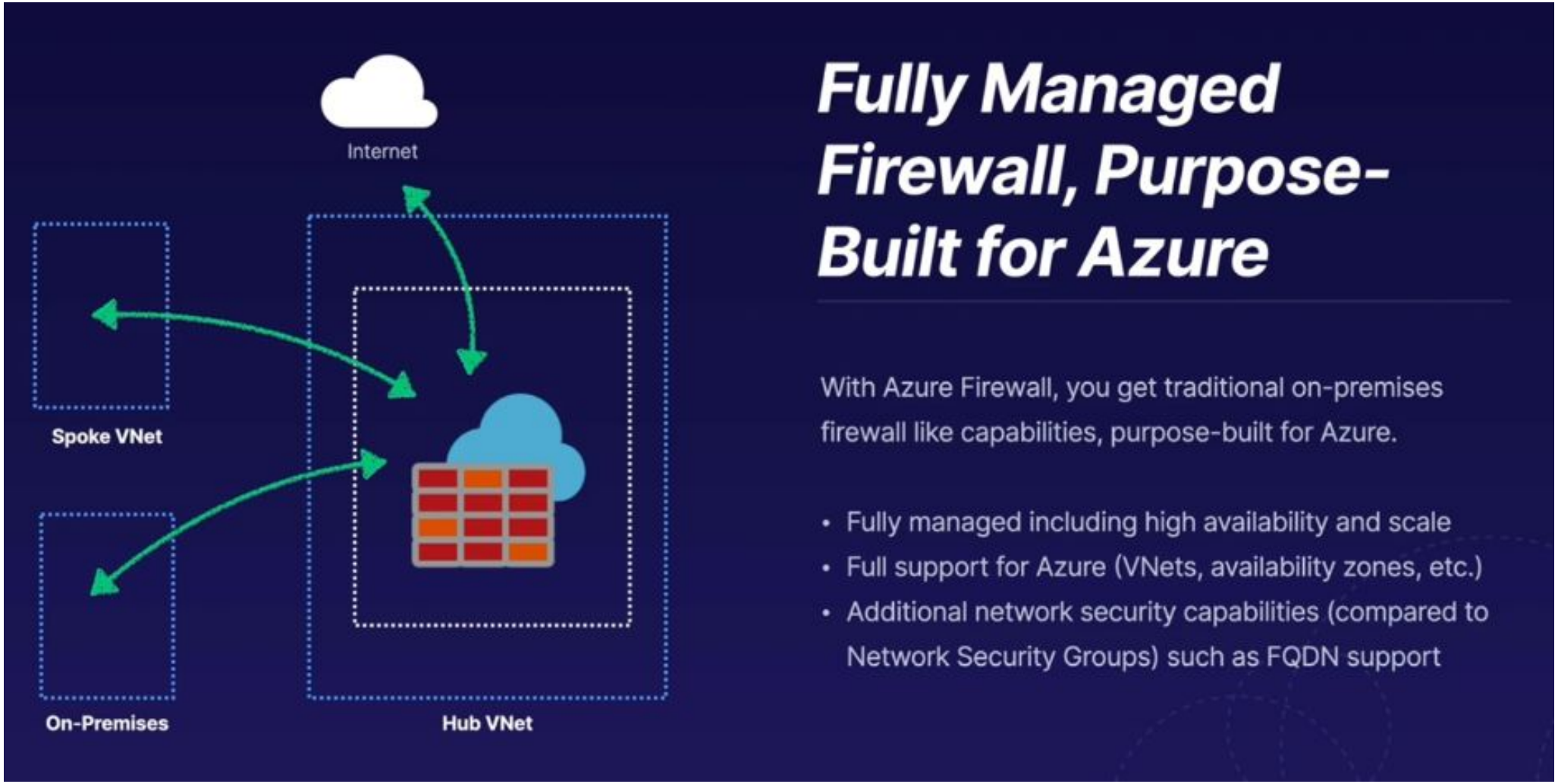
An ASG can be used easily within NSG rules, to simplify the management of security rules for a solution.

Virtual Network (VNet) Limitation

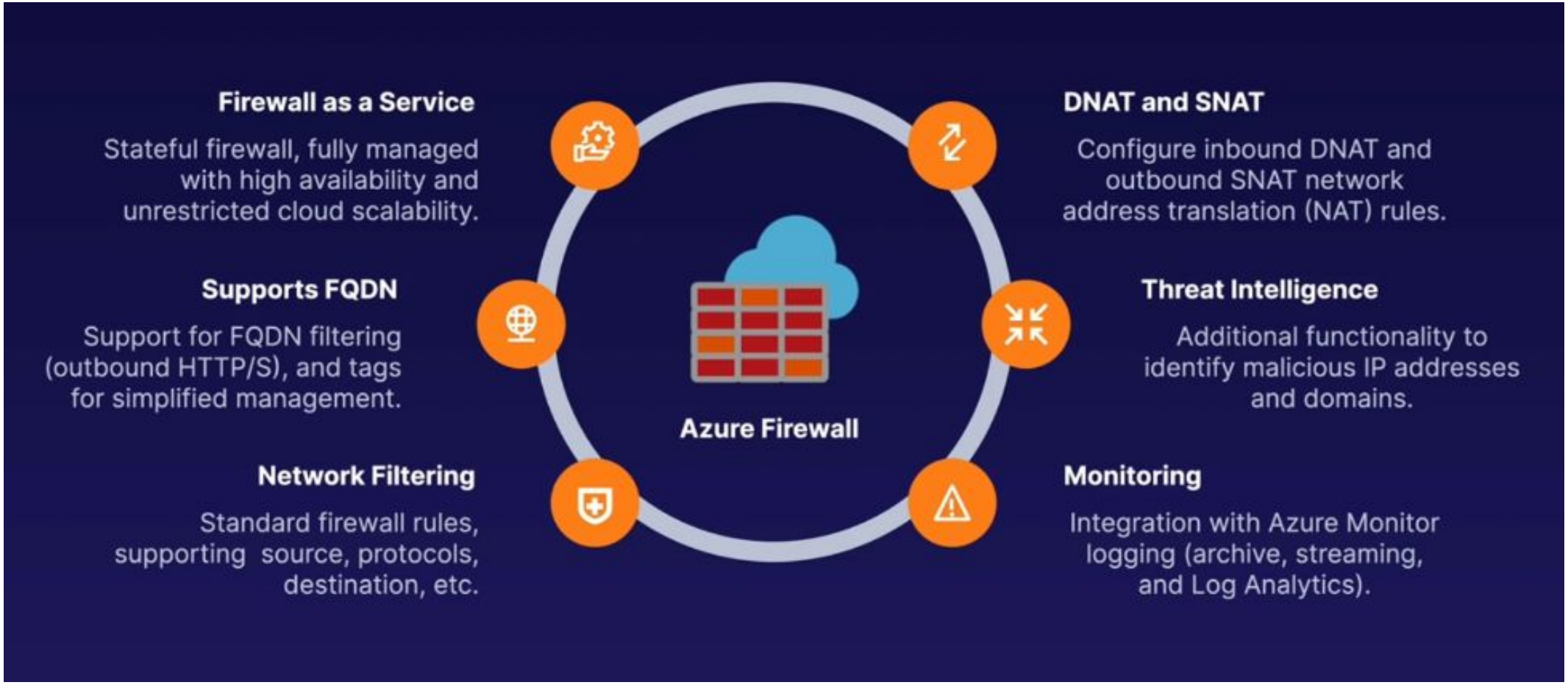
All NICs for an ASG must exist in the same VNet. This is also true when an ASG is used in a rule for both source and destination.



Azure Firewall



Azure Firewall



Azure Firewall | Implementation Tasks

1 **Configure a Virtual Network**

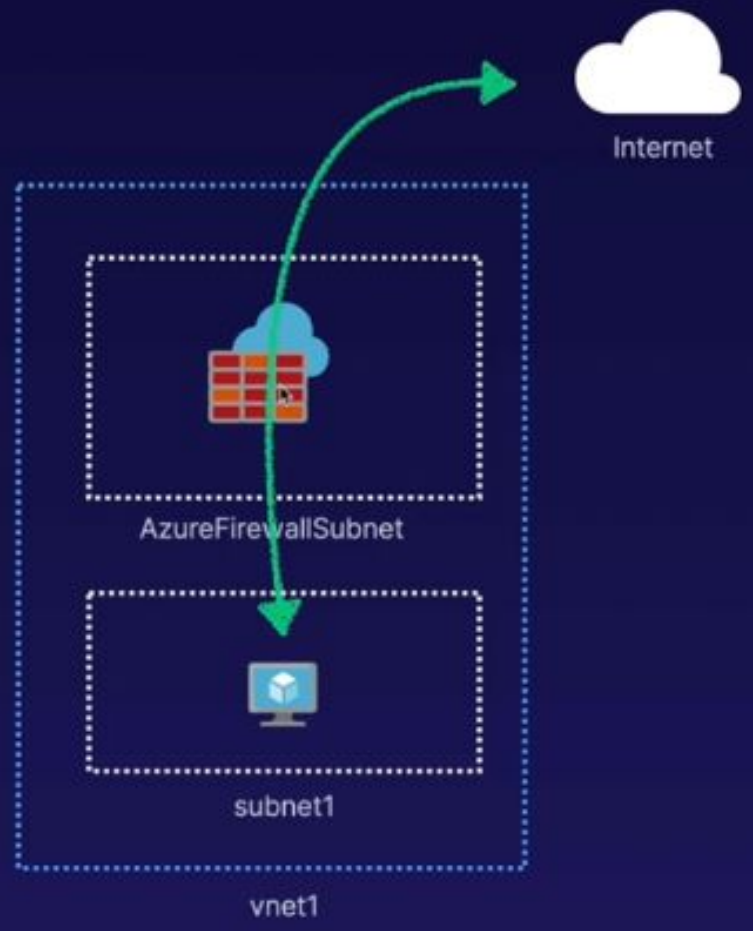
This can be an existing Virtual Network (VNet) but is often a centralized VNet that is connected to your other VNets (and on-premises).

