

# AZURE 104



Azure Identities and  
Governance

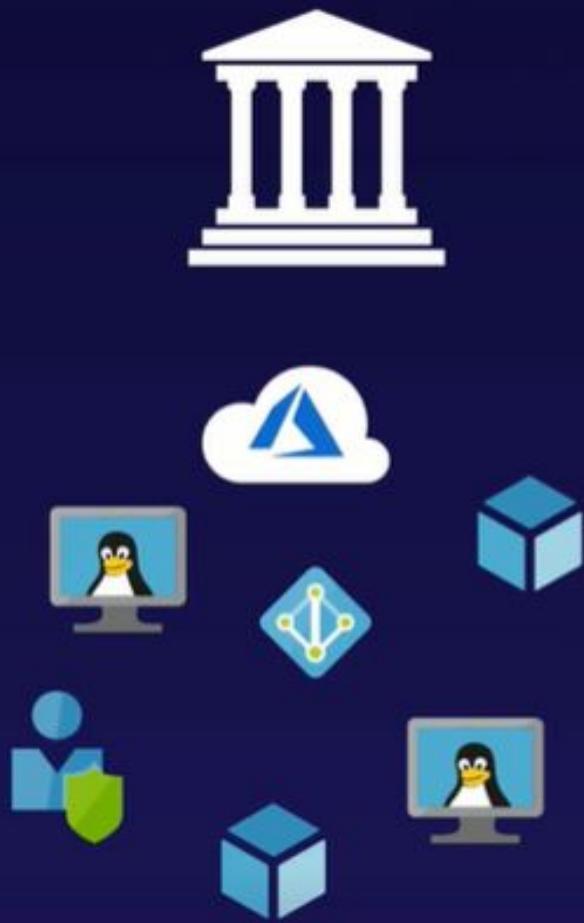
# Plan

- 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



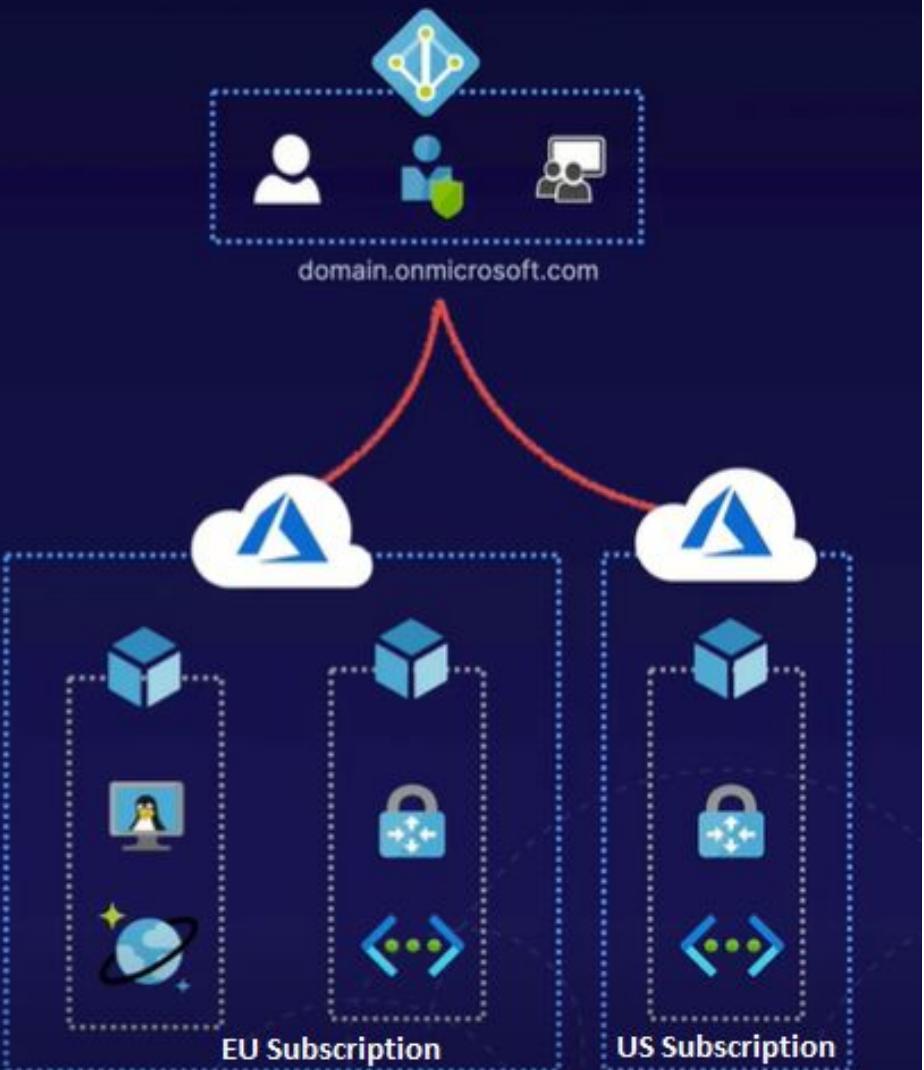
## Azure Subscription

- 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 - Microsoft Azure

https://portal.azure.com/#@jazlab1.com/resource/subscriptions/f5bde2a6-146a-4e8a-b255-b2dc0ad6180a/resourceGroups/jazlab-dev-financeweb-rg/overview

Guest JAZ LAB adm.jlee@jazlab1.onmicrosoft.com

Microsoft Azure Search resources, services, and docs (G+)

Home > Subscriptions > JAZ Lab Development Subscription | Resource groups >

jazlab-dev-financeweb-rg Resource group

Add Edit columns Delete resource group Refresh Move Export to CSV Assign tags Delete Export template Feedback

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 - Microsoft Azure

https://portal.azure.com/#@jazlab1.com/resource/subscriptions/5bde2a6-146a-4e8a-b255-b2dc0ad6180a/resourceGroups/jazlab-dev-financeweb-rg/providers/Microsoft.Compute/virtualMachines/devfinanceweb1/tags

Guest JAZ LAB

Microsoft Azure

Search resources, services, and docs (G+?)

Home > Subscriptions > JAZ Lab Development Subscription | Resource groups > **jazlab-dev-financeweb-rg** >

devfinanceweb1 | Tags

Virtual machine

Search (Ctrl + F)

Save Delete all Revert changes

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

Overview  
Activity log  
Access control (IAM)  
**Tags**  
Diagnose and solve problems  
Networking  
Connect  
Disks  
Size  
Security  
Extensions  
Continuous delivery  
Availability + scaling  
Configuration  
Identity  
Properties  
Locks

# 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

Asia Pacific  
•  
•  
•  
•  
•  
•  
•  
•  
Finance

Americas  
•  
•  
•  
•  
Marketing

IT

# 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

The screenshot shows the Microsoft Azure portal interface with the URL [https://portal.azure.com/#blade/Microsoft\\_Azure\\_ManagementGroups/HierarchyBlade](https://portal.azure.com/#blade/Microsoft_Azure_ManagementGroups/HierarchyBlade). The page title is "Management groups - Microsoft Azure". The top navigation bar includes "Guest", "adm.jlee@jazlab1.onmicrosoft.com", and "JAZ LAB". The left sidebar shows "Home > Management groups" under "JAZ Lab". The main content area displays a search bar with "Search resources, services, and docs (G+I)" and a search history list containing "management group", "firewall", "network security g", "privil", and "access review". Below the search history are sections for "Recent services" (Management groups, Subscriptions, Resource groups, All resources, Firewalls, Network security groups, Azure AD Privileged...), "Recent resources" (devfinanceweb1, jazlab-dev-financeweb-rg, JAZ Lab Development Subscription, JAZ Lab Production Subscription, jazlab-dev-corevnet-rg), and a note about grouping subscriptions for policy and compliance. At the bottom, it says "Searching 1 of 2 subscriptions".

# Azure Management Groups

The screenshot shows the Microsoft Azure Management Groups HierarchyBlade interface. At the top, there's a navigation bar with links for Home, Management groups, and JAZ Lab. Below the navigation bar, there's a search bar labeled "Search resources, services, and docs (G+ /)". On the right side of the header, there are user profile icons for "Guest" and "adm.jlee@jazlab1.onmicrosoft.com" with "JAZ LAB" below it.

The main content area is titled "Management groups" and shows a "Tenant Root Group". A search bar at the top of this section allows searching by name or ID. A note indicates that the user is registered as a directory admin but does not have the necessary permissions to access the root management group, with a link to learn more.

The "Tenant Root Group (details)" table lists three items:

Name	ID	Type	My Role	...
(A) Asia Pacific	asiapacific	Management Group	Owner	...
JAZ Lab Development Subscription	f5bde2a6-146a-4e8a-b255-b2dc0ad6180a	Subscription	Owner	...
JAZ Lab Production Subscription	2ed17b0d-359f-4220-be01-60080a67bb22	Subscription	Owner	...

# Azure Management Groups

The screenshot shows the Microsoft Azure portal interface with the following details:

- Page Title:** Add subscription - Microsoft
- URL:** https://portal.azure.com/#blade/Microsoft\_Azure\_ManagementGroups/MenuBlade/overview/name/asiapacific
- User Information:** Guest, adm.jlee@jazlab1.onmicrosoft.com, JAZ LAB
- Breadcrumbs:** Home > Management groups >
- Management Group Overview:** Asia Pacific (Management group)
  - Search bar: Search (Cmd + /)
  - Action buttons: Rename Group, Delete, Move, Add management group, Add subscription, Refresh.
  - Properties:
    - Name: Asia Pacific
    - ID: asiapacific
    - Access Level: Owner
  - Relationships:
    - Parent management group: Tenant Root Group
    - Child management groups: 0
  - Subscription dropdown: Subscription \* (dropdown menu open, showing options: JAZ Lab Development Subscription (f5bde2a6-146a-4e8a-b255-b2dc0ad6180a) and JAZ Lab Production Subscription (2ed17b0d-359f-4220-be01-60080a67bb22))
- Add subscription Dialog:** Move an existing subscription to be a child of 'Asia Pacific'
  - Subscription \* (dropdown menu open, showing options: JAZ Lab Development Subscription (f5bde2a6-146a-4e8a-b255-b2dc0ad6180a) and JAZ Lab Production Subscription (2ed17b0d-359f-4220-be01-60080a67bb22))

# Azure Management Groups

The screenshot shows the Azure Management Groups blade for the 'Asia Pacific' management group. The URL is https://portal.azure.com/#blade/Microsoft\_Azure\_ManagementGroups/MenuBlade/overview/name/asiapacific. The left sidebar includes links for Home, Management groups, Asia Pacific (selected), Activity Log, Access control (IAM), Policies, Cost Management, Cost analysis, Budgets, Settings, and Deployments. The main content area displays the 'Overview' tab for the 'Asia Pacific' management group. It shows the following details:

Name	ID	Access Level	Parent management group	Child management groups
Asia Pacific	asiapacific	Owner	Tenant Root Group	0

Below this, there is a search bar labeled 'Search by name or ID' and a table showing a single subscription entry:

Name	ID
JAZ Lab Production Subscription	zed17b0d-359f-4220-be01-60080a67bb22

# Role-Based Access Control

## Secure Access to Azure Resources

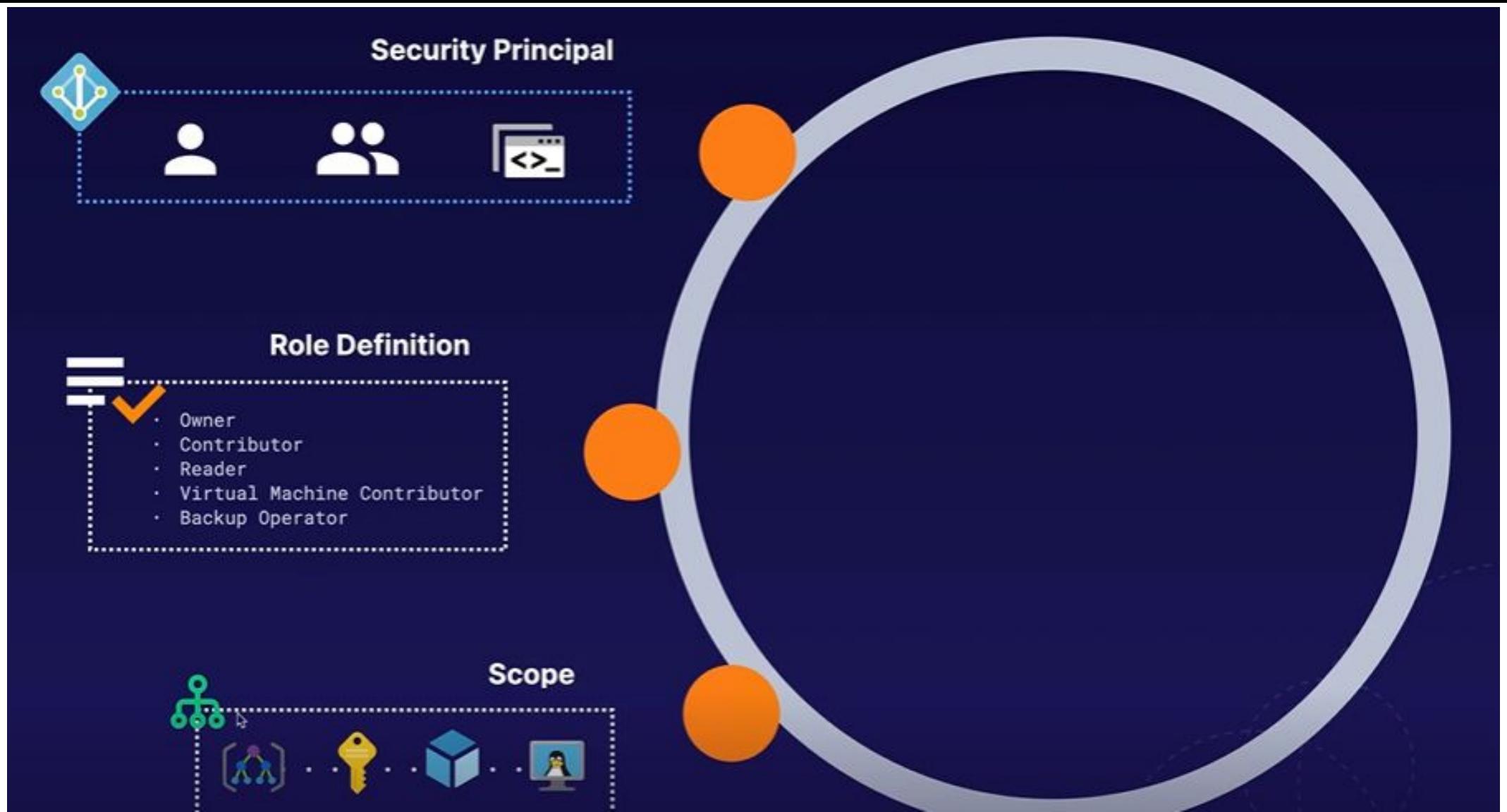


Role-based access control (RBAC) allows us to implement secure access, following the principle of least privilege.

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

Microsoft Azure Guest JAZ LAB

https://portal.azure.com/#@jazlab1.com/resource/subscriptions/2ed17b0d-359f-4220-be01-60080a67bb22/resourceGroups/jazlab-prod-phoenix-rg/users

Home > Resource groups >

**Resource groups**

JAZ Lab

+ Add Manage view ...

Filter by name...

Name	...
cloud-shell-storage-southeastasia	...
jazlab-dev-corevnet-rg	...
jazlab-dev-financeweb-rg	...
jazlab-prod-corenet-rg	...
<b>jazlab-prod-phoenix-rg</b>	...
jazlab-prod-project123-rg	...
NetworkWatcherRG	...
NetworkWatcherRG	...
nsg01-rg	...

**jazlab-prod-phoenix-rg | Access control (IAM)**

Search resources, services, and docs (G+)

+ Add Edit columns Refresh Remove Got feedback?

Check access Role assignments Deny assignments Classic administrators Roles

**Check access**  
Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Find: Azure AD user, group, or service principal

Search by name or email address

**Add a role assignment**  
Grant access to resources at this scope by assigning a role to a user, group, service principal, or managed identity.

Add Learn more

**View role assignments**  
View the users, groups, service principals and managed identities that have role assignments granting them access at this scope.