2 **Configure a Subnet**

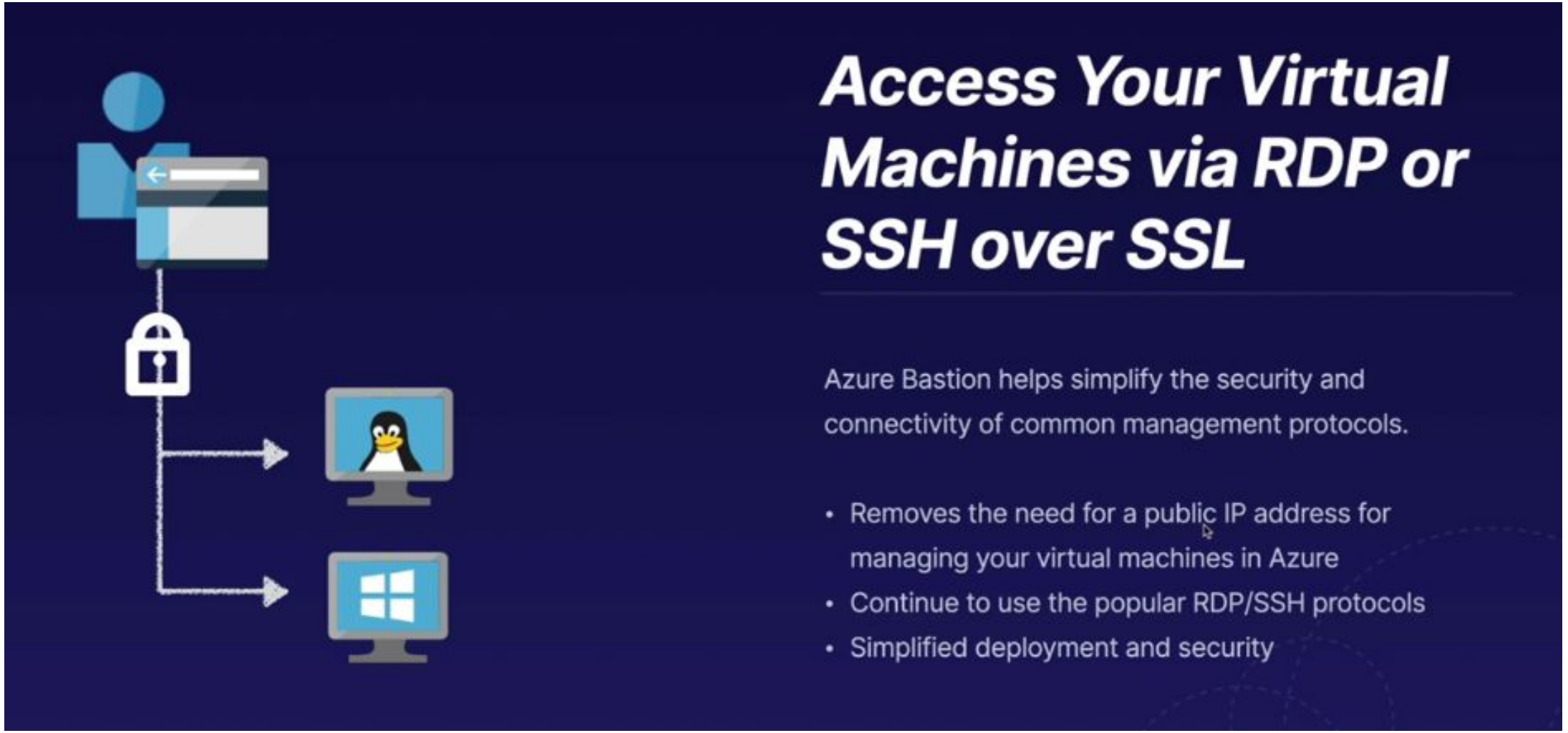
The Azure Firewall must be deployed to a dedicated subnet called "`AzureFirewallSubnet`". This subnet must have no associated NSGs.

3 **Configure Routing**

In order to have VNet resources leverage the Azure Firewall, a custom route must direct traffic to the Azure Firewall.



Azure Bastion



Azure Bastion | Implementation

Deploy a Bastion Host

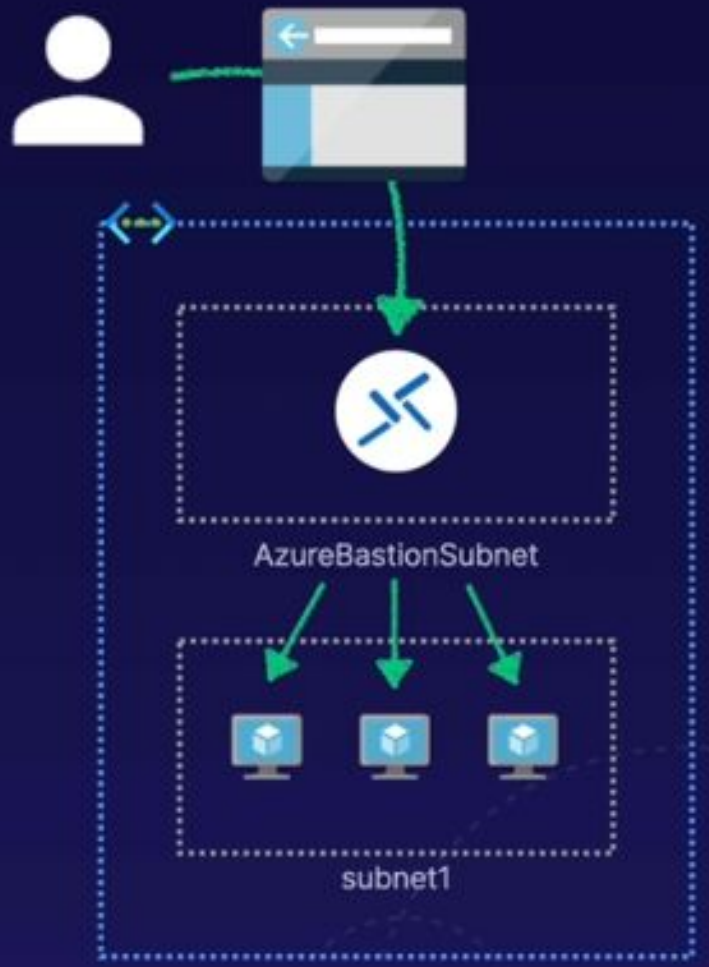
Create and deploy to a VNet. Note that a Bastion must be deployed to a subnet called "`AzureBastionSubnet`".

Connect to a Virtual Machine

Use the Bastion option in the Azure Portal, for both virtual machines and instances with a VM Scale Set.

Important Considerations

Connectivity requires port 443 outbound, and HTML5 support in a web browser.



Azure Load Balancer

Azure Load Balancer

Azure Load Balancer | Key Components

10.0.0.0

Frontend IP

The IP address (public or private) associated with the load balancer.

Backend Pool

The group of resources which will ultimately receive traffic from end-users.

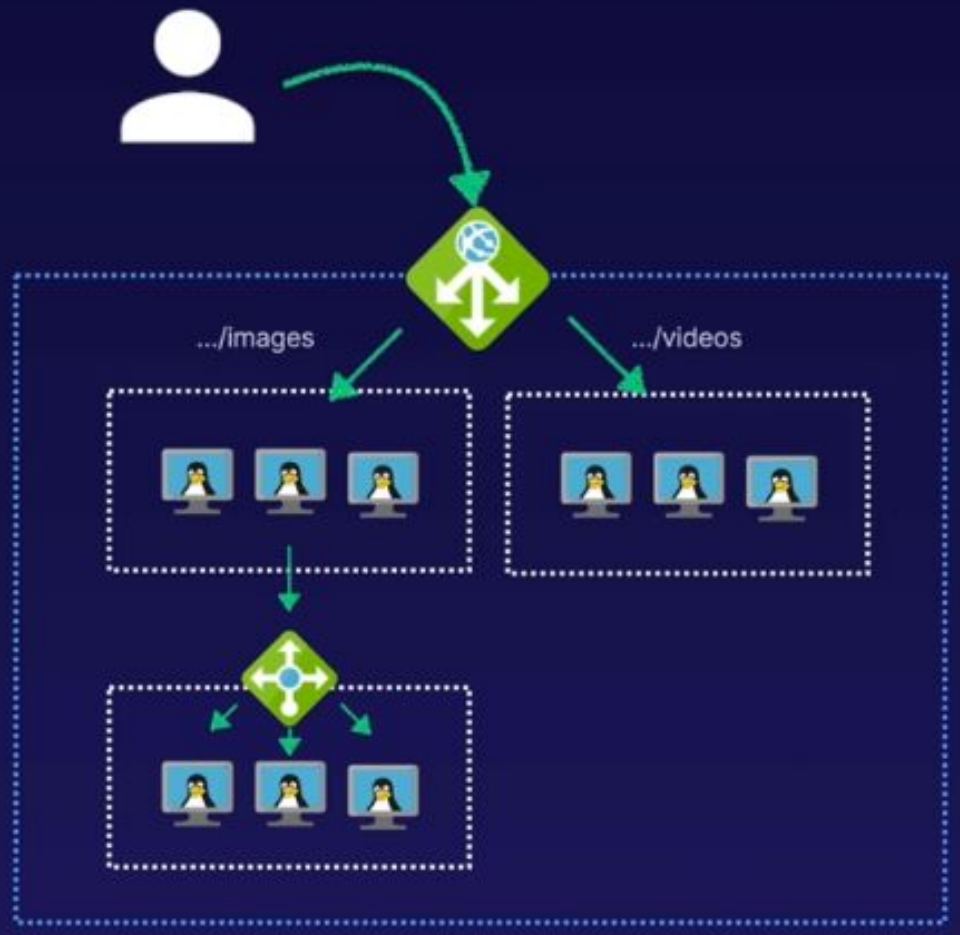
Health Probe

Used for determining whether the destination instance is available.

Rules

Load balancing or NAT rules to configure inbound/outbound access.

Azure Application Gateway

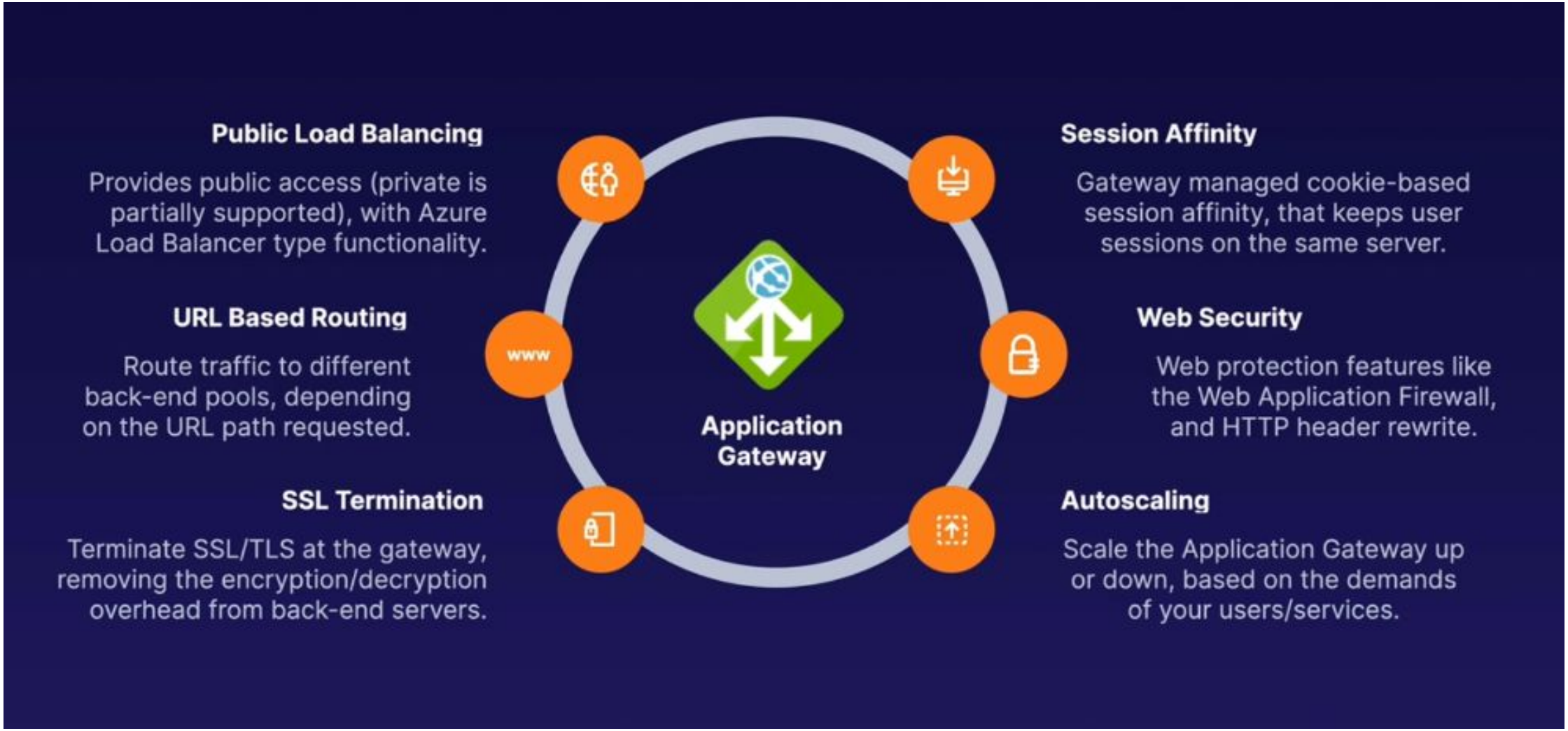


Layer 7 Traffic Distribution for Highly Available Web Apps

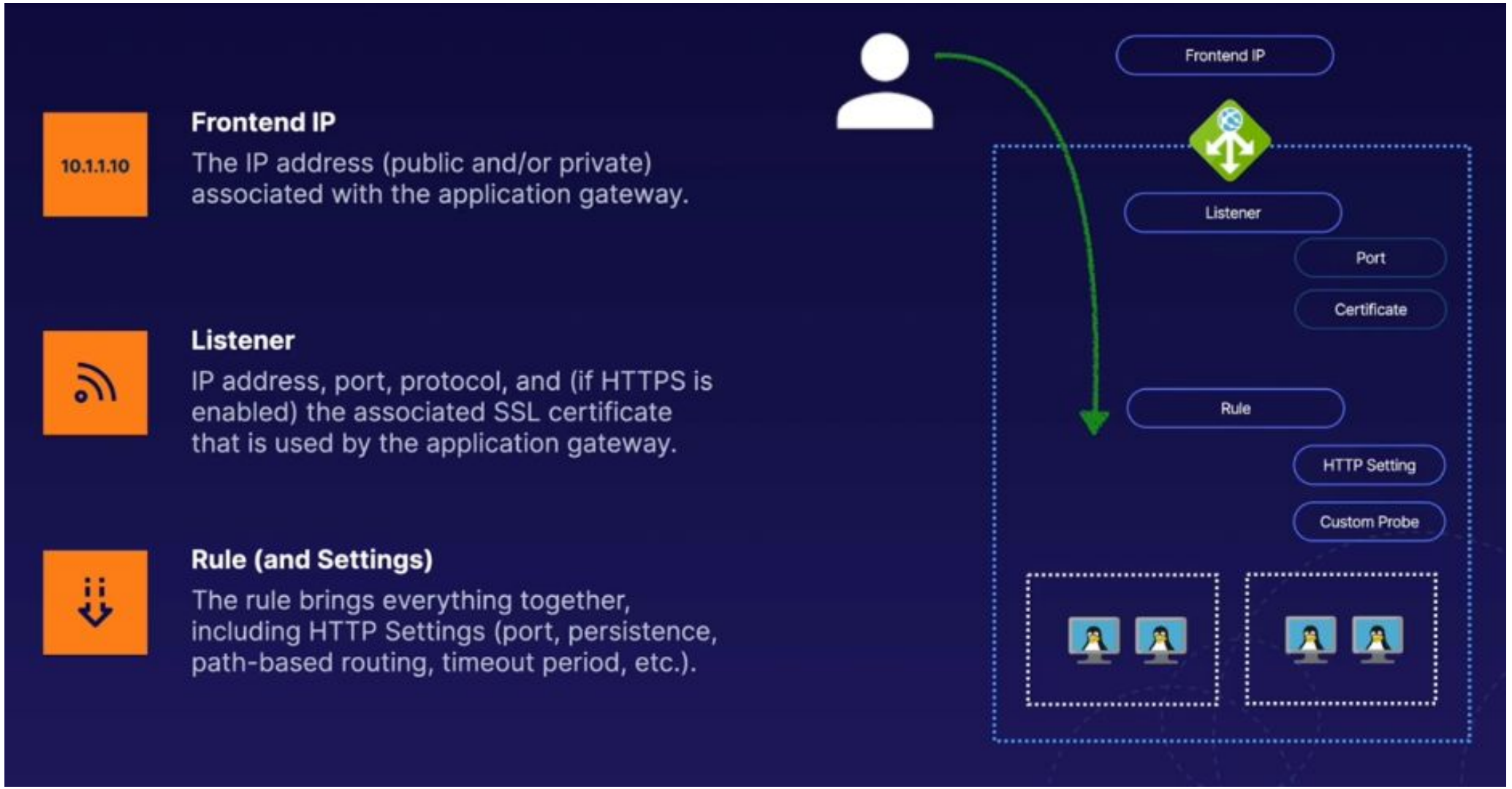
Azure Application Gateway provides load balancing capabilities, plus additional load balancing features to support web applications.