View Learn more

**View deny assignments**  
View the users, groups, service principals and managed identities that have been denied access to specific actions at this scope.

View Learn more

**Add role assignment**

Role: Virtual Machine Contributor

Assign access to: Azure AD user, group, or service principal

Select: Search by name or email address

Admin - James Lee  
adm.jlee@jazlab1.onmicrosoft.com

Egwene al'Vere  
egwene@jazlab1.com

J.lee@live.com.au Lee  
j.lee\_live.com.au#EXT#@jelivecom.onmicrosoft.com

Heilo Agathon  
karl@jazlab1.com

Laura Roslin  
laura@jazlab1.com

Apollo Adama  
jeel@jazlab1.com

Selected members:  
No members selected. Search for and add one or more members you want to assign to the role for this resource.

Learn more about RBAC

# Role-Based Access Control – Custom RBAC Roles

```
{  
  "name": "Helpdesk Admins",  
  "description": "Permissions for Helpdesk staff",  
  
  "actions": [  
    "*/read",  
    "Microsoft.Compute/virtualMachines/start/action",  
    "Microsoft.Support/*",  
  ],  
  "notActions": [],  
  "dataActions": [],  
  "notDataActions": [],  
  
  "assignableScopes": [  
    "/subscriptions/{subscriptionId}"  
  ]  
}
```



## METADATA (NAME, ID, ETC.)

Details information such as the name of the custom role, ID, description, and whether it is a custom or built-in role.



## ACTIONS

Includes actions and notActions, which define management operations that are (or are not) allowed to be performed.



## DATA ACTIONS

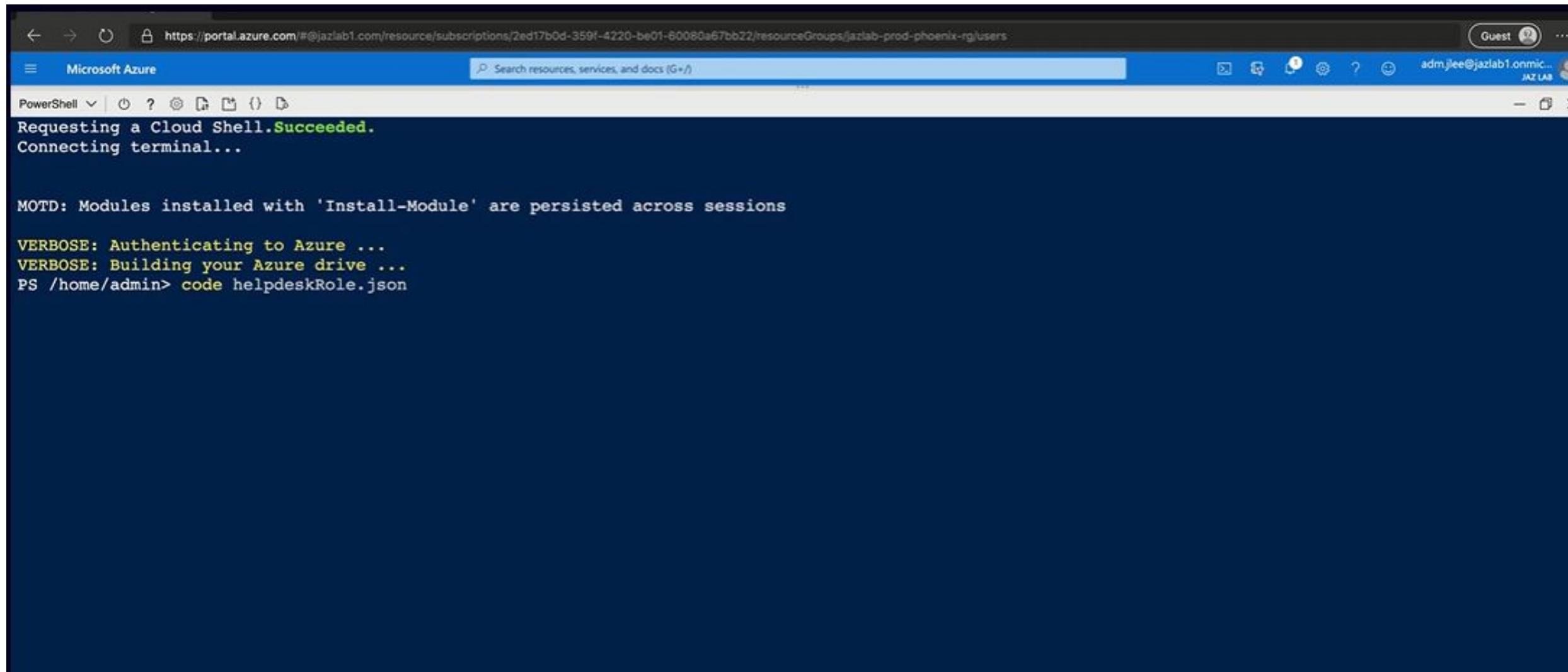
Defines dataActions and notDataActions, which define operations the role can (or cannot) perform on data.



## Assignable Scopes

Specifies where the management groups, subscriptions, or resource groups this role can be assigned to.

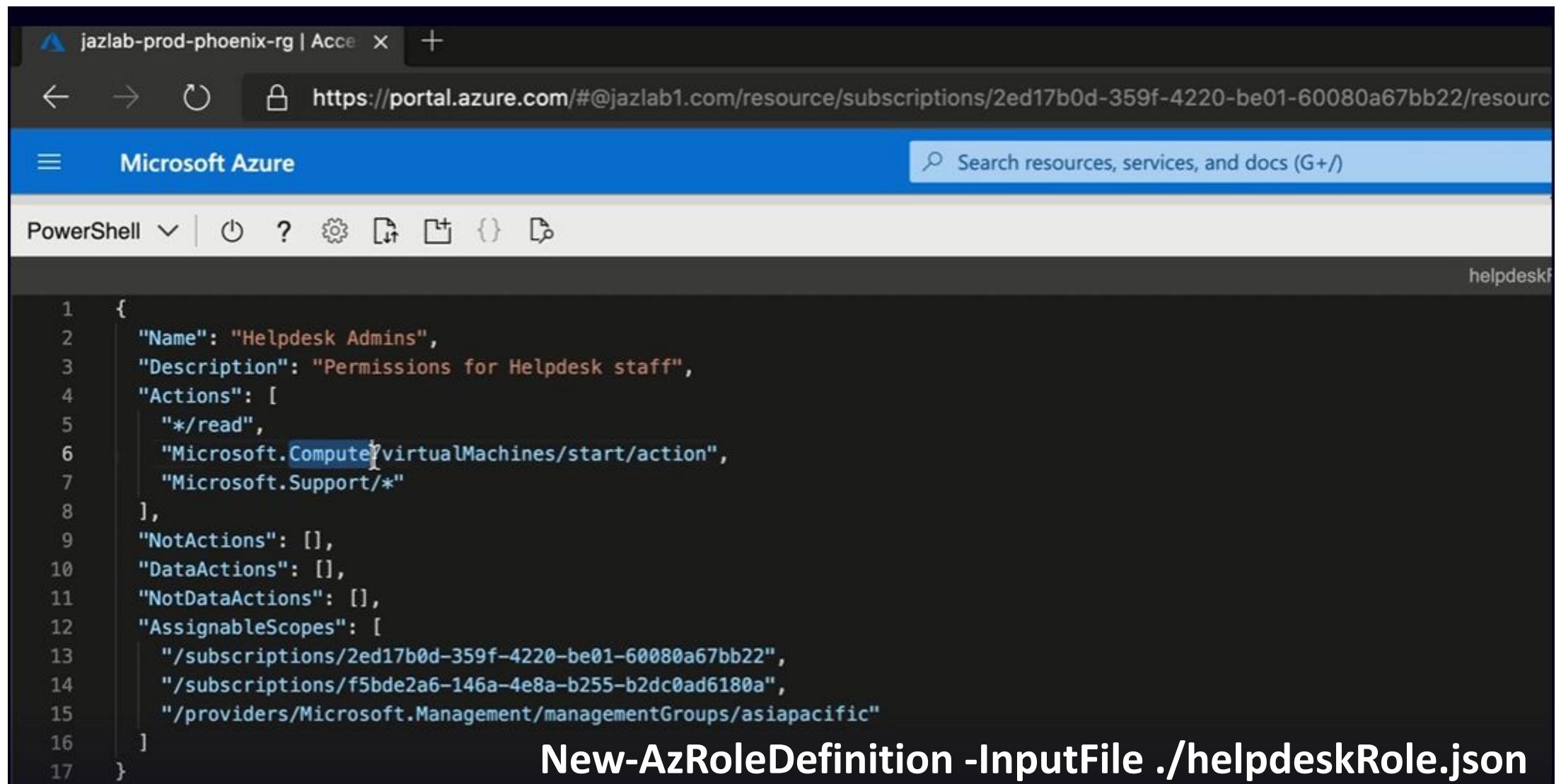
# Role-Based Access Control



The screenshot shows a Microsoft Azure Cloud Shell interface. The URL in the address bar is <https://portal.azure.com/#@jazlab1.com/resource/subscriptions/2ed17b0d-359f-4220-be01-60080a67bb22/resourceGroups/jazlab-prod-phoenix-rg/users>. The top navigation bar includes 'Guest' and 'admjlee@jazlab1.onmicrosoft.com JAZ LAB'. The main content area is a terminal window titled 'PowerShell'.

```
Requesting a Cloud Shell. Succeeded.  
Connecting terminal...  
  
MOTD: Modules installed with 'Install-Module' are persisted across sessions  
  
VERBOSE: Authenticating to Azure ...  
VERBOSE: Building your Azure drive ...  
PS /home/admin> code helpdeskRole.json
```

# Role-Based Access Control



A screenshot of the Microsoft Azure portal interface. The title bar shows the subscription name "jazlab-prod-phoenix-rg | Acce" and a URL pointing to the Azure portal's resource management section. The main content area displays a JSON role definition titled "Helpdesk Admins". The JSON code is as follows:

```
1  {
2      "Name": "Helpdesk Admins",
3      "Description": "Permissions for Helpdesk staff",
4      "Actions": [
5          "*/*",
6          "Microsoft.Compute/virtualMachines/start/action",
7          "Microsoft.Support/*"
8      ],
9      "NotActions": [],
10     "DataActions": [],
11     "NotDataActions": [],
12     "AssignableScopes": [
13         "/subscriptions/2ed17b0d-359f-4220-be01-60080a67bb22",
14         "/subscriptions/f5bde2a6-146a-4e8a-b255-b2dc0ad6180a",
15         "/providers/Microsoft.Management/managementGroups/asiapacific"
16     ]
17 }
```

The command at the bottom of the image is:

New-AzRoleDefinition -InputFile ./helpdeskRole.json

# Role-Based Access Control

https://portal.azure.com/#blade/Microsoft\_Azure\_ManagementGroups/MenuBlade/fam/name/asiapacific

Microsoft Azure Guest, JAZ LAB adm.jlee@jazlab1.onmicrosoft.com

Home > Management groups >

## Asia Pacific | Access control (IAM)

Management group

Search (Cmd+.) Add Edit columns Refresh Remove Got feedback?

Overview Activity Log Access control (IAM) Policies Cost Management Cost analysis Budgets Settings Deployments

Check access Role assignments Deny assignments Classic administrators Roles

**Check access**  
Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Find: Azure AD user, group, or service principal Search by name or email address

**Add a role assignment**  
Grant access to resources at this scope by assigning a role to a user, group, service principal, or managed identity.

**View role assignments**  
View the users, groups, service principals and managed identities that have role assignments granting them access at this scope.

**View deny assignments**  
View the users, groups, service principals and managed identities that have been denied access to specific actions at this scope.

**Add role assignment**

Role: Helpdesk Admins

Assign access to: Azure AD user, group, or service principal

Select: Search by name or email address

Admin - James Lee  
adm.jlee@jazlab1.onmicrosoft.com

Egwene al'Vere  
egwene@jazlab1.com

j.lee@live.com.au Lee  
j.lee.live.com.au#EXT#@jelivecom.onmicrosoft.com

Helo Agathon  
karl@jazlab1.com

Laura Roslin  
laura@jazlab1.com

DnsAdmins

Selected members:

Apollo Adama  
lee@jazlab1.com

Remove

The screenshot shows the Microsoft Azure portal interface for managing access control in a specific management group. The main page displays four main sections: 'Check access', 'Add a role assignment', 'View role assignments', and 'View deny assignments'. A modal window on the right is titled 'Add role assignment' and shows the 'Helpdesk Admins' role being assigned to the user 'Apollo Adama' (email: lee@jazlab1.com). The user is listed under the 'Selected members:' section. The portal URL in the browser bar is https://portal.azure.com/#blade/Microsoft\_Azure\_ManagementGroups/MenuBlade/fam/name/asiapacific.

# 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"



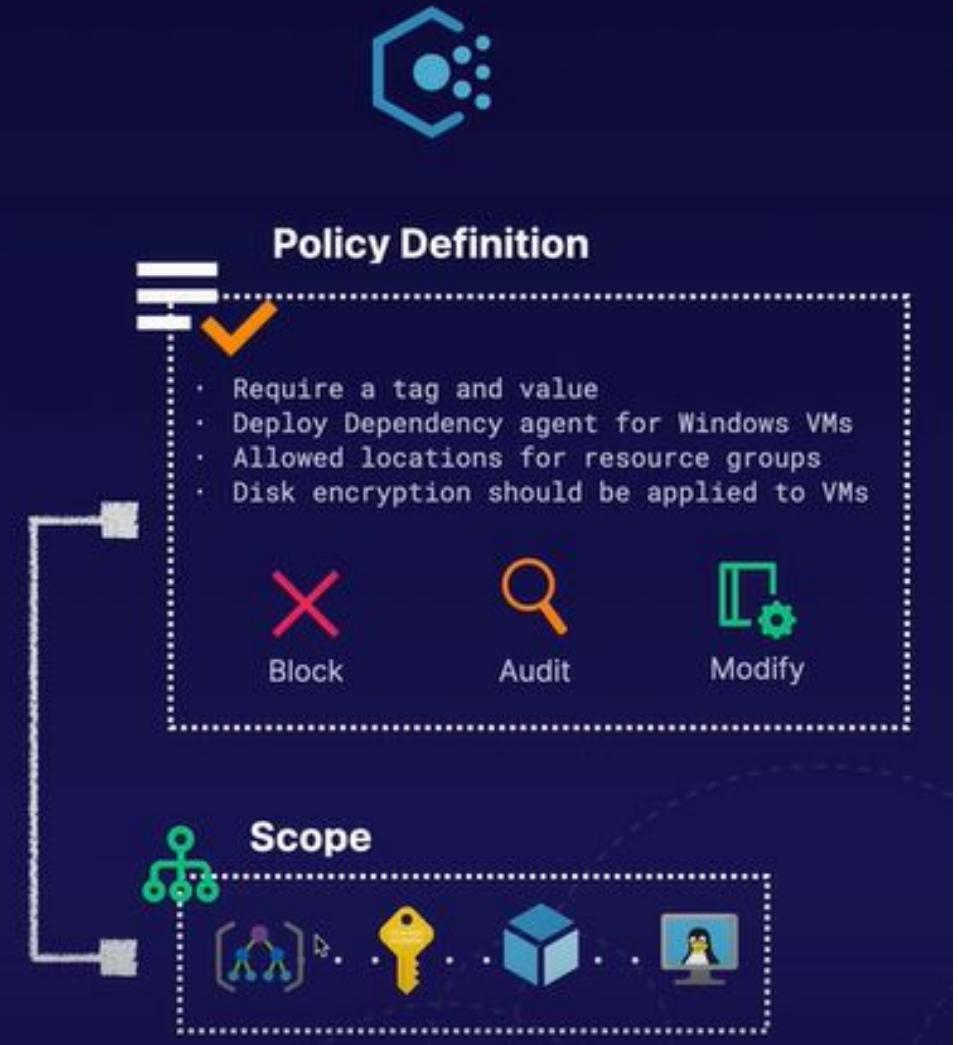
## Trigger an Effect

- 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

The screenshot shows the Microsoft Azure portal home page. At the top, there is a navigation bar with links for Home - Microsoft Azure, Guest, and admjlee@jazlab1.onmicrosoft.com (JAZ LAB). Below the navigation bar is a search bar labeled "Search resources, services, and docs (G+ /)". The main content area is titled "Azure services" and features a "Create a resource" button, a "Policy" button (which is highlighted with a white border), "Blueprints", "Azure Active Directory", "All resources", "Management groups", "Resource groups", "Subscriptions", "Firewalls", and a "More services" link. Below this is a section titled "Recent resources" which lists various Azure resources with their names, types, and last viewed times. At the bottom, there is a "Navigate" section with links for Subscriptions, Resource groups, All resources, and Dashboard.