- Standard load balancing features
- Layer 7 functionality such as:
  - URL-based routing
  - SSL termination

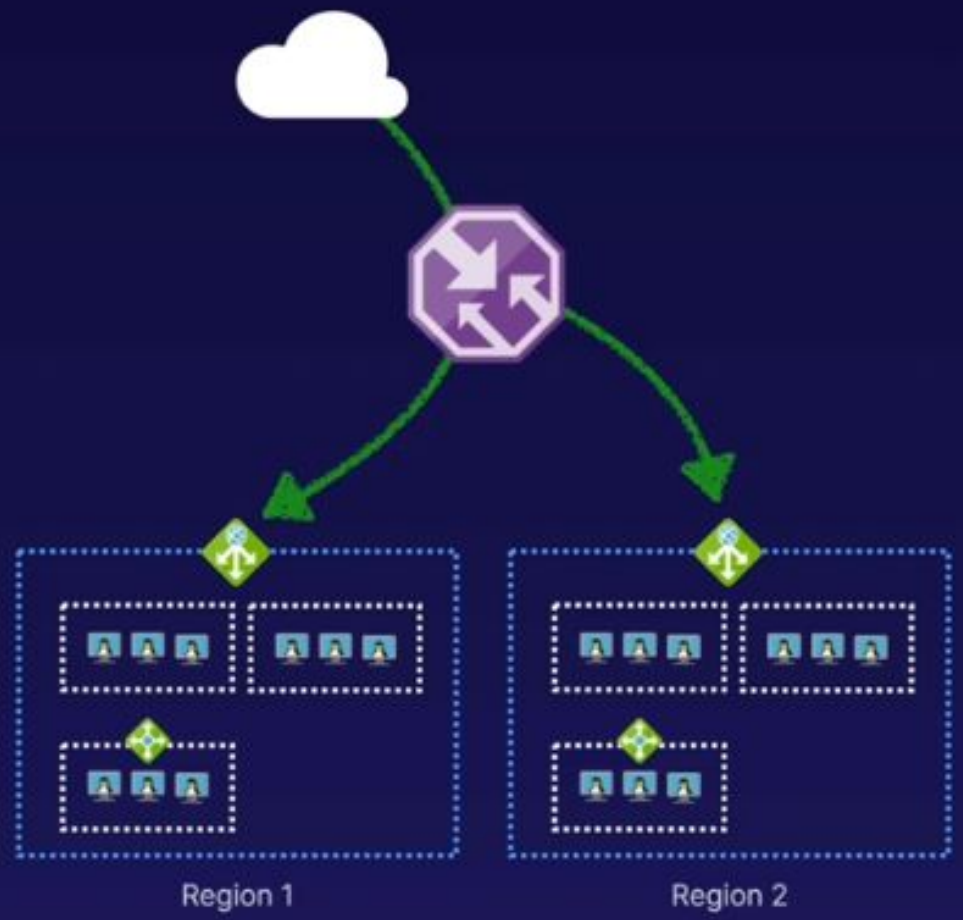
Azure Application Gateway



Azure Application Gateway | Key Components



Azure Traffic Manager



Traffic Distribution for Geographically Resilient Solutions

Azure Traffic Manager distributes traffic across regions to facilitate high geographic availability.

- Leverages DNS to facilitate traffic distribution
- Provides many different routing methods, and supports several endpoint types
- Leverages endpoint health to support availability

Azure Traffic Manager | Architecture Overview

Region-Redundant Solution

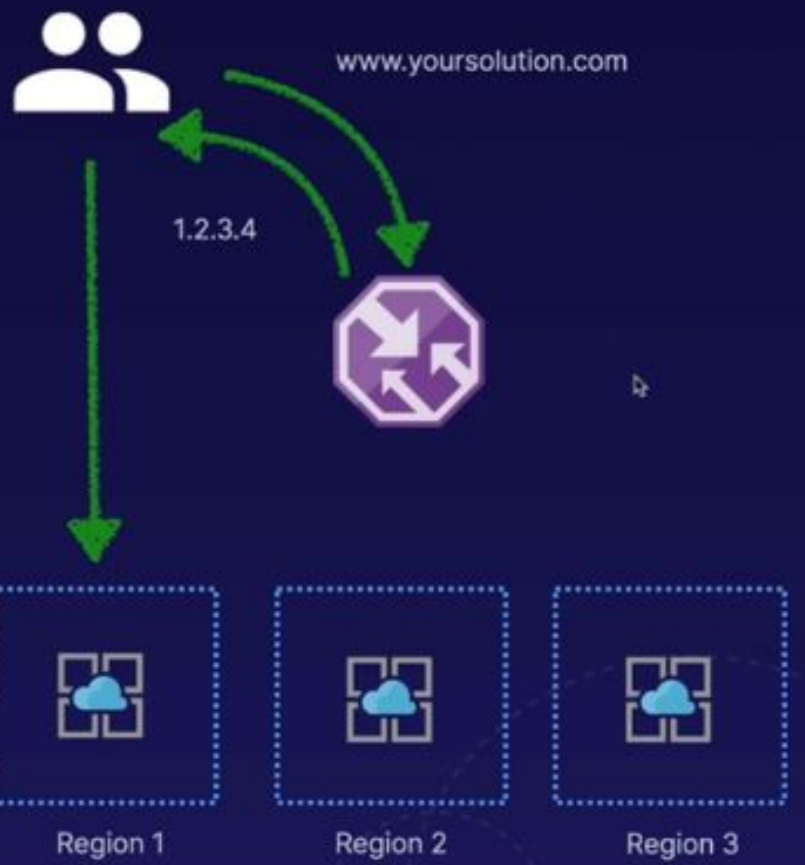
Traffic Manager can route to many different endpoints types (Azure, external, nested). These endpoints should be redundant.

Communication Flow

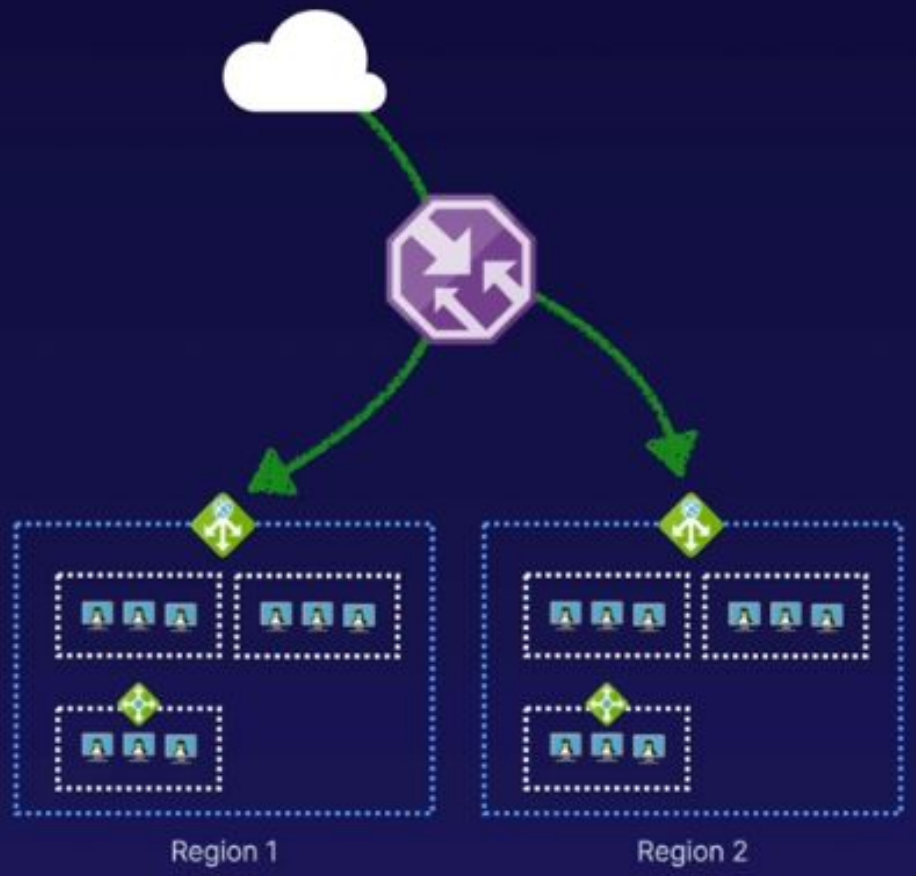
1. User loads solution (DNS lookup)
2. Traffic Manager provides IP address
3. User navigates to the appropriate solution

Traffic Manager Profile

The profile is used to configure the endpoints which will be used, as well as the routing priority.