Name	Type	Last Viewed
[RG] jazlab-prod-phoenix-rg	Resource group	7 minutes ago
[RG] jazlab-prod-project123-rg	Resource group	22 hours ago
[S] JAZ Lab Production Subscription	Subscription	22 hours ago
[VM] devfinanceweb1	Virtual machine	23 hours ago
[RG] jazlab-dev-financeweb-rg	Resource group	23 hours ago
[S] JAZ Lab Development Subscription	Subscription	23 hours ago
[RG] jazlab-dev-corevnet-rg	Resource group	23 hours ago
[RG] jazlab-prod-corenet-rg	Resource group	23 hours ago
[ASG] asg01	Application security group	7 days ago
[NSG] nsg01	Network security group	7 days ago

**Recent resources**

**Subscriptions**

**Resource groups**

**All resources**

**Dashboard**

# Azure Policy – How it works

Screenshot of the Azure Policy Overview blade in the Microsoft Azure portal.

The URL is [https://portal.azure.com/#blade/Microsoft\\_Azure\\_Policy/PolicyMenuBlade/Overview](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyMenuBlade/Overview).

The scope is set to "JAZ Lab Production Subscription".

Overall resource compliance: 98% (181 out of 184)

Non-compliant initiatives: 1 out of 1

Non-compliant policies: 5 out of 99

Non-compliant resources: 3 out of 184

**Authoring**

Name	Scope	Compliance state	Resource compliance	Non-Compliant Resources	Non-compliant policies
ASC Default (subscription: 2ed17b0d-359f-4220-...)	JAZ Lab Production Subscription	Non-compliant	98% (181 out of 184)	3	5

**Related Services**

- Blueprints (preview)
- Resource Graph
- User privacy

**Assignments by Compliance (Last 7 Days)**

Date	Count
5/21/2020	1
5/22/2020	1
5/23/2020	1
5/24/2020	1
5/25/2020	1
5/26/2020	1
5/27/2020	1
5/28/2020	1
5/29/2020	1

# Azure Policy – How it works

The screenshot shows the Azure Policy Definitions blade in the Azure portal. The URL is https://portal.azure.com/#blade/Microsoft\_Azure\_Policy/PolicyMenuBlade/Definitions. The left sidebar shows navigation options like Overview, Getting started, Join Preview, Compliance, Remediation, Authoring, Assignments, and Definitions (which is selected). The main area has search and filter controls: Scope (2 selected), Definition type (Policy), Type (All types), Category (All categories), and a search bar for location. A table lists several policy definitions:

Name	Definition location	Policies	Type	Definition type	Category
Azure Cosmos DB allowed locations			Built-in	Policy	Cosmos DB
Configure backup on VMs of a location to an existing central Vault in the ...			Built-in	Policy	Backup
Audit resource location matches resource group location			Built-in	Policy	General
Allowed locations			Built-in	Policy	General
Allowed locations for resource groups			Built-in	Policy	General

# Azure Policy – How it works

The screenshot shows the Azure Policy Definitions blade. The URL is https://portal.azure.com/#blade/Microsoft\_Azure\_Policy/PolicyMenuBlade/Definitions. The policy definition is named 'Allowed locations'. It has a description: 'This policy enables you to restrict the locations your organization can specify when deploying resources. Use to enforce your geo-compliance requirements. Excludes resource groups, Microsoft.AzureActiveDirectory/b2cDirectories, and Microsoft.FluentIdentityPlatform/b2cApplications.' The available effects are 'Deny', and the category is 'General'. The mode is 'Indexed'. The JSON code for the policy definition is displayed below:

```
1 {
2   "properties": {
3     "displayName": "Allowed locations",
4     "policyType": "BuiltIn",
5     "mode": "Indexed",
6     "description": "This policy enables you to restrict the locations your organization can specify when deploying resources. Use to enforce your geo-compliance requirements. Excludes resource groups, Microsoft.AzureActiveDirectory/b2cDirectories, and Microsoft.FluentIdentityPlatform/b2cApplications.",
7     "metadata": {
8       "version": "1.0.0",
9       "category": "General"
10    },
11    "parameters": {
12      "listOfAllowedLocations": {
13        "type": "Array",
14        "metadata": {
15          "description": "The list of locations that can be specified when deploying resources.",
16          "strongType": "location",
17          "displayName": "Allowed locations"
18        }
19      }
20    },
21    "policyRule": {
22      "if": {
23        "allOf": [
24          {
25            "field": "location",
26            "operator": "notEqual",
27            "values": [
28              "Microsoft.FluentIdentityPlatform/b2cApplications"
29            ]
30          }
31        ]
32      }
33    }
34  }
35 }
```

# Azure Policy – How it works

The screenshot shows the Azure portal interface for creating a policy definition. The URL in the address bar is [https://portal.azure.com/#blade/Microsoft\\_Azure\\_Policy/PolicyMenuBlade/Definitions](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyMenuBlade/Definitions). The top navigation bar includes 'Scope - Microsoft Azure', 'Guest', and the user 'admjlee@jazlab1.onmicrosoft.com JAZ LAB'. The main content area is titled 'Allowed locations' under 'Policy | Definitions > Allowed locations'. It has tabs for 'Basics', 'Parameters', 'Remediation', and 'Review + create'. The 'Basics' tab is selected. The 'Scope' section contains dropdown menus for 'Management Group' (set to 'Tenant Root Group (c4d46e81-4400-49cf-a173-b10d0034a178)'), 'Region' (set to 'Asia Pacific (asiapacific)'), 'Subscription' (set to 'JAZ Lab Development Subscription'), and 'Resource Group' (set to 'jazlab-dev-financeweb-rg'). The 'Basics' section includes fields for 'Policy definition' (set to 'Allowed locations'), 'Assignment name' (set to 'Allowed locations'), and a large 'Description' text area.

# Azure Policy – How it works

The screenshot shows the 'Allowed locations' configuration page in the Azure portal. The URL is https://portal.azure.com/#blade/Microsoft\_Azure\_Policy/PolicyMenuBlade/Definitions. The page title is 'Allowed locations'. There are tabs for 'Basics', 'Parameters' (which is selected), 'Remediation', and 'Review + create'. Below the tabs, it says 'Specify parameters for this policy assignment.' and 'Allowed locations \*'. A dropdown menu shows '0 selected'. A scrollable list of Azure regions follows:

- Australia Central
- Australia Central 2
- Australia East
- Australia Southeast
- Brazil South
- Canada Central
- Canada East
- Central India
- Central US
- East Asia
- East US
- East US 2
- France Central
- France South
- Germany North
- Germany West Central
- Global

# Azure Policy – How it works

The screenshot displays two instances of the 'Create a virtual machine' wizard side-by-side, illustrating the validation process and successful creation.

**Left Side (Validation Failed):**

- Subscription:** JAZ Lab Development Subscription
- Resource group:** jazlab-dev-financeweb-rg
- Virtual machine name:** (empty)
- Region:** (Europe) UK West
- Availability options:** No infrastructure redundancy required
- Image:** Windows Server 2016 Datacenter
- Azure Spot Instance:** No
- Size:** Standard DS1 v2 (1 vCPU, 3.5 GB memory, A\$147.34/month)
  - This size is currently unavailable in this location for this subscription: NotAvailableForSubscription.
  - Your subscription doesn't support virtual machine creation in UK West. Choose a different location. Learn more.

**Right Side (Success):**

- Subscription:** JAZ Lab Development Subscription
- Resource group:** jazlab-dev-financeweb-rg
- Virtual machine name:** vm1
- Region:** West Central US
- Availability options:** No infrastructure redundancy required
- Username:** adm-jlee
- Public inbound ports:** RDP

**Common UI Elements:**

- Basics Tab:** Selected tab for both forms.
- Review + create Tab:** Available in both forms.
- Validation Error Message:** Validation failed. Click here to view details.
- Product Details:** Standard DS1 v2 by Microsoft.
- Subscription Credits:** 0.1606 AUD/hr.
- Terms:** By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.
- Warning Message:** You have set RDP port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

# Azure Policy – How it works

Initiative definition - Microsoft | X +

https://portal.azure.com/#blade/Microsoft\_Azure\_Policy/PolicyMenuBlade/Definitions

Microsoft Azure Guest ...

Search resources, services, and docs (G+/)

Home > Policy | Definitions >

## Initiative definition

New Initiative definition

**BASICS**

Definition location \* JAZ Lab Development Subscription

Name \* Allowed Locations

Description Describe the initiative you are authoring

Category Create new (radio button selected) Use existing

Category

**AVAILABLE DEFINITIONS**

Type All types Search location

Policy Definitions (5)

+ Azure Cosmos DB allowed locations  
Built-in This policy enables you to restrict the locations your organization can specify when deploying Azure Cosmos DB resources. Use to enforce your geo-compliance requirements.

+ Configure backup on VMs of a location to an existing central Vault in the same location  
Built-in This policy configures Azure Backup protection on VMs in a given location to an existing central vault in the same location. It applies to only those VMs that are not already configured for backup. It is recommended that this policy is assigned to not more than 200 VMs. If the policy is assigned for more than 200 VMs, it can result in the backup getting triggered a few hours beyond the defined schedule. This policy will be enhanced to support

+ Audit resource location matches resource group location  
Built-in Audit that the resource location matches its resource group location

+ Allowed locations  
Built-in This policy enables you to restrict the locations your organization can specify when deploying resources. Use to enforce your geo-compliance requirements. Excludes resource groups, Microsoft.AzureActiveDirectory/b2cDirectories, and resources that use the 'global' region.

+ Allowed locations for resource groups  
Built-in This policy enables you to restrict the locations your organization can create resource groups in. Use to enforce your geo-compliance requirements.

Initiative parameters	Parameter name	Display name	Type	Allowed values
-----------------------	----------------	--------------	------	----------------

# 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

The diagram illustrates the Azure Blueprints architecture. It starts with a **Blueprint Definition** (represented by a blue icon with a gear and pencil), which is published as **v2.0** (represented by an orange icon with a downward arrow). This leads to **Assignments** (represented by a green icon with a user icon) and finally the execution of the Blueprint (represented by a yellow icon with a play button).

**Blueprint Definition**

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

**v2.0**

**Publishing and Version Control**

- 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**

**Definition**

**Assignments**

**I**

# Azure Blueprints

Blueprints | Getting started - + https://portal.azure.com/#blade/Microsoft\_Azure\_Policy/BlueprintsMenuBlade/GetStarted Microsoft Azure Search resources, services, and docs (G+) Home > Blueprints | Getting started

Search (Cend +/)

Getting started Blueprint definitions Assigned blueprints

Welcome to Azure Blueprints PREVIEW

Blueprints enable quick creation of governed subscriptions. This allows Cloud Architects to design environments that comply with organizational standards and best practices – enabling your app teams to get to production faster.

Blueprints Overview ⓘ Create a blueprint in the Azure Portal ⓘ Create a blueprint with the REST API ⓘ

Create a blueprint

Compose artifacts such as templates, policies, role assignments, and resource groups based on common or organization-based patterns into re-usable blueprints.

Create

Apply to a scope

Apply your blueprint to one or more subscriptions

Apply

Track assignments

Track where blueprints have been applied and share them across your organization

Track

# Azure Blueprints

The screenshot shows the Microsoft Azure portal interface for creating a blueprint. The title bar reads "Create blueprint - Microsoft Azure". The address bar shows the URL: [https://portal.azure.com/#blade/Microsoft\\_Azure\\_Policy/BlueprintsMenuBlade/GetStarted](https://portal.azure.com/#blade/Microsoft_Azure_Policy/BlueprintsMenuBlade/GetStarted). The top navigation bar includes the Microsoft Azure logo and a search bar labeled "Search resources, services, and docs (G+I)". Below the navigation bar, the breadcrumb trail shows "Home > Blueprints | Getting started > Create blueprint".

**Create blueprint**

**Choose a blueprint sample**

You can start with a blank blueprint or pick one of our pre-defined samples to help you get started quickly

**Blank Blueprint**  
An empty blueprint with no initial properties or artifacts.  
**Start with blank blueprint**

**Other Samples**

Filter samples by name and description

Name	Description
Azure Security Benchmark	Assigns policies to address specific recommendations from the Azure Security Benchmark. <a href="#">Learn more</a>
Basic Networking (VNET)	Configures a virtual network with a subnet and an NSG.
CAF Foundation	Microsoft Cloud Adoption Framework for Azure – Configure Foundational best practices <a href="#">Learn more</a>
CAF Migration landing zone	Microsoft Cloud Adoption Framework for Azure – Migrations landing zone <a href="#">Learn more</a>
Canada Federal PBMM	Assigns policies to address Canada Federal PBMM controls. <a href="#">Learn more</a>
CIS Microsoft Azure Foundations Bench...	Assigns policies to address specific recommendations from the CIS Microsoft Azure Foundations Benchmark v1.1... <a href="#">Learn more</a>
Common Policies	A set of popular policies to apply to a subscription
FedRAMP High	Assigns policies to address specific FedRAMP High controls. <a href="#">Learn more</a>

# Azure Blueprints

Add artifact - Microsoft Azure + https://portal.azure.com/#blade/Microsoft\_Azure\_Policy/BlueprintsMenuBlade/GetStarted Guest adm.jiee@jazlab1.onmicrosoft.com JAZ LAB

Microsoft Azure Search resources, services, and docs (G+) Home > Blueprints | Getting started > Create blueprint

Basics Artifacts Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

Name	Artifact type	Param
Subscription	Resource group	0 out
+ Add artifact...		
Resource Group		
+ Add artifact...		

Add artifact

Artifact type \* Azure Resource Manager template

Artifact display name \* Enter display name for the artifact in the blueprint definition

Description Enter description

Template Parameters Import template Select a file

```
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {},
5   "variables": {
6     "storageAccountName": "[toLowerCase(concat('azurelalab', uniqueString(resourceGroup().id)))]",
7     "networkSecurityGroupName": "shared-nsg",
8     "vNet1": {
9       "name": "vnet1",
10      "addressSpacePrefix": "10.1.0.0/16",
11      "subnetName": "subnet1",
12      "subnetPrefix": "10.1.1.0/24"
13    },
14    "adminUserName": "azureuser",
15    "adminPassword": "labh01-2021-learn!",
16    "imagePublisher": "MicrosoftWindowsServer",
17    "imageOffer": "WindowsServer",
18  }
}
```

# Azure Blueprints

The screenshot shows the Microsoft Azure portal interface for creating a blueprint. The top navigation bar includes the 'Add artifact - Microsoft Azure' tab, the URL [https://portal.azure.com/#blade/Microsoft\\_Azure\\_Policy/BlueprintsMenuBlade/GetStarted](https://portal.azure.com/#blade/Microsoft_Azure_Policy/BlueprintsMenuBlade/GetStarted), and the user 'Guest'. The main content area is titled 'Create blueprint' and has tabs for 'Basics' and 'Artifacts', with 'Artifacts' selected. A sub-header says 'Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.' Below this, there are three rows of artifact types:

Name	Artifact type	Param
Subscription	Resource group	0 out
+ Add artifact...	Azure Resource Manager template	None

To the right, an 'Add artifact' dialog is open. It has a title 'Add artifact' and a section for 'Artifact type \*' which is set to 'Role assignment'. A note says 'You can choose to fill these parameters in now or when assigning the blueprint.' Below this, a 'Role' section shows 'Owner' selected. A note says 'Add user, app or group:'. At the bottom of the dialog is a checked checkbox: 'This value should be specified when the blueprint is assigned'.