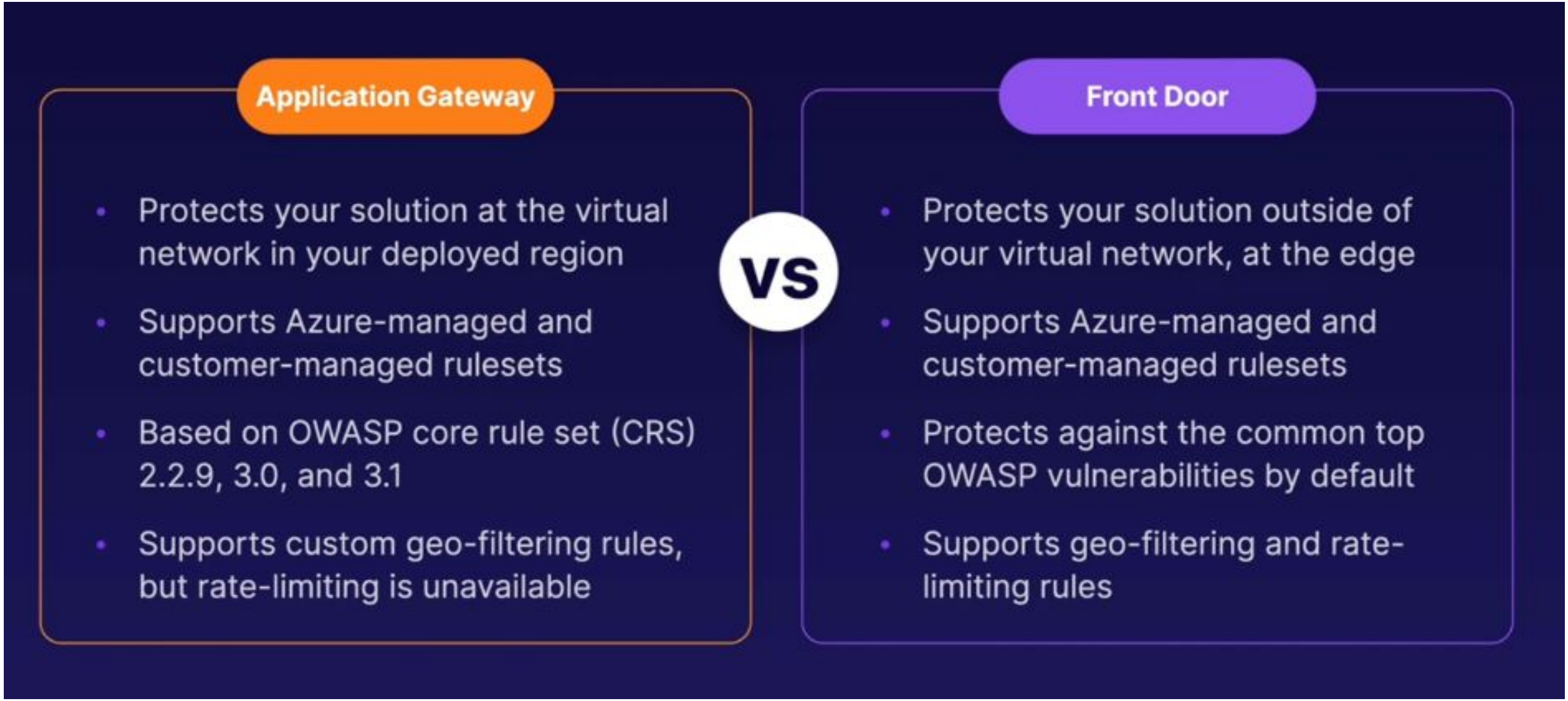
Azure Traffic Manager | Routing Methods



Method	Description
Priority	Prioritized primary and backup endpoints.
Weighted	Distribution of traffic according to a weight value.
Performance	Send traffic to the "closest" endpoint.
Geographic	Route traffic based on the geographic location of the client.
MultiValue	Returns multiple endpoints to a request.
Subnet	Route based on the requester's IP address.

Web Application Firewall in Azure

Web Application Firewall in Azure



Azure AD Application Security

1

Application Registration

Registration of an application within Azure Active Directory, including secret configuration.

2

Application Permissions

Using role-based access control with an application registered within Azure AD.

3

Demonstration

Demonstration of some basic code that can authenticate to Azure AD to access resources.

Azure AD Application Security | Components

Application Object

The application object within Azure AD represents various details about a real-world application.

Service Principal

When an application object is created, a corresponding service principal is created in the Azure AD tenant.

Application Secrets

So the application code can prove it is the registered application, we must use secret information (like credentials).

Managed Identities

Features of Managed Identities

1. **Azure AD Identities for Azure Resources**

   The platform manages integrated identities in Azure AD identities for Azure resources.

2. **Credential Security**

   Avoid the need for having to store credentials for your application/script within code.

3. **Support for Several Azure Resources**

   Many services support managed identities, and these can authenticate to Azure AD.

Managed Identities

Managed Identity

An Azure resource must be assigned a system or user-managed identity.

Azure AD Service Principal

The managed identity establishes a service principal within Azure.

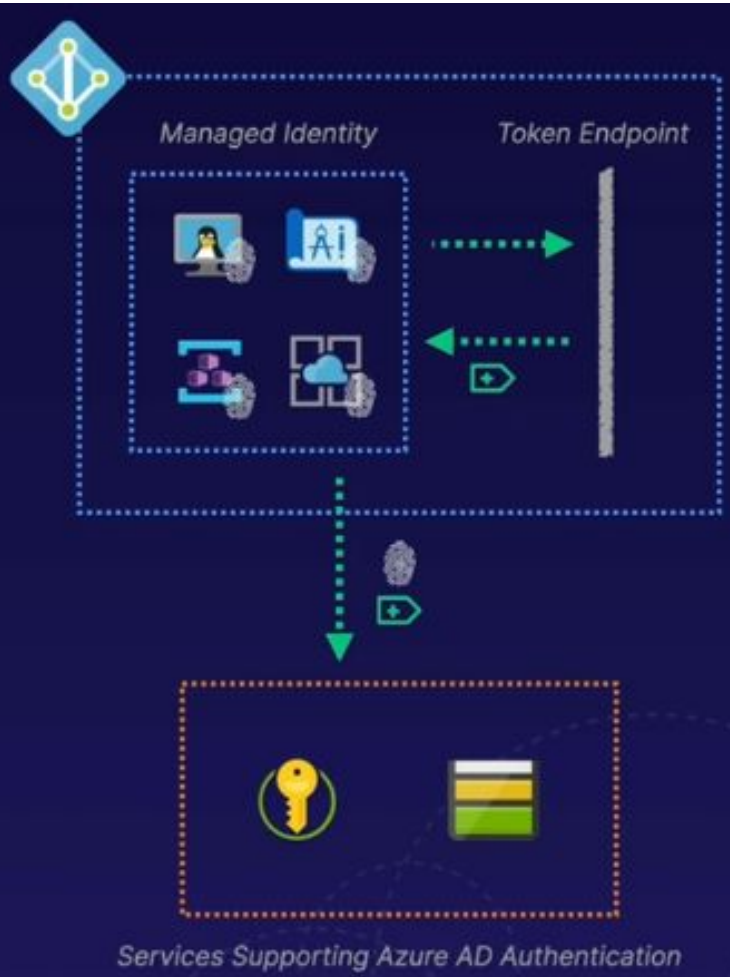
REST

Instance Metadata Service (IMDS)

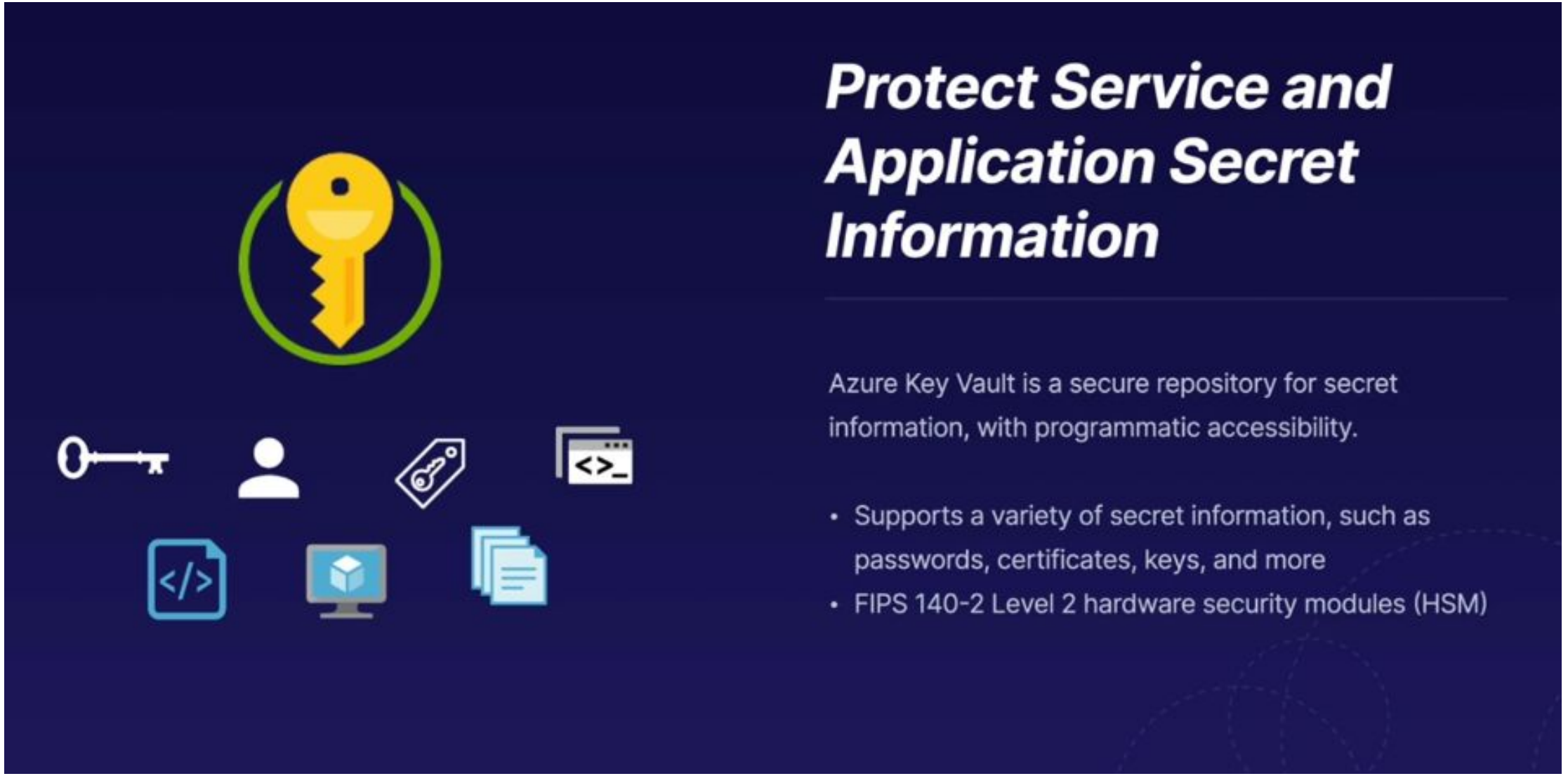
Your solution (code, script, etc.) can request a token from the IMDS.