# Azure Blueprints

Create blueprint - Microsoft Azure

https://portal.azure.com/#blade/Microsoft\_Azure\_Policy/BlueprintsMenuBlade/GetStarted

Microsoft Azure

Search resources, services, and docs (G + /)

Guest (17) ...

adm.jlee@jazlab1.onmicrosoft.com JAZ LAB

Home > Blueprints | Getting started >

## Create blueprint

Basics Artifacts

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

Name	Artifact type	Parameters
✓ Subscription		
+ Add artifact...		
✓ Resource Group	Resource group	0 out of 2 parameters populated
ARMTemplate	Azure Resource Manager template	None
{User group or application name} : Owner	Role assignment	0 out of 1 parameters populated
Allowed locations	Policy assignment	1 out of 1 parameters populated
+ Add artifact...		

# Azure Blueprints

Assign blueprint - Microsoft Azure

https://portal.azure.com/#blade/Microsoft\_Azure\_Policy/BlueprintsMenuBlade/Blueprints

Microsoft Azure

Search resources, services, and docs (G+F)

Home > Blueprints | Blueprint definitions >

## Assign blueprint

Basics

Subscription(s) ○  
JAZ Lab Development Subscription

Assignment name \* ○  
Assignment-devfinanceweb

Location \* ○  
Australia Southeast

Blueprint definition version \* ○  
v1.0

v1.0  
Lock Assignment

Don't Lock Do Not Delete Read Only

The assignment is not locked. Users, groups, and service principals with permissions can modify and delete deployed resources.  
[Learn more](#)

Managed Identity ○  
 System assigned  
 User assigned

By clicking "Assign" with a system assigned identity, you agree to grant the Azure Blueprints service temporary Owner access to this subscription so that we can properly deploy all Artifacts. We will automatically remove this access when the blueprint assignment process is finished.

# Azure Blueprints

The screenshot shows the 'Assign blueprint' page in the Microsoft Azure portal. The URL in the address bar is [https://portal.azure.com/#blade/Microsoft\\_Azure\\_Policy/BlueprintsMenuBlade/Blueprints](https://portal.azure.com/#blade/Microsoft_Azure_Policy/BlueprintsMenuBlade/Blueprints). The page title is 'Assign blueprint'.

**Lock Assignment:**

- Don't Lock
- Do Not Delete
- Read Only

The assignment is not locked. Users, groups, and service principals with permissions can modify and delete deployed resources. [Learn more](#)

**Managed Identity:**

- System assigned
- User assigned

By clicking "Assign" with a system assigned identity, you agree to grant the Azure Blueprints service temporary Owner access to this subscription so that we can properly deploy all Artifacts. We will automatically remove this access when the blueprint assignment process is finished.

**Artifact parameters:**

Artifact / Parameter	Parameter Value
Subscription	
Resource Group	
Resource Group: Name	Set value(s) <input type="button" value="I"/>
Resource Group: Location	<input type="button" value="▼"/>
[User group or application name] : Owner	<input type="button" value="Set value(s)"/>
[User group or application name] : Owner	<input type="button" value="▼"/>
Allowed locations	

# Azure Blueprints

Blueprints | Blueprint definitions

https://portal.azure.com/#blade/Microsoft\_Azure\_Policy/BlueprintsMenuBlade/Blueprints

Microsoft Azure

Home > Blueprints | Blueprint definitions

Search (Cmd +/)

+ Create blueprint

Refresh

Scope: JAZ Lab Development Subscription

Blueprints: All

Search by blueprint name:

Name	Latest Version	Unpublished changes	Last modified	Definition location
devfinanceweb	v1.0	No	5/28/2020	JAZ Lab Development Subscription

Blueprints | Assigned blueprint

https://portal.azure.com/#blade/Microsoft\_Azure\_Policy/BlueprintsMenuBlade/BlueprintAssignments

Microsoft Azure

Home > Blueprints | Assigned blueprints

Search (Cmd +/)

Refresh

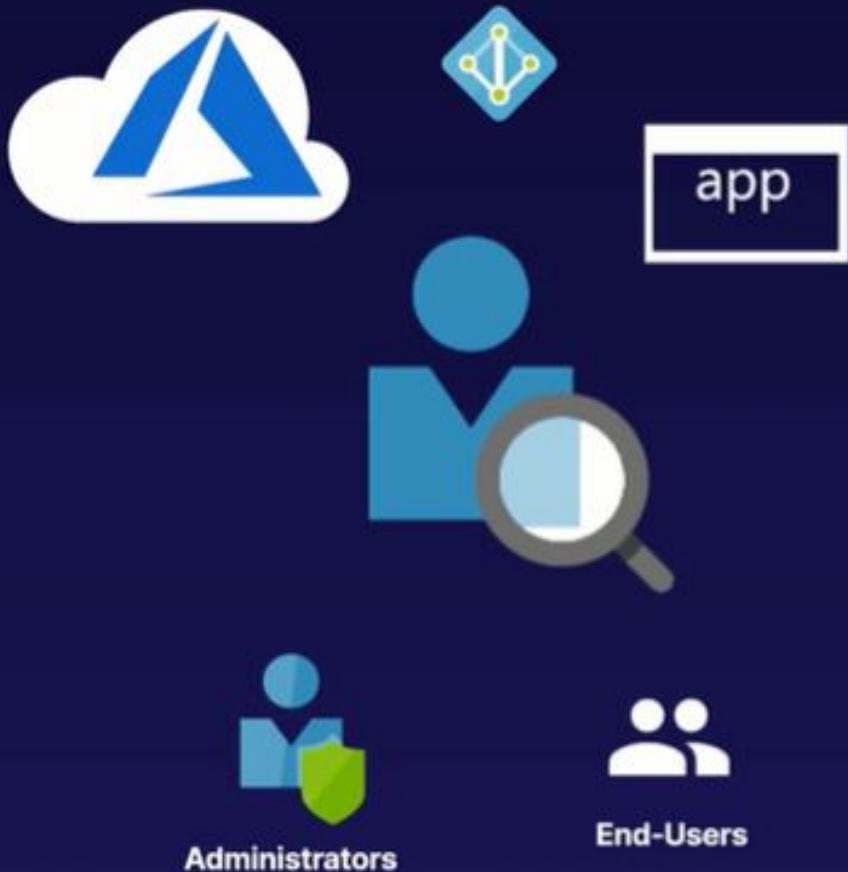
Subscriptions: All 2 selected – Don't see a subscription? Open Directory + Subscription settings

Search by subscription or blueprint

All subscriptions

Assignment name	Subscription	Blueprint	Version	Provisioning state	Date assigned
Assignment-devfinanceweb	JAZ Lab Development Subscription	devfinanceweb	v1.0	Deploying	5/28/2020

# 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



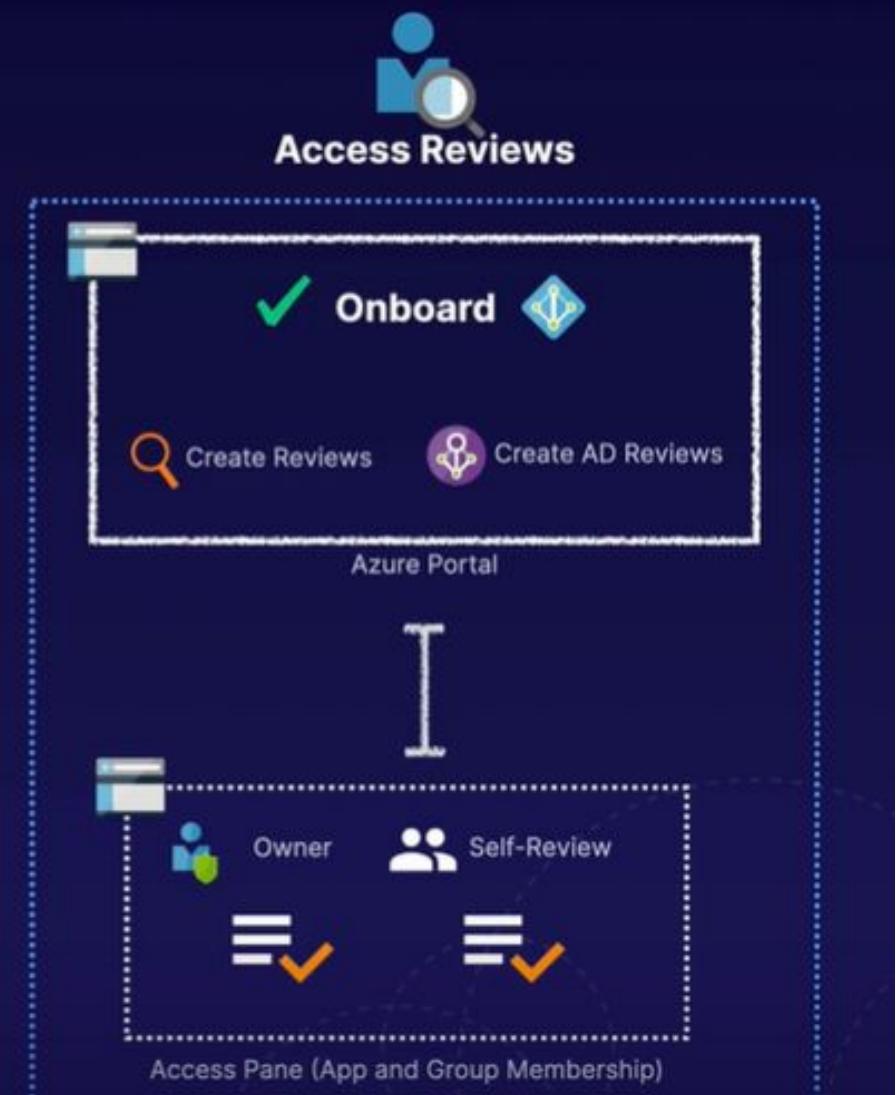
## Access Reviews

- 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

The screenshot shows the Microsoft Azure Identity Governance portal at the URL [https://portal.azure.com/#blade/Microsoft\\_AAD\\_ERM/DashboardBlade/GettingStarted](https://portal.azure.com/#blade/Microsoft_AAD_ERM/DashboardBlade/GettingStarted). The page title is "Identity Governance". The main heading is "Ensure the right people have the right access at the right time". Below it, a subtext reads "Azure AD Identity Governance helps you to protect, monitor, and audit access to critical assets while ensuring employee productivity".

The page features four main sections:

- Entitlement management:** Shows a flow from a user icon to a group icon, with the subtext "Govern the lifecycle of access to groups, applications, and SharePoint Online sites for both employees and guests." A "Create an access package" button is present.
- Access reviews:** Shows a flow from a group icon through a search icon to two user icons, one with a checkmark and one with an X. The subtext reads "Enable organizations to recertify group memberships, application access, and privileged role assignments." A "Create an access review" button is present.
- Conditional access:** Shows a flow from a user icon to a lock icon, then to another user icon with a clock icon, representing multi-factor authentication or session monitoring.
- Compliance:** Shows a flow from a user icon to a document icon, then to another user icon with a checkmark, representing audit or reporting features.

# Azure AD Access Reviews - Implementation

The screenshot shows the 'Create an access review' page in the Microsoft Azure portal. The URL is https://portal.azure.com/#blade/Microsoft\_AAD\_ERM/DashboardBlade/GettingStarted.

**Frequency:** One time

**Duration (in days):** 1

**End:** Never

**Number of times:** 0

**End date \***: 06/27/2020

**Users:**

- Users to review:** Members of a group
- Scope:** Everyone (selected)

**\*Group:** Helpdesk Admins

**Info message:** There is already an active review 'Helpdesk Review' for the Group 'Helpdesk Admins' that started on 5/28/2020 and will end on 6/27/2020. Click to view.

**Reviewers:** Group owners

**Programs:**

- Link to program
- Default Program

**Members (self):**

# Azure AD Access Reviews - Implementation

The screenshot shows the 'Create an access review' page in the Microsoft Azure portal. The URL is https://portal.azure.com/#blade/Microsoft\_AAD\_ERM/DashboardBlade/GettingStarted.

**Review Settings:**

- End:  Never  End by  Occurrences
- Number of times: 0
- End date \*: 06/27/2020

**Users:**

- Users to review: Members of a group
- Scope:  Guest users only  Everyone

**Group:**

- \*Group: Helpdesk Admins

**Information:**

There is already an active review 'Helpdesk Review' for the Group 'Helpdesk Admins' that started on 5/28/2020 and will end on 6/27/2020. Click to view.

**Reviewers:**

- Reviewers: Members (self)

**Programs:**

- Link to program: Default Program

**Upon completion settings:**

- Auto apply results to resource:  Enable  Disable
- If reviewers don't respond: Remove access

# Azure AD Access Reviews - Implementation

The image shows a two-step process for implementing Azure AD Access Reviews.

**Step 1: Sign In**  
A Microsoft sign-in window is displayed. The email address "egwene@jaz" is entered in the text field. Below the field are links for "No account? Create one!" and "Can't access your account?". At the bottom is a blue "Next" button.

**Step 2: Access Panel Applications**  
A browser window titled "Access Panel Applications" shows the URL <https://account.activedirectory.windowsazure.com/r#applications>. The page displays the Microsoft logo and a user profile for "Egwene JAZ LAB". It features a search bar labeled "Search apps" and categories for "Apps", "Add-Ins", "Groups", and "Access reviews".

# Azure AD Access Reviews - Implementation

The screenshot shows the Microsoft My Access portal. The URL in the browser is <https://myaccess.microsoft.com/@jazlab1.mail.onmicrosoft.com?enableReviews=true#/access-reviews/>. The page title is "Access reviews". On the left sidebar, under "My Account", there are links for "Access packages", "Request history", "Approvals", and "Access reviews". The "Access reviews" link is selected and highlighted in blue. The main content area displays a single review entry:

Name	Due	Resource	Progress
Helpdesk Review	Jun 27, 2020	Helpdesk Admins	0 / 1

On the right side, there is a "My Account" sidebar with the user's profile picture (EA), name (Egwene al'Vere), email (egwene@jazlab1.com), and options to "View my account", "Leave new experience", and "Sign out".

# Azure AD Access Reviews - Implementation

The screenshot shows a Microsoft Edge browser window with the URL [@jazlab1.mail.onmicrosoft.com?enableReviews=true#/access-reviews">https://myaccess.microsoft.com/@jazlab1.mail.onmicrosoft.com?enableReviews=true#/access-reviews](https://myaccess.microsoft.com). The page title is "My Access". The left sidebar has "Access reviews" selected. The main content area is titled "Helpdesk Review" and asks "Do you still need access to the group 'Helpdesk Admins'?" with "Yes" checked. A "Reason" field contains "I am still a helpdesk administrator." There are "Submit" and "Cancel" buttons.

The screenshot shows a Microsoft Edge browser window with the same URL as the previous screenshot. The page title is "My Access". The left sidebar has "Access reviews" selected. The main content area is titled "Access reviews" and shows "1 review". It lists a single review for "Helpdesk Review" due on Jun 27, 2020, for the resource "Helpdesk Admins" with progress "1 / 1". There are tabs for "Groups and Apps" and "Access packages".

Name	Due	Resource	Progress
Helpdesk Review	Jun 27, 2020	Helpdesk Admins	1 / 1

# Azure AD Access Reviews - Implementation

Helpdesk Review - Microsoft | x +

https://portal.azure.com/#blade/Microsoft\_AAD\_ERM/DashboardBlade/Controls

Microsoft Azure

Search resources, services, and docs (G+)

Home > JAZ Lab > Identity Governance | Access reviews >

## Helpdesk Review

Overview

Stop Reset Apply Delete

Owner : Admin - James Lee[adm.jlee@jazlab1.onmicrosoft.com]  
Group : Helpdesk Admins  
Access review period : 5/28/2020 - 6/27/2020  
Object Id : 0d178e96-0df1-4832-96e7-b5a09295d355

Scope : Everyone  
Review status : Active  
Selected reviewers : Members (self)  
Description :  
Recurrence type : One time

Manage

Results

Reviewers

Settings

Activity

Audit logs

Progress

The chart displays the status of 2 users. 1 user has been approved, 0 users have been denied, and 0 users are in the 'Not reviewed' state.

Status	Count
Not reviewed	1
Approved	1
Denied	0
Don't know	0

# Azure AD Access Reviews - Implementation

The screenshot shows the 'Helpdesk Review | Results' page in the Microsoft Azure portal. The left sidebar has 'Results' selected under 'Manage'. The main area displays two review items:

User	Outcome	Reason	Reviewed by	Applied by	Apply result	Recommended action
Apollo Adama lee@jazlab1.com	Not reviewed					Deny This user has not signed in during the last 30 days.
Egwene al'Vere egwene@jazlab1.com	Approved	I am still a helpdesk administrator.	Egwene al'Vere egwene@jazlab1.com			Approve This user has signed in at least once in the last 30 days.

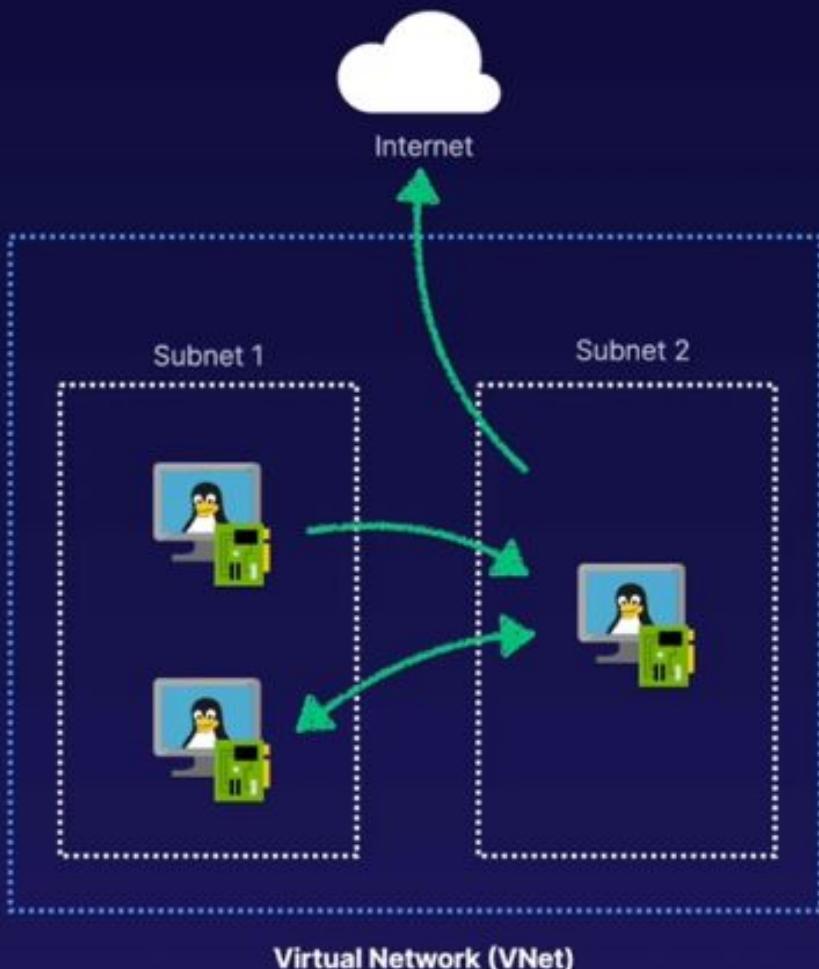
# Azure AD Access Reviews - Implementation

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the URL [https://portal.azure.com/#blade/Microsoft\\_AAD\\_IAM/ActiveDirectoryMenuBlade/Licenses](https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Licenses), a guest sign-in link, and a user account for `admjlee@jazlab1.onmicrosoft.com`. The main content area displays the 'Licenses | All products' page for the 'JAZ Lab' tenant. The left sidebar lists navigation options: Overview, Diagnose and solve problems, Manage, Licensed features, All products (which is selected), and Self-service sign up products. The right pane shows a table of assigned licenses:

Name	Assigned	Available	Expiring soon
Azure Active Directory Premium P2	99	0	0
Enterprise Mobility + Security E5	0	0	0

# **Virtual Network Security**

# Network Security Groups



## ***Control the Flow of Information Across a Virtual Network***

Network Security Groups (NSG) are used to control the flow of traffic. Specifically, this includes:

- Create rules to define what is and is not allowed
- Control security at the subnet and NIC layers
- Leverage priorities to define complex rules

# 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 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	<span style="color: green;">Allow</span>	
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	<span style="color: green;">Allow</span>	
65500	DenyAllInBound	Any	Any	Any	Any	<span style="color: red;">Deny</span>	

Outbound security rules							
Priority	Name	Port	Protocol	Source	Destination	Action	
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	<span style="color: green;">Allow</span>	
65001	AllowInternetOutBou...	Any	Any	Any	Internet	<span style="color: green;">Allow</span>	
65500	DenyAllOutBound	Any	Any	Any	Any	<span style="color: red;">Deny</span>	

# 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.



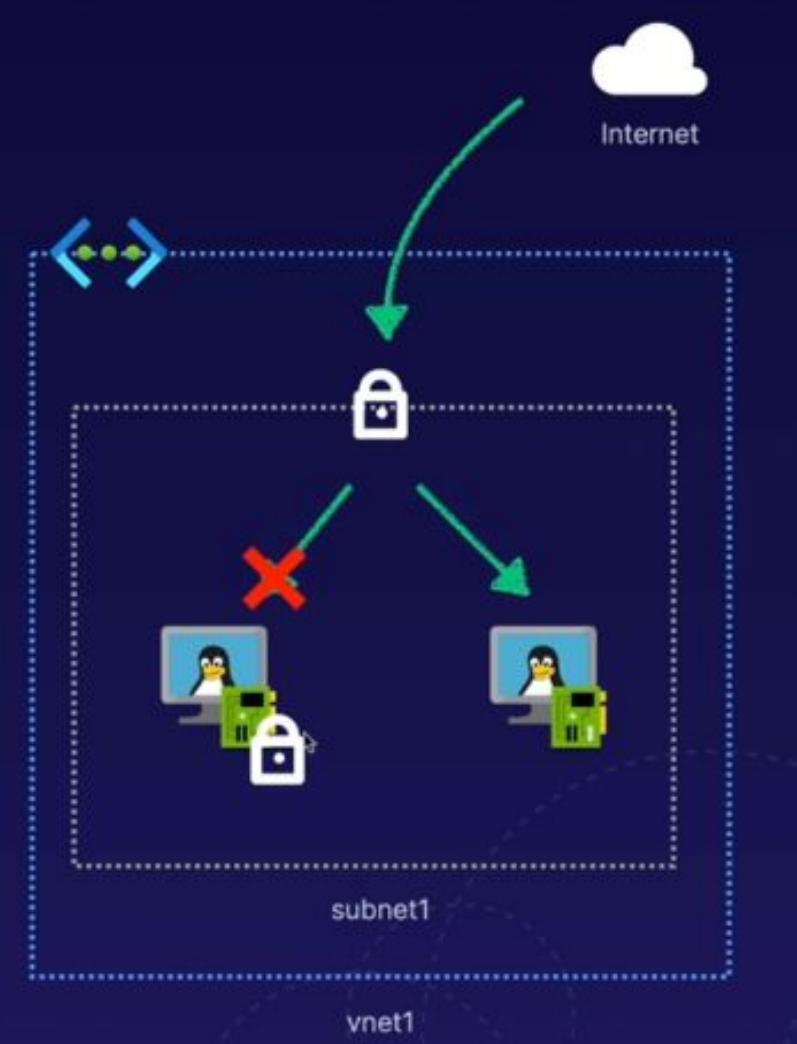
## Assign to a Subnet

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.



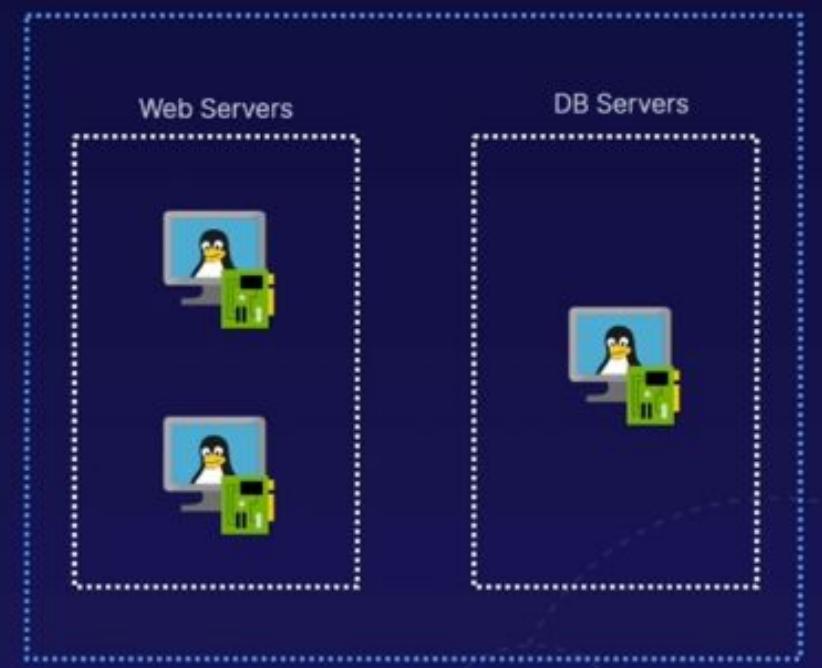
## Simplified Network Security Groups

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



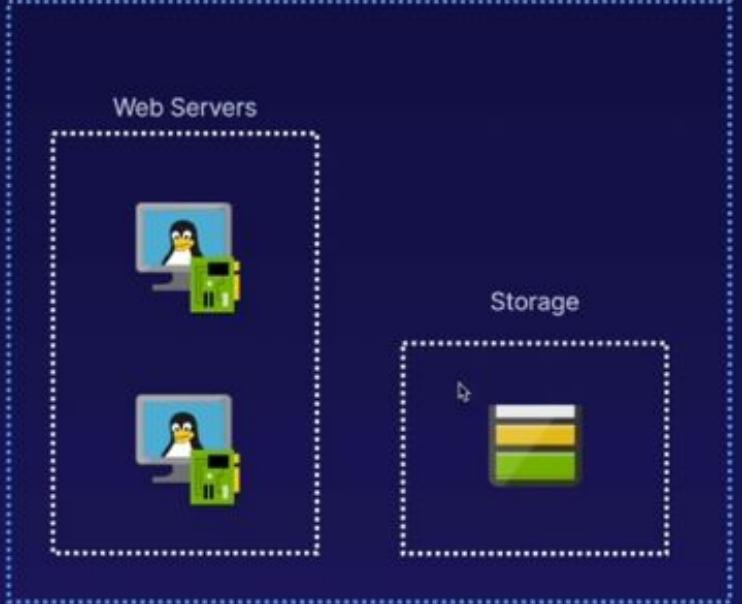
## Virtual Network (VNet) Limitation

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.



Virtual Network (VNet)

# Augmented Security Rules | Overview



**Simplified Network Security Rules**

With augmented security rules, we can more logically define security rules to match real-world solutions.

- Leverage **Service Tags** for Microsoft services that are otherwise cumbersome to configure
- Create and configure **Application Security Groups** that represent our solution network

# 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.



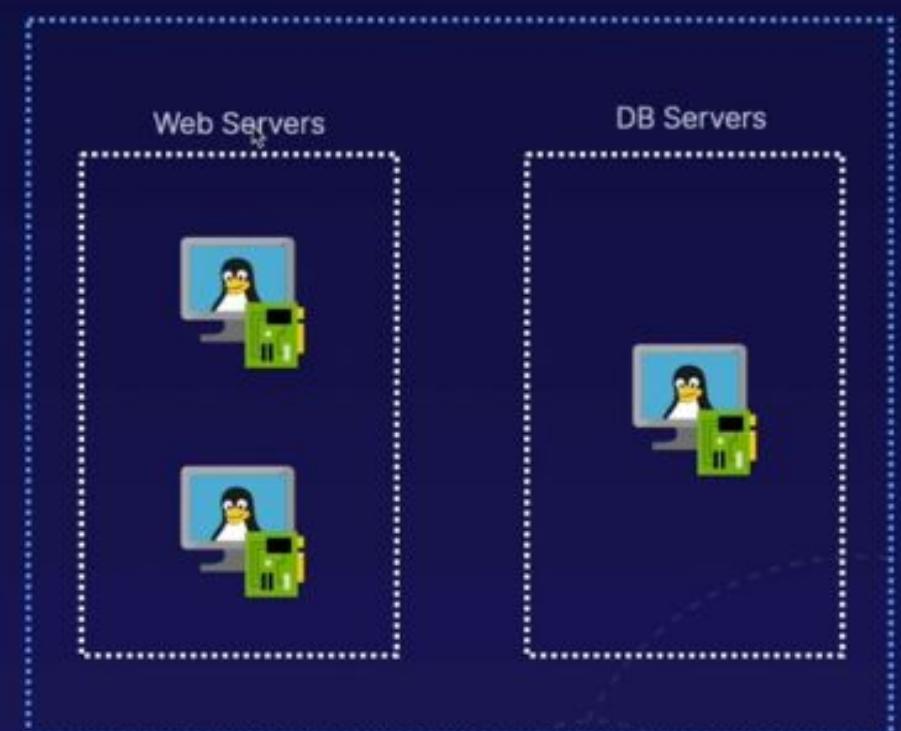
## Simplified Network Security Groups

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



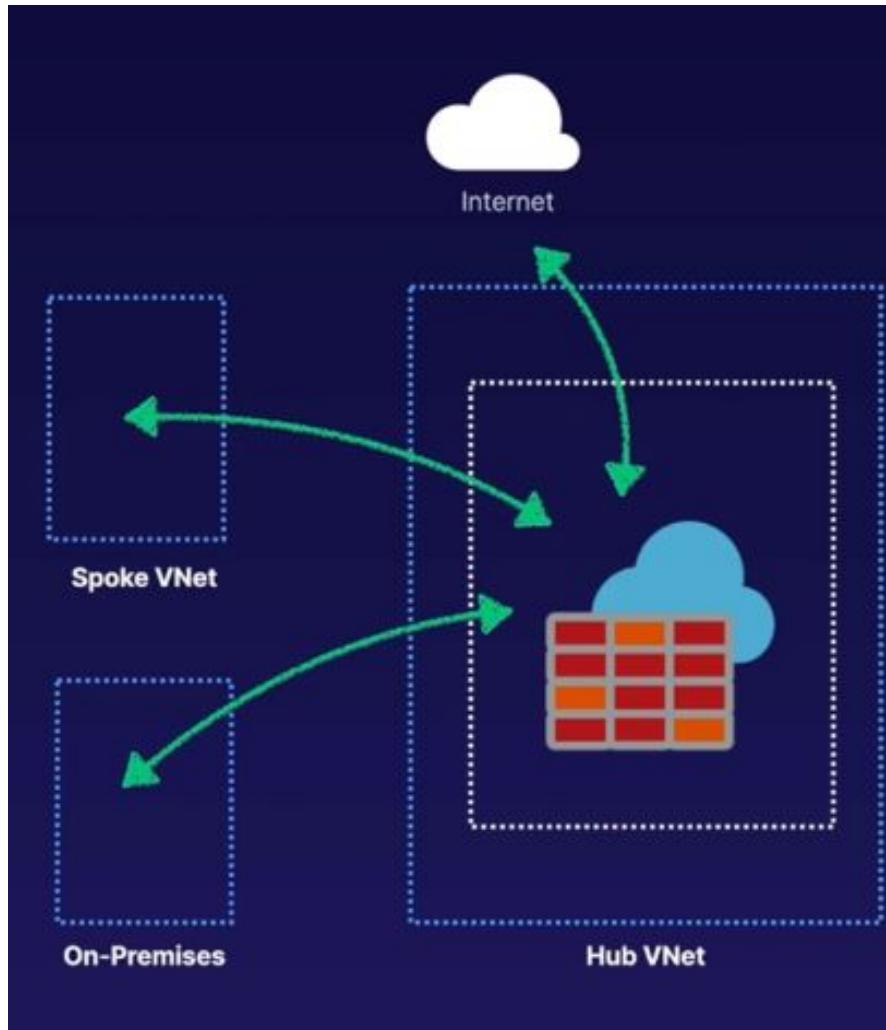
## Virtual Network (VNet) Limitation

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.