Access Token

The access token can be used to authenticate with Azure AD.



Key Vault


Protect Service and Application Secret Information
Azure Key Vault is a secure repository for secret information, with programmatic accessibility.
• Supports a variety of secret information, such as passwords, certificates, keys, and more
• FIPS 140-2 Level 2 hardware security modules (HSM)

Key Vault | Components

Key Vault

Houses the secret information using hardware security modules (HSM) and is accessible by REST API.

Secret Information

Support for secrets, keys, and certificates. It also includes some management capabilities for keys and certificates.

Access Policies

Control the access to secret information at the data layer using access policies.

Azure Update Management

Azure Update Management

Automation Account

Service to facilitate the process automation and configuration management.

Hybrid Runbook Worker

Customer-managed Windows or Linux operating system which performs tasks.

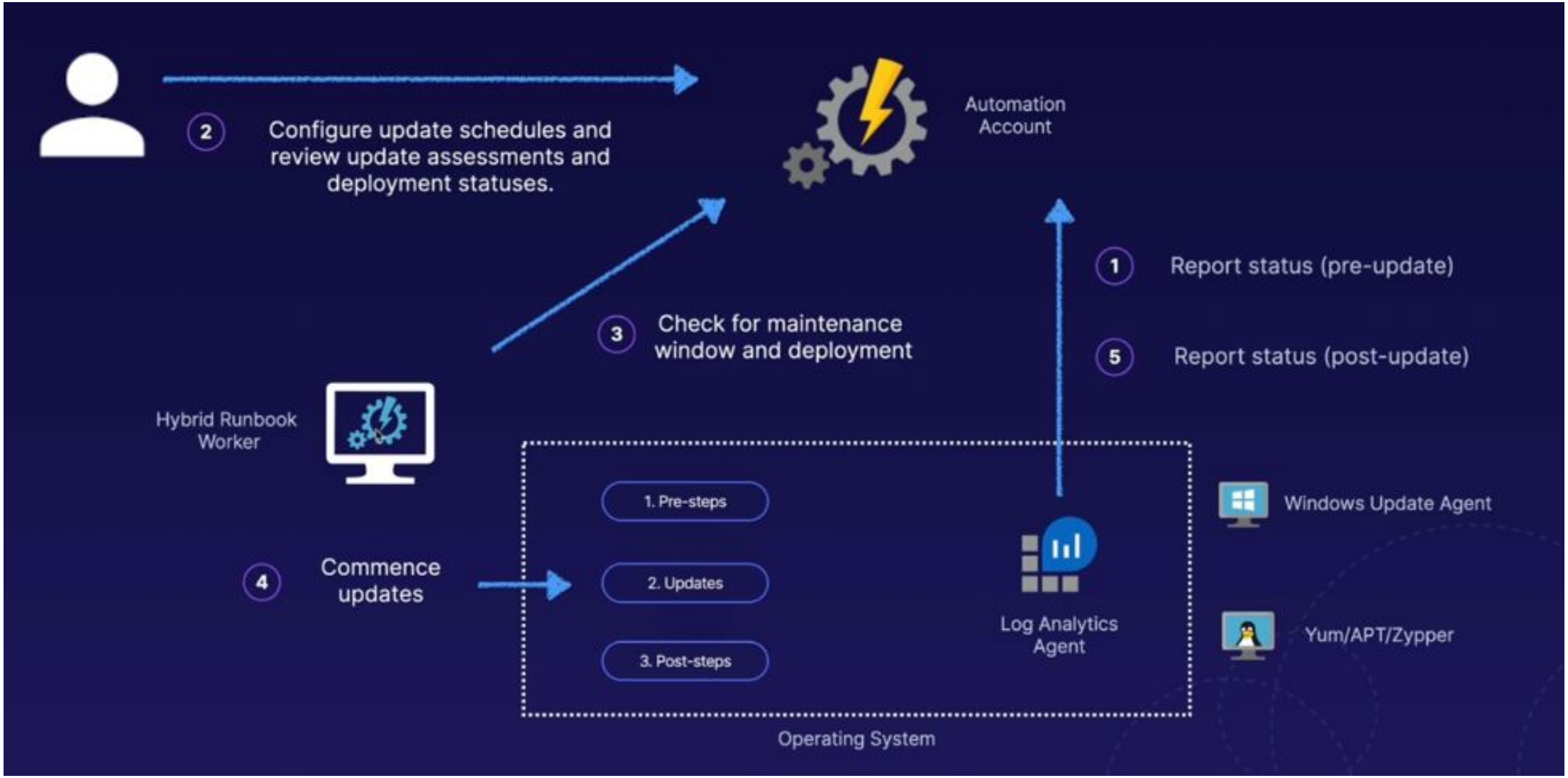
Log Analytics Workspace

Repository for log information. In this scenario, it is for updating management data.

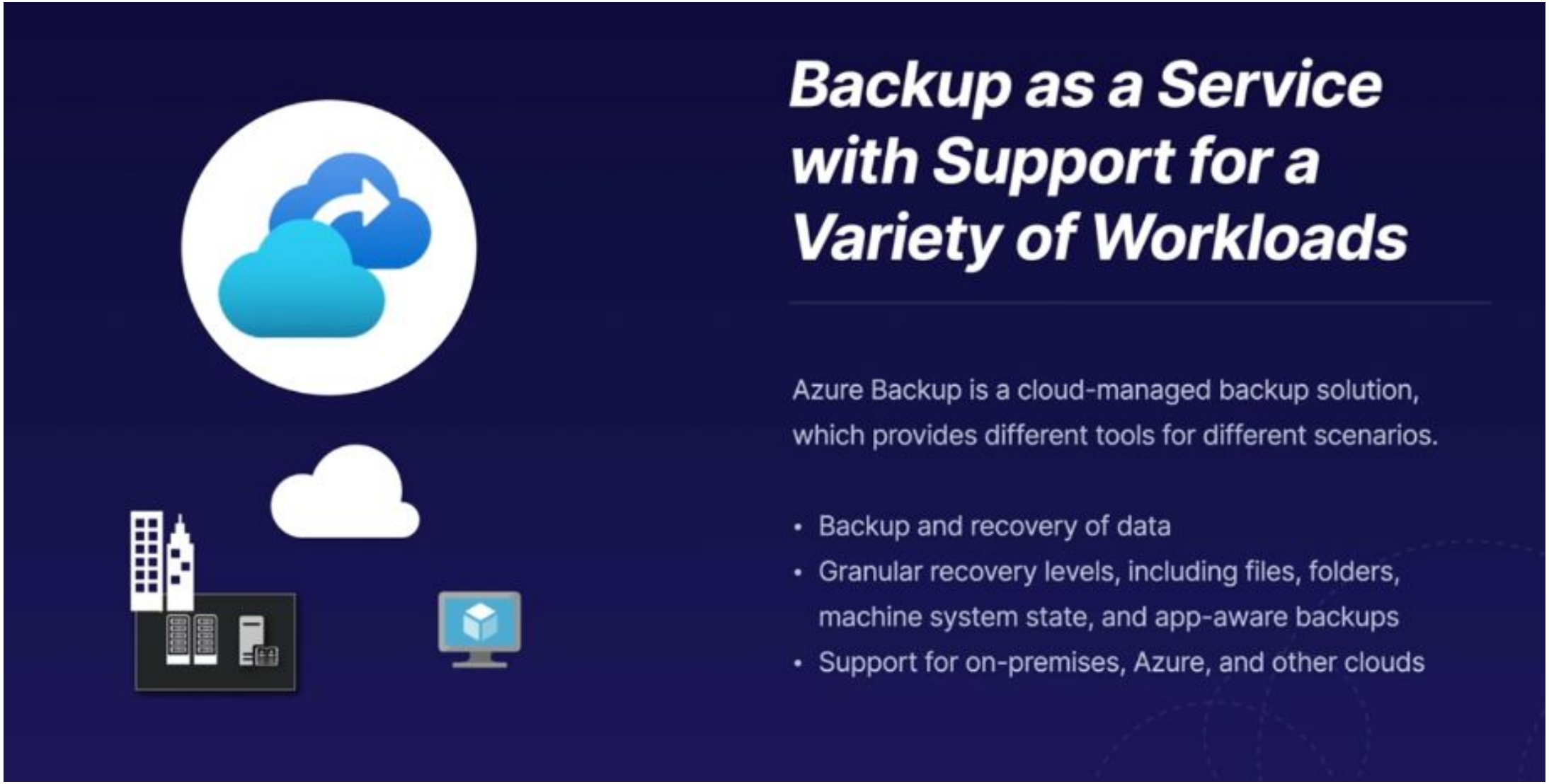
Log Analytics Agent

The software which routes logs/metric data from Linux or Windows to the workspace.