Virtual Network (VNet)

# Azure Firewall

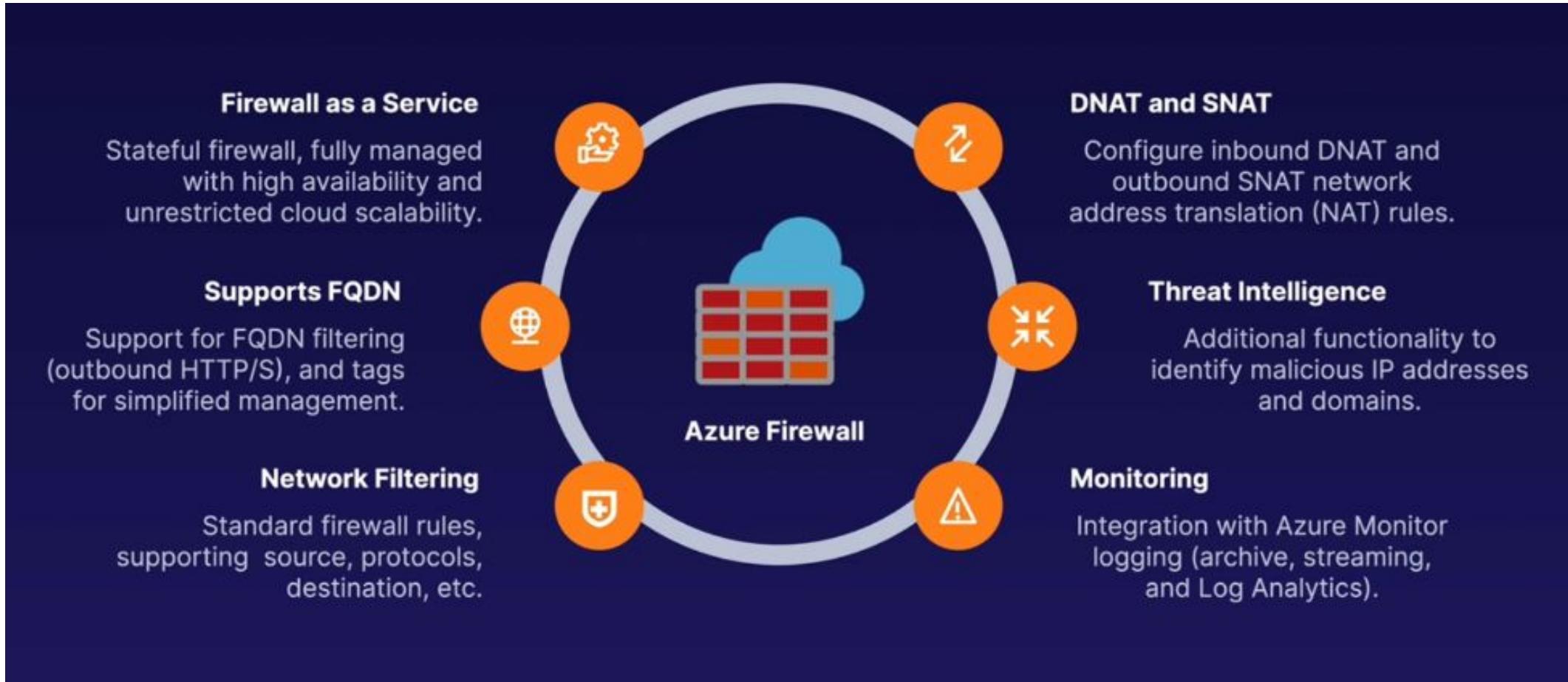


## ***Fully Managed Firewall, Purpose-Built for Azure***

With Azure Firewall, you get traditional on-premises firewall like capabilities, purpose-built for Azure.

- Fully managed including high availability and scale
- Full support for Azure (VNets, availability zones, etc.)
- Additional network security capabilities (compared to Network Security Groups) such as FQDN support

# 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

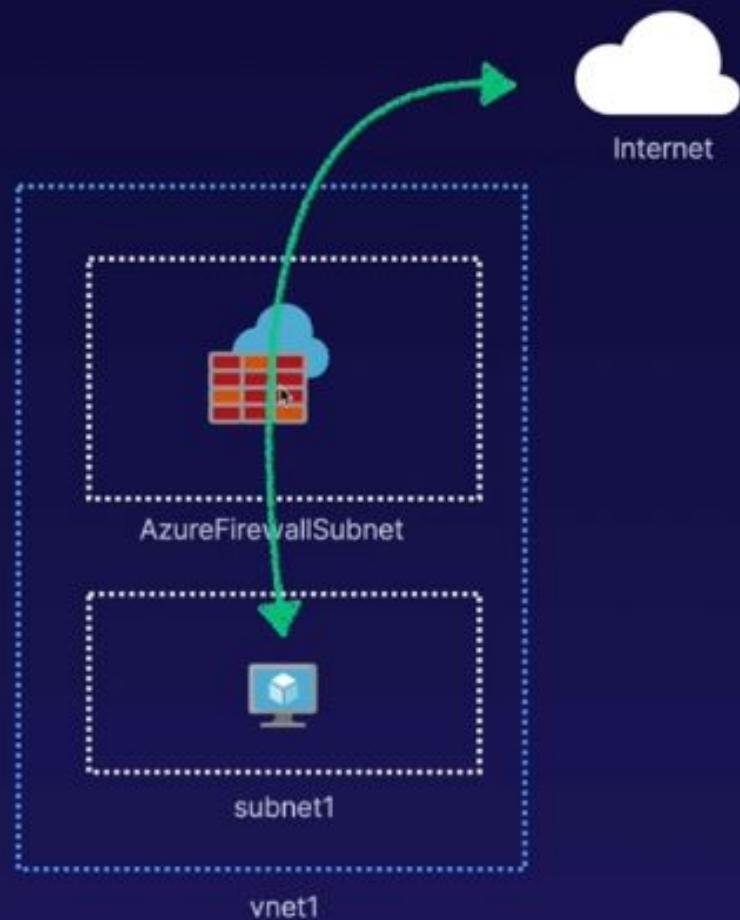
## Configure a Subnet

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

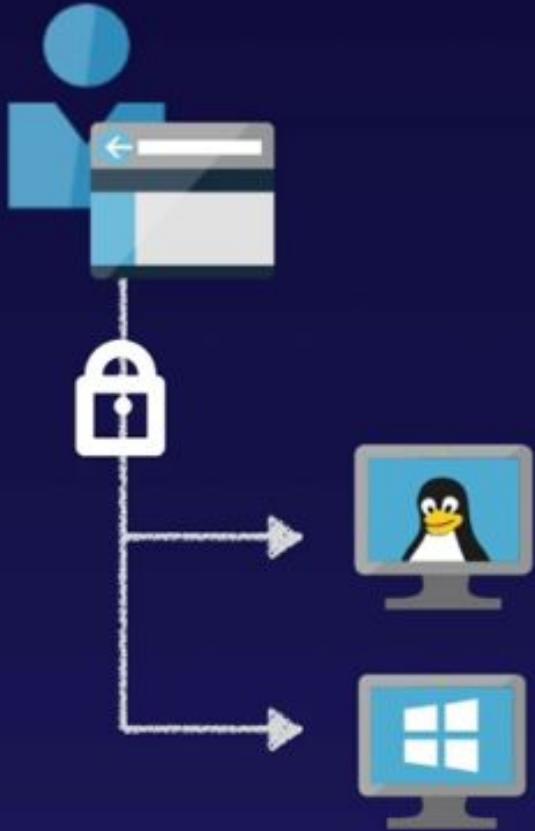
3

## Configure Routing

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



# Azure Bastion



## ***Access Your Virtual Machines via RDP or SSH over SSL***

Azure Bastion helps simplify the security and connectivity of common management protocols.

- Removes the need for a public IP address for managing your virtual machines in Azure
- Continue to use the popular RDP/SSH protocols
- Simplified deployment and security

# 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".



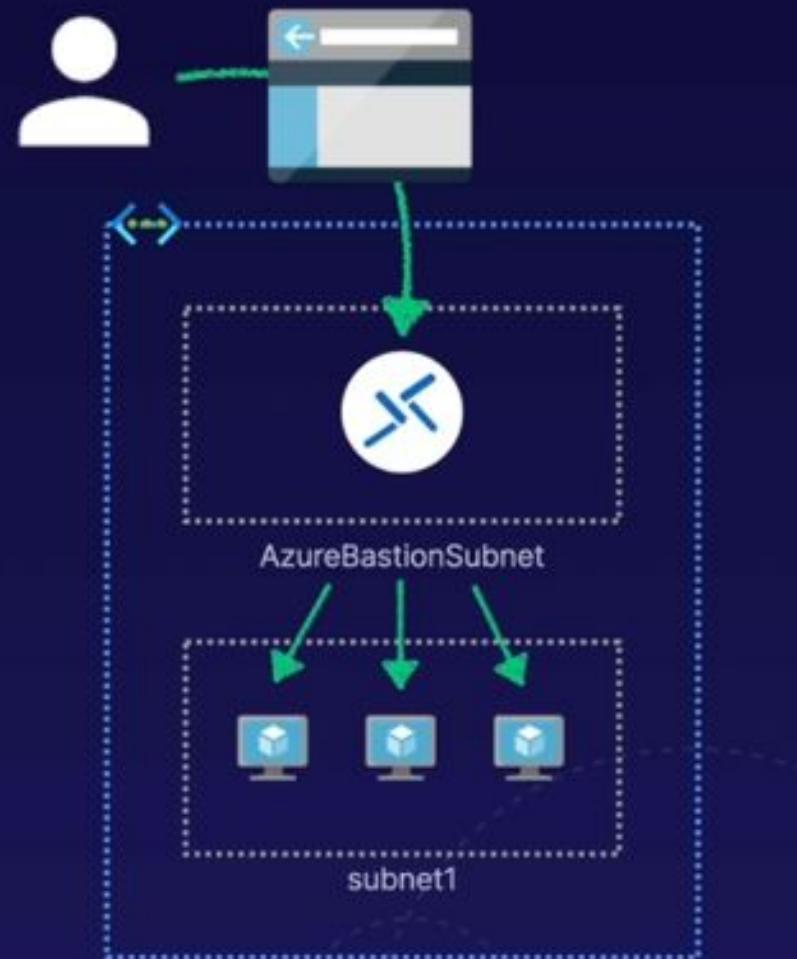
## Connect to a Virtual Machine

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

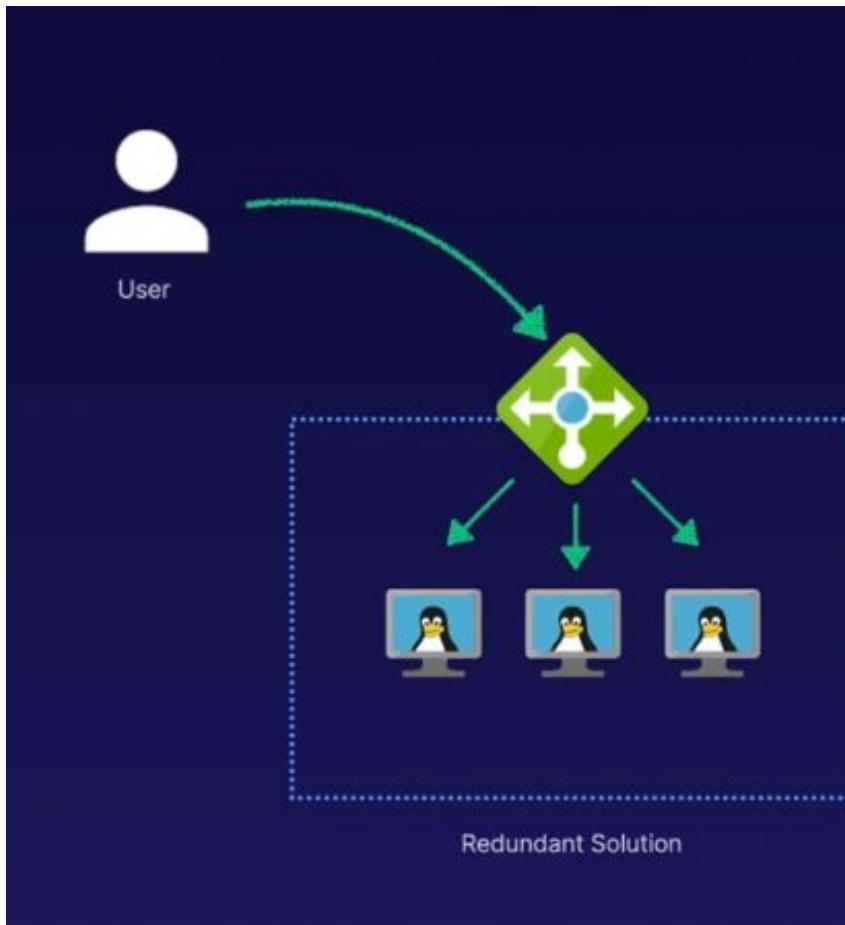


## Important Considerations

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



# Azure Load Balancer



## ***Layer 4 Traffic Distribution for Highly Available Solutions***

Traffic distribution amongst multiple redundant resources, helping to support availability and elasticity.

- Distribution of traffic at layer 4 (TCP, UDP)
- Requires redundant resources as endpoints
- Supports load-balancing capabilities such as session affinity, and health probes

# Azure Load Balancer

**Public Load Balancing**  
Load balances your solution with public accessibility (allows access from outside of Azure).

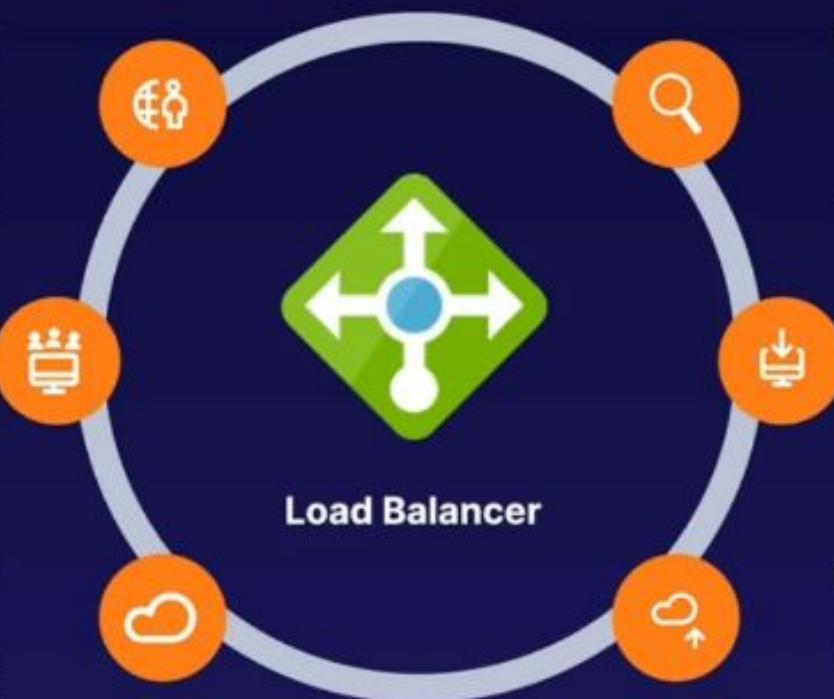
**Private Load Balancing**  
Load balances internal solutions, which do not require public accessibility.

**Availability Zones**  
Support distribution of traffic to services that exist across availability zones.

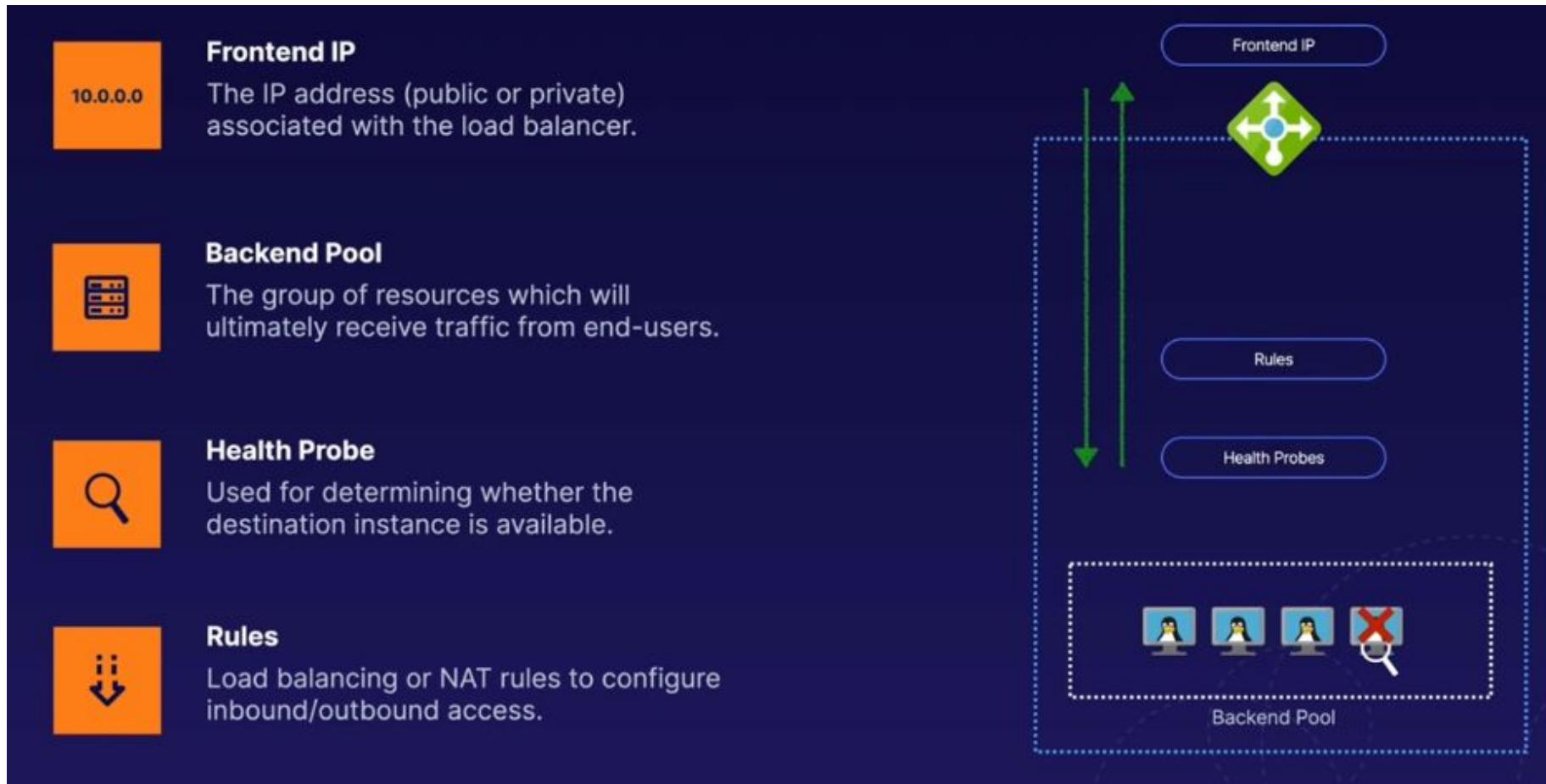
**Health Probes**  
TCP, HTTP, HTTPS probes which determine the status of resources within your solution.

**Port Forwarding**  
Configure direct, inbound access to resources that sit behind the load balancer.

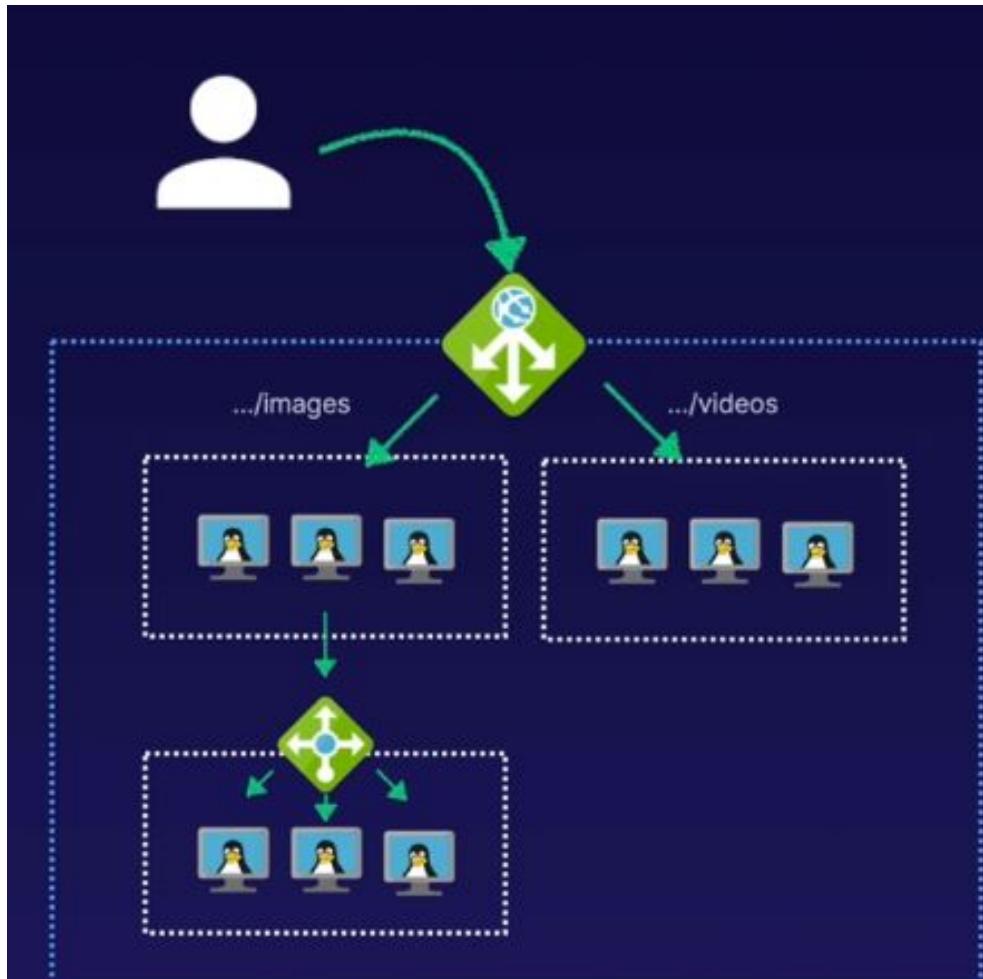
**Outbound Connectivity**  
Control outbound connectivity (SNAT) from resources within your virtual network.



# Azure Load Balancer | Key Components



# 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

**Public Load Balancing**  
Provides public access (private is partially supported), with Azure Load Balancer type functionality.

**URL Based Routing**  
Route traffic to different back-end pools, depending on the URL path requested.

**SSL Termination**  
Terminate SSL/TLS at the gateway, removing the encryption/decryption overhead from back-end servers.

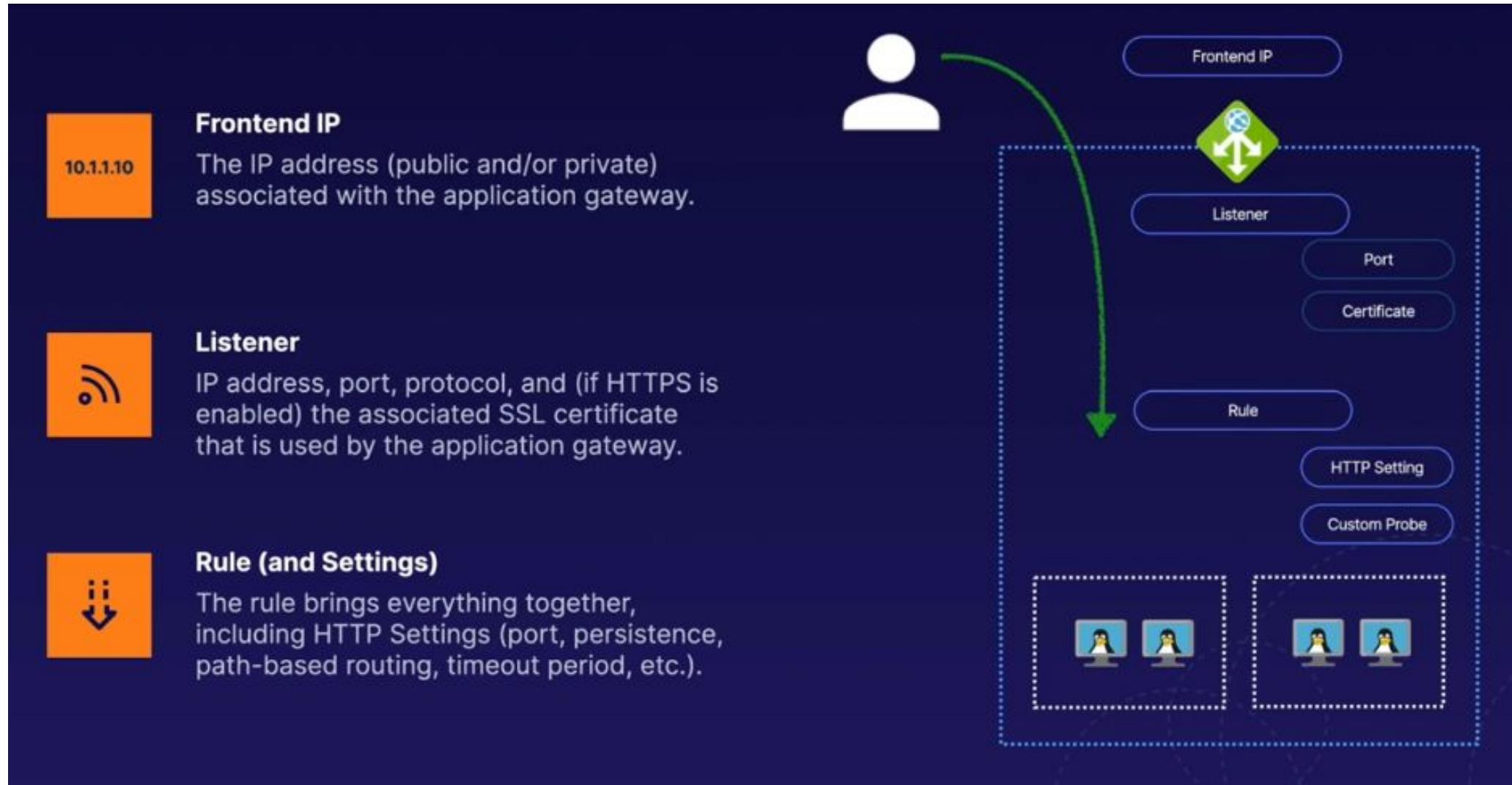


**Session Affinity**  
Gateway managed cookie-based session affinity, that keeps user sessions on the same server.

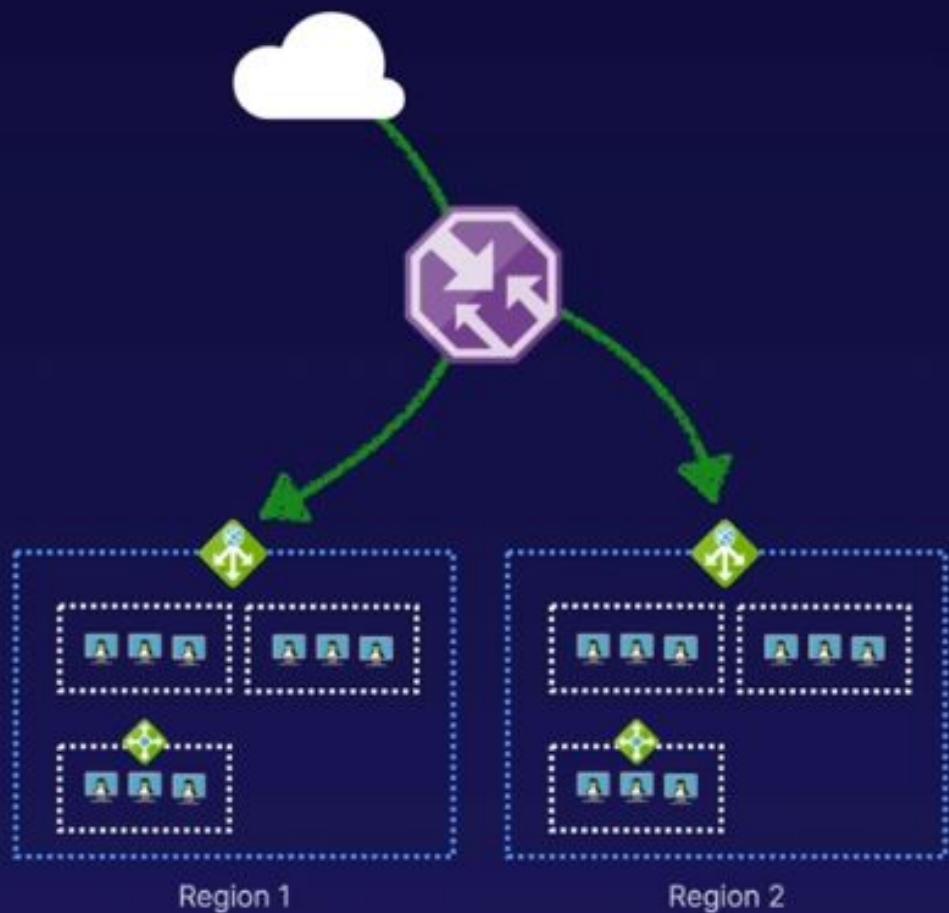
**Web Security**  
Web protection features like the Web Application Firewall, and HTTP header rewrite.