Azure Update Management



Azure Backups



Azure Backups

Recovery Services Vault

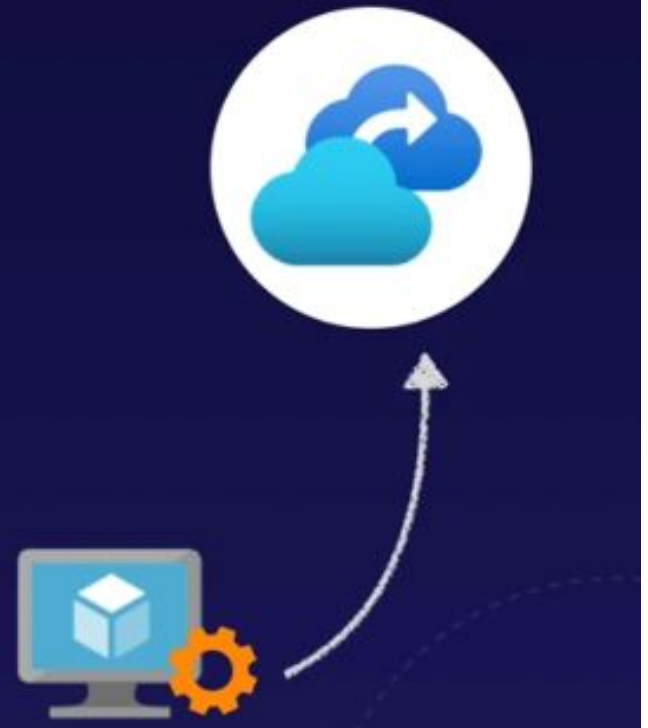
A repository for backup data (used for both backups and disaster recovery) that controls many backup related settings.

Workload

Azure Backup supports a range of workloads, such as Windows, Linux, and some backup-aware applications.

Backup Agent

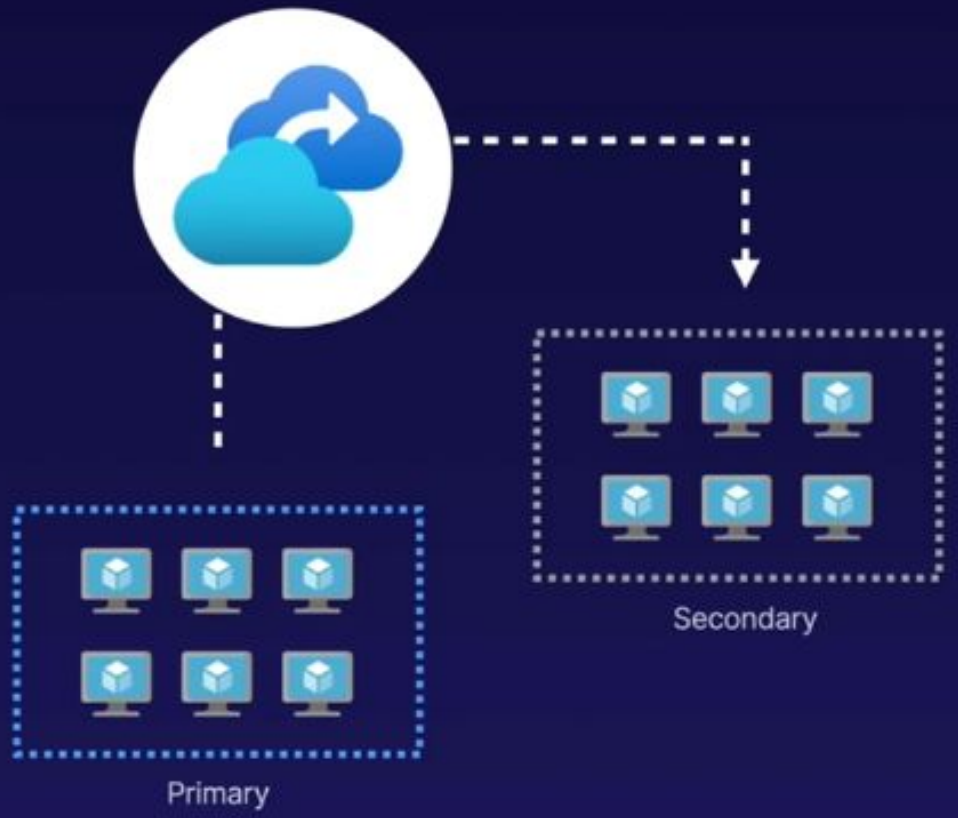
Sever backup agents exist to support different backup workloads and scenarios (such as on-premises, within Azure, etc.).



Azure Backups | Backup Agents

Agent	Description	Considerations
Microsoft Azure Recovery Services (MARS) Agent	Software installed on Windows to perform file-level backups to a registered recovery services vault.	• Provides file, folder, and system-state backups for Windows only • Backs up three times a day • Restores files to a server
Microsoft Azure Backup Server (MABS)	Backup suite which integrates with Azure backup to support traditional backups.	• Provides file, folder, volume, application, and system state backup • Protects both Windows and Linux • Customizable backup frequency
Azure Virtual Machine Backup Extension	Leverages a virtual machine extension to backup a virtual machine within Azure.	• Supports virtual machine-level backups of Windows and Linux • Only Windows backups are application-consistent • Backs up once per day • Restores virtual machines, disks, and files
Microsoft Data Protection Manager (DPM)	Traditional on-premises Microsoft backup solution.	• Used for on-premises backups, but can also integrate with Azure Backup • Supports tape

Azure Site Recovery



Disaster Recovery as a Service (DRaaS) for Business Continuity

Azure Site Recovery helps businesses improve their ability to recover from major disasters:

- Recover from major failures at a region/site level
- Automated recovery processes
- Support for many different workloads (Azure, Hyper-VMware, and physical servers)
- Supports both Windows and Linux

Azure Site Recovery

Replicated Items

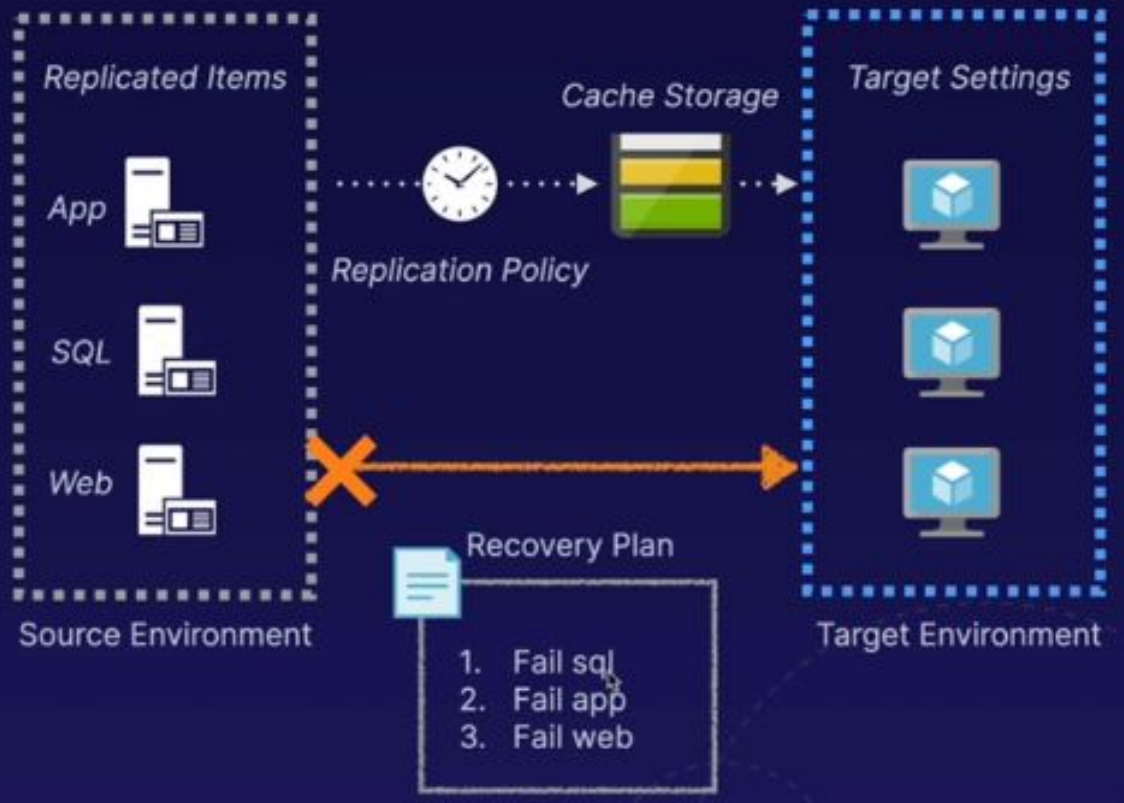
Workloads which are replicated between sites by Azure Site Recovery. These can be grouped (multi-VM consistency).

Replication Policies

Defines recovery point objectives (RPO) and recovery point retention (0 - 72 hours) and supports app-consistent snapshots.

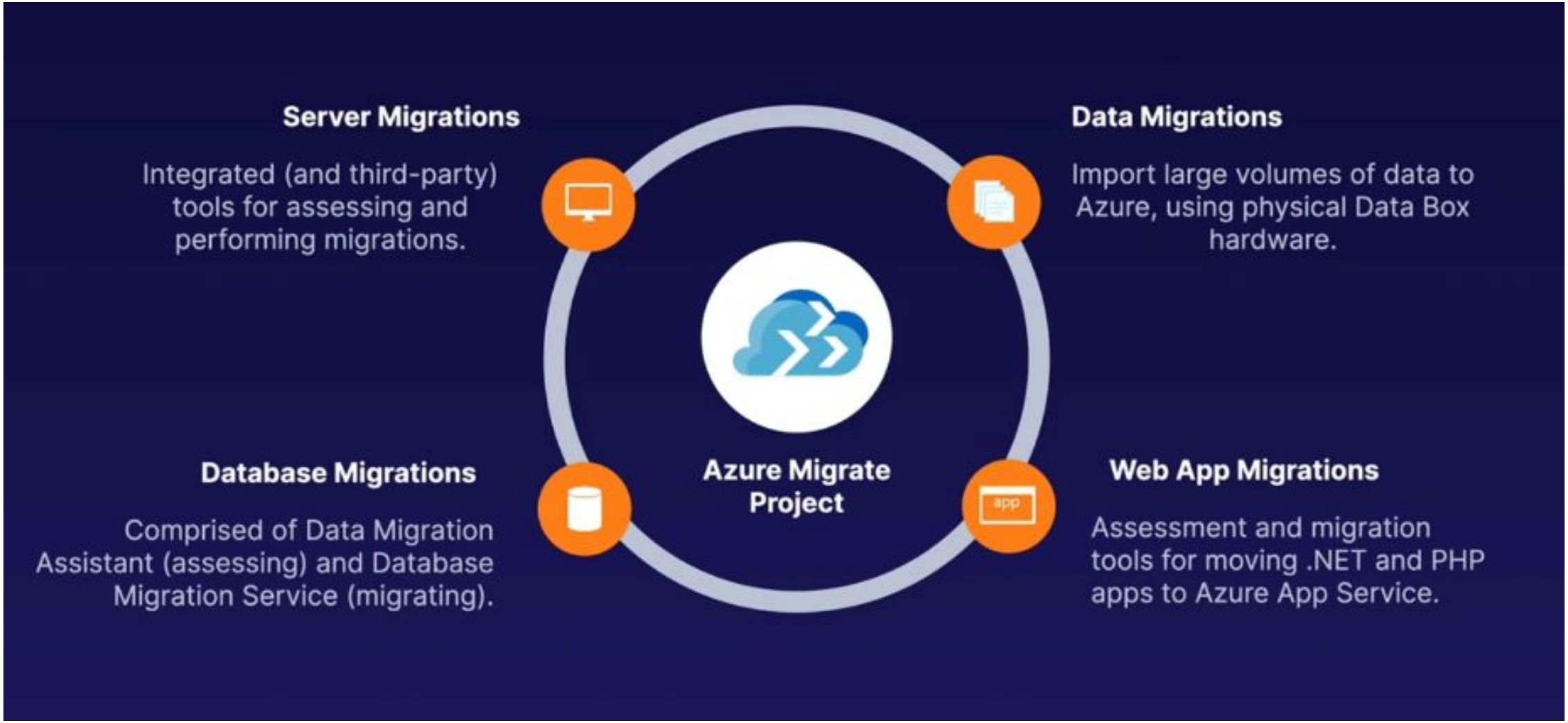
Recovery Plans

Helps reduce recovery time objectives (RTO) by providing functionality to automate failover.

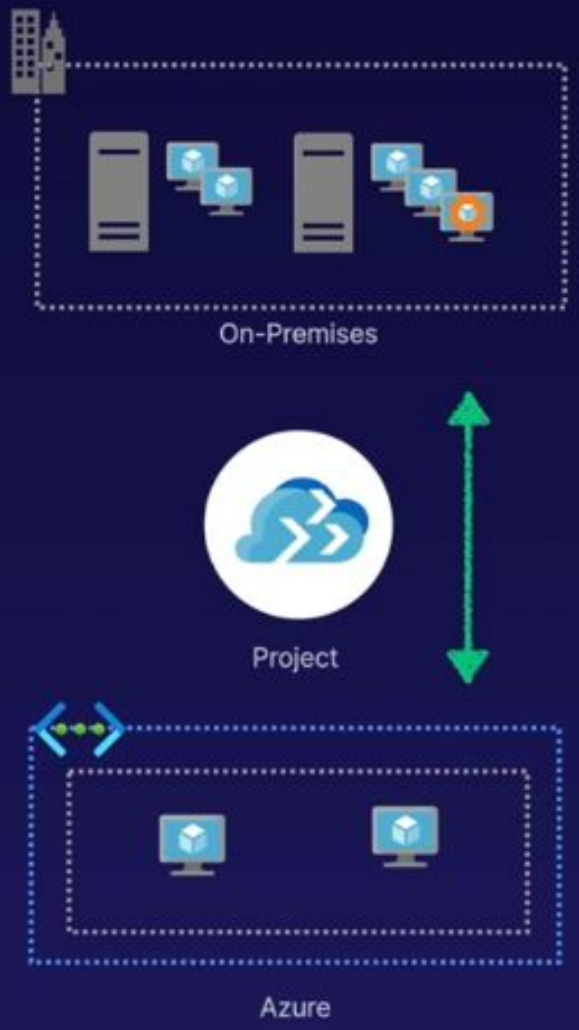


Azure Migrate

Azure Migrate

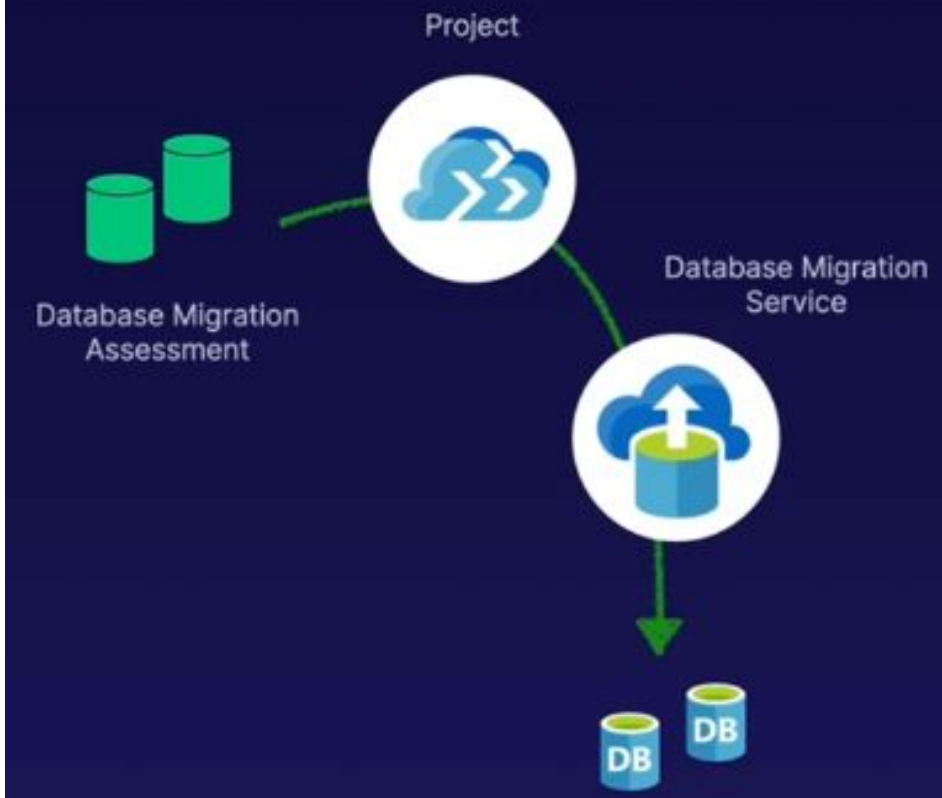


Azure Migrate For Servers



Property	Description
Migrate Project	Houses important metadata regarding assessment findings and migration activities.
Discovery	Performed using the Azure Migrate appliance in your source environment, to identify servers to migrate.
Assessment	Evaluate the identified server(s), provide estimated costs, and provide an assessment of the readiness for migration.
Migration	Migrate workloads, including VMware VMs, Hyper-V VMs, physical servers, and public cloud VMs.

Azure Migrate For Databases



Property	Description
Migrate Project	Houses important metadata regarding assessment findings and migration activities.
Assessment	Performed using the Azure Database Migration Assessment (DMA) tool. Evaluates a source database, with a target destination (e.g. Azure SQL).
Database Migration Service	To facilitate the migration of data between source and target services, we use the Azure Database Migration Service (DMS).
Migration	Migrations can be performed offline, or online. The options available depend on the source/target pair scenario.

Thank you!