**Autoscaling**  
Scale the Application Gateway up or down, based on the demands of your users/services.

# 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.



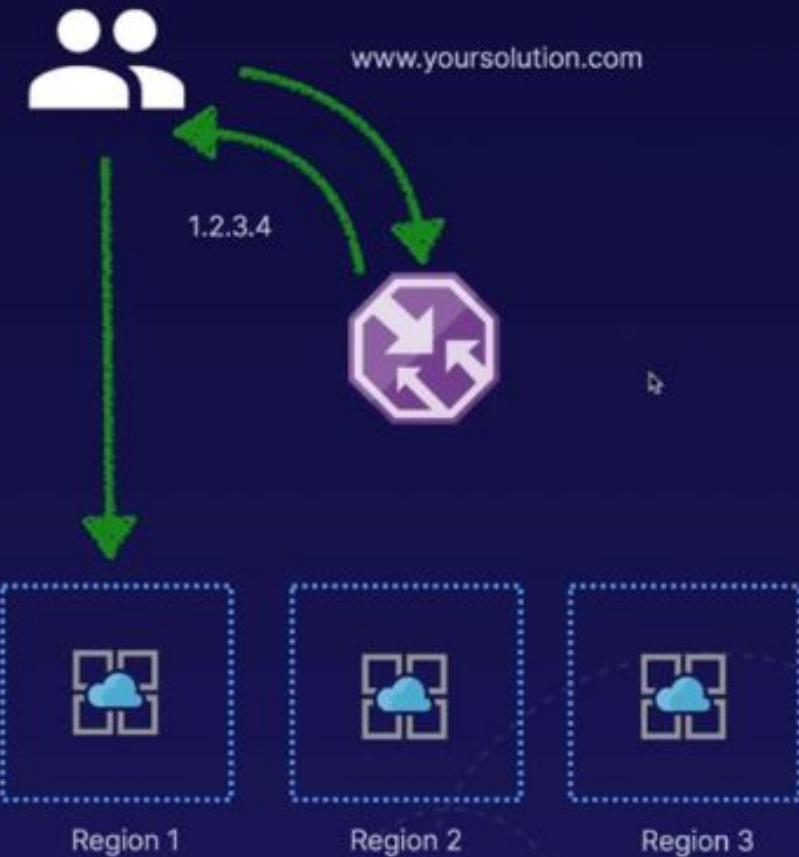
## Communication Flow

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

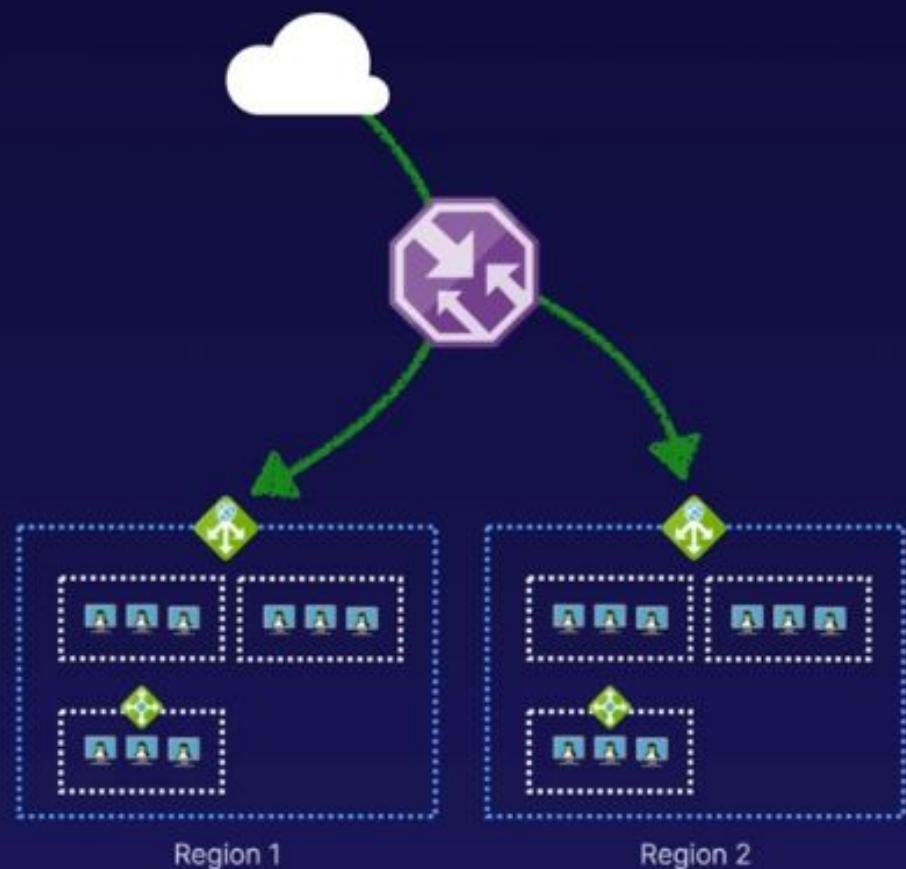


## Traffic Manager Profile

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

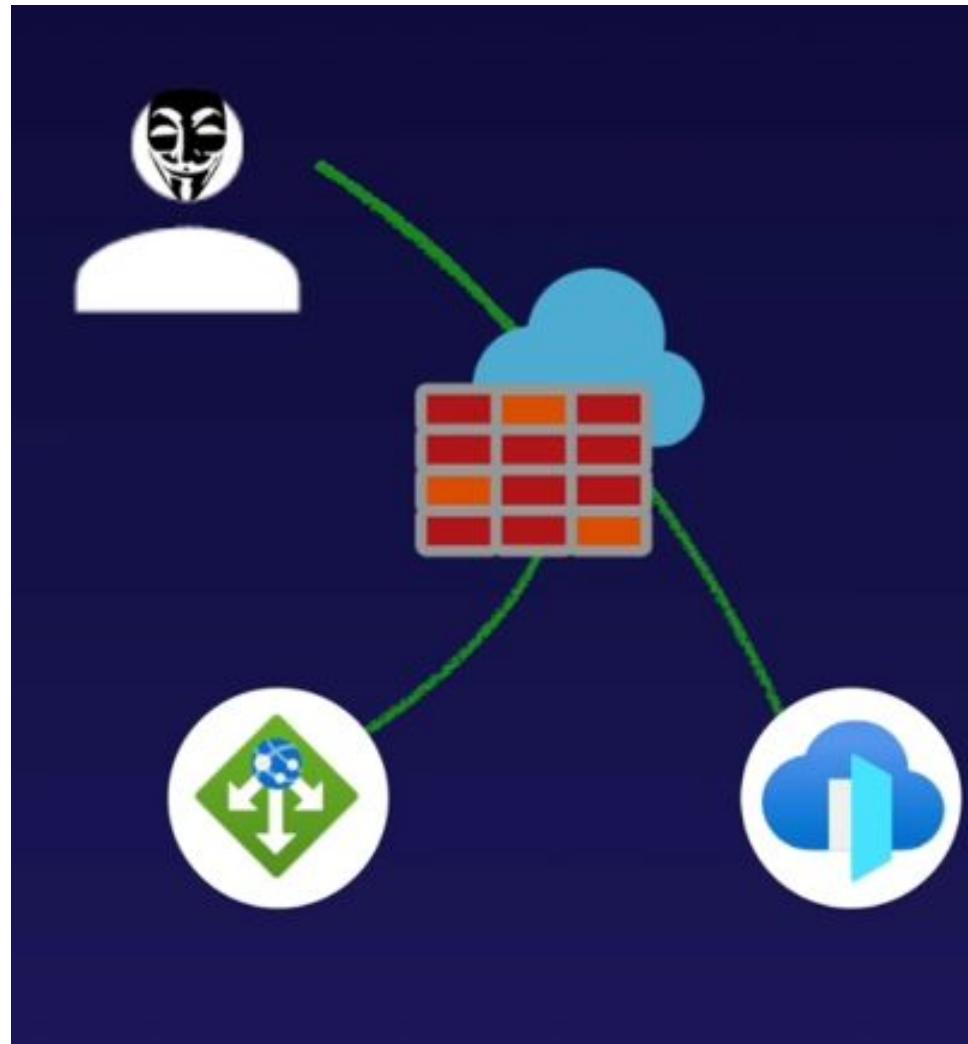


# Azure Traffic Manager | Routing Methods



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



The diagram shows a user icon (person with a mask) connected by a green arrow to a cloud icon containing a database grid. This is followed by another green arrow pointing to a cloud icon containing a blue 'I' symbol, representing the application layer.

**Protect Web Applications Against Threats and Exploits**

Microsoft provides a web application firewall (WAF) capabilities within Azure, to protect web applications:

- Protect against common threats and exploits, like SQL injection and cross-site scripting
- Managed and custom rules for controlling access
- Supported by Application Gateway and Front Door

# Web Application Firewall in Azure

## Application Gateway

- Protects your solution at the virtual network in your deployed region
- Supports Azure-managed and customer-managed rulesets
- Based on OWASP core rule set (CRS) 2.2.9, 3.0, and 3.1
- Supports custom geo-filtering rules, but rate-limiting is unavailable

## Front Door

- Protects your solution outside of your virtual network, at the edge
- Supports Azure-managed and customer-managed rulesets
- Protects against the common top OWASP vulnerabilities by default
- Supports geo-filtering and rate-limiting rules

VS

# 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.



## 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.



Services Supporting Azure AD Authentication

# 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.

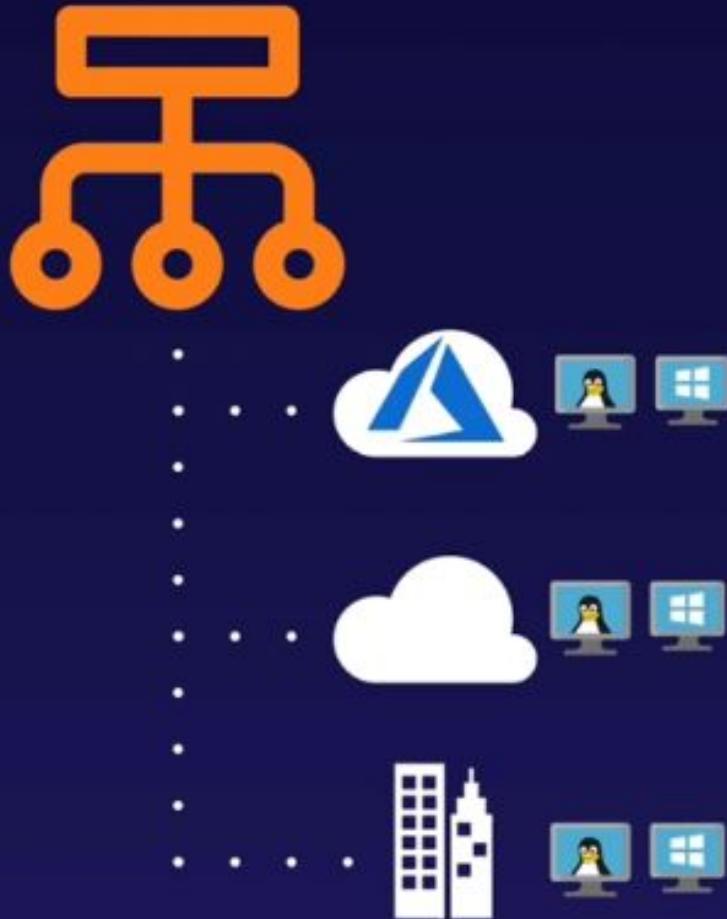


## Access Policies

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



# Azure Update Management

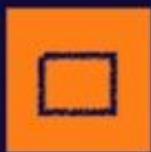


## ***Update Management for Windows and Linux***

Centralized update management, which provides the following capabilities:

- Operating system patch management, scheduling, and reporting

# 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.



## Automation Account

Hybrid Runbook Worker



## Log Analytics Workspace

Log Analytics Data



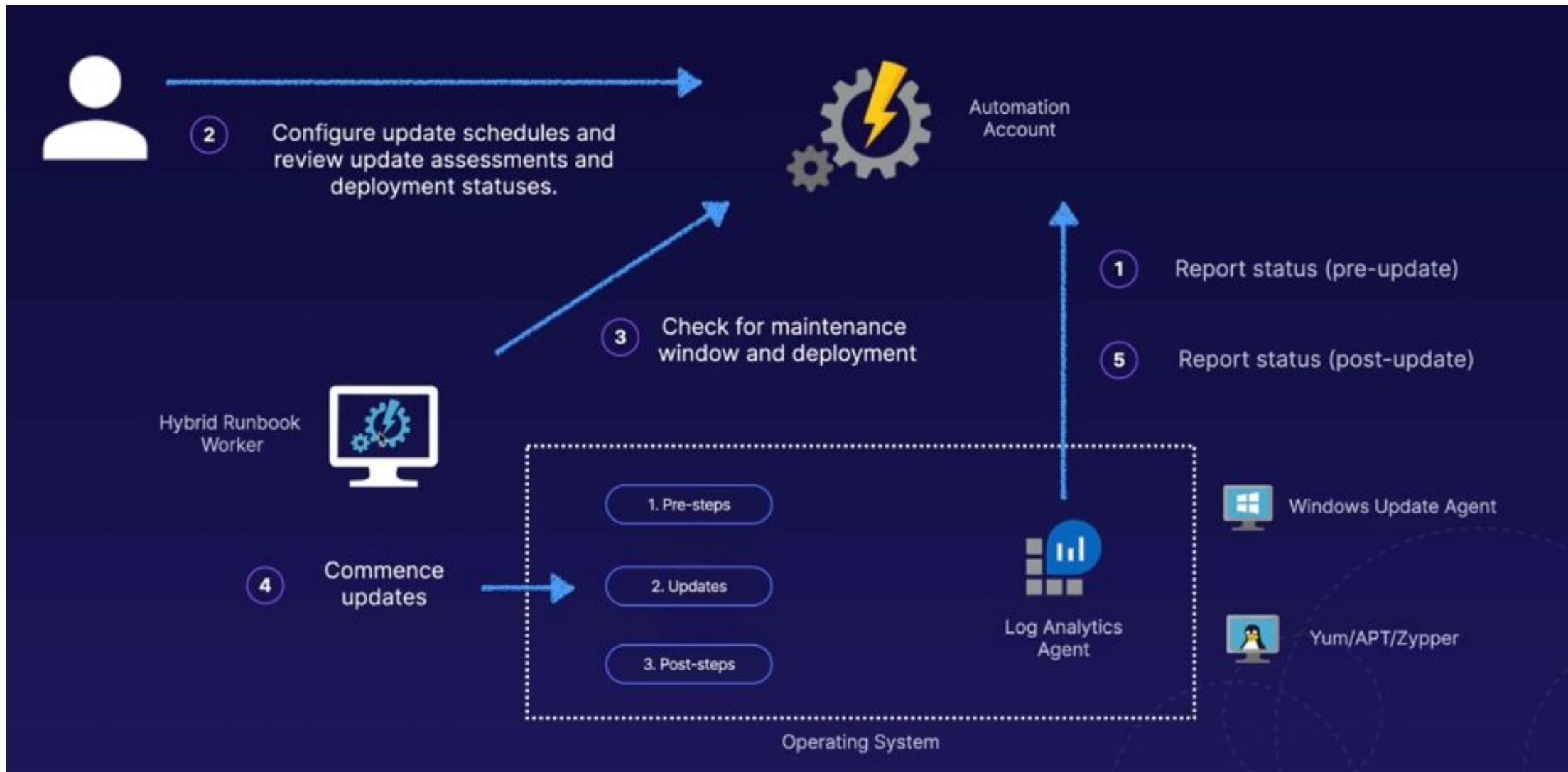
## Operating System



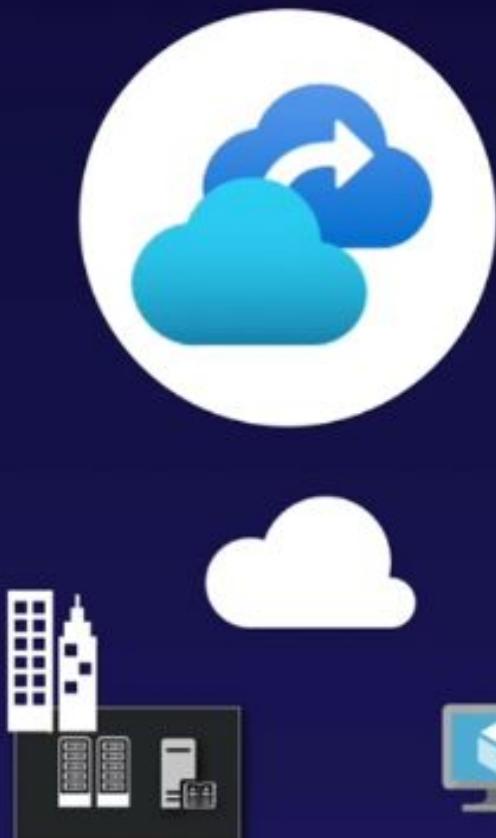
Log Analytics Agent



# Azure Update Management



# Azure Backups



## ***Backup as a Service with Support for a Variety of Workloads***

Azure Backup is a cloud-managed backup solution, which provides different tools for different scenarios.

- Backup and recovery of data
- Granular recovery levels, including files, folders, machine system state, and app-aware backups
- Support for on-premises, Azure, and other clouds

# Azure Backups



## Recovery Services Vault

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



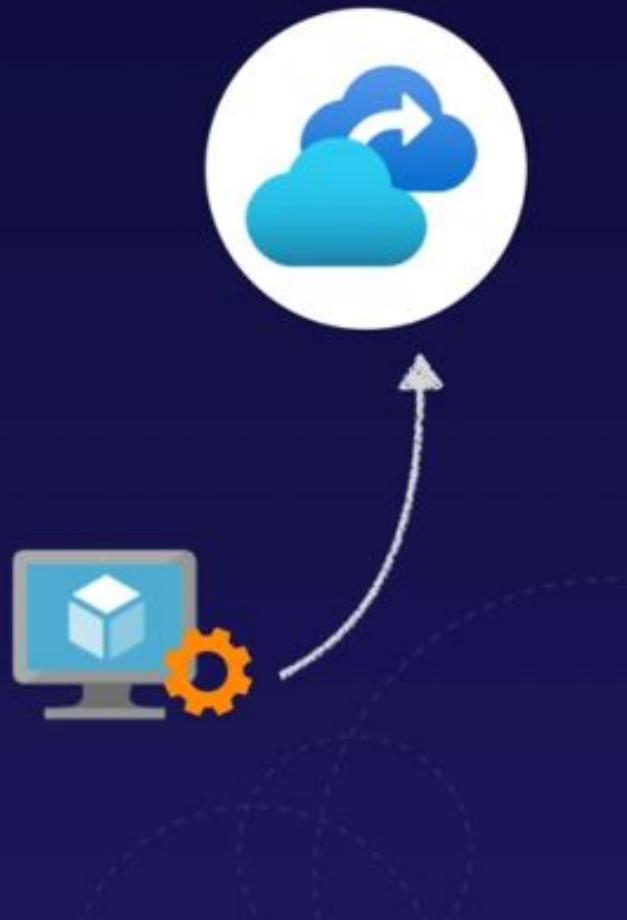
## Workload

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



## Backup Agent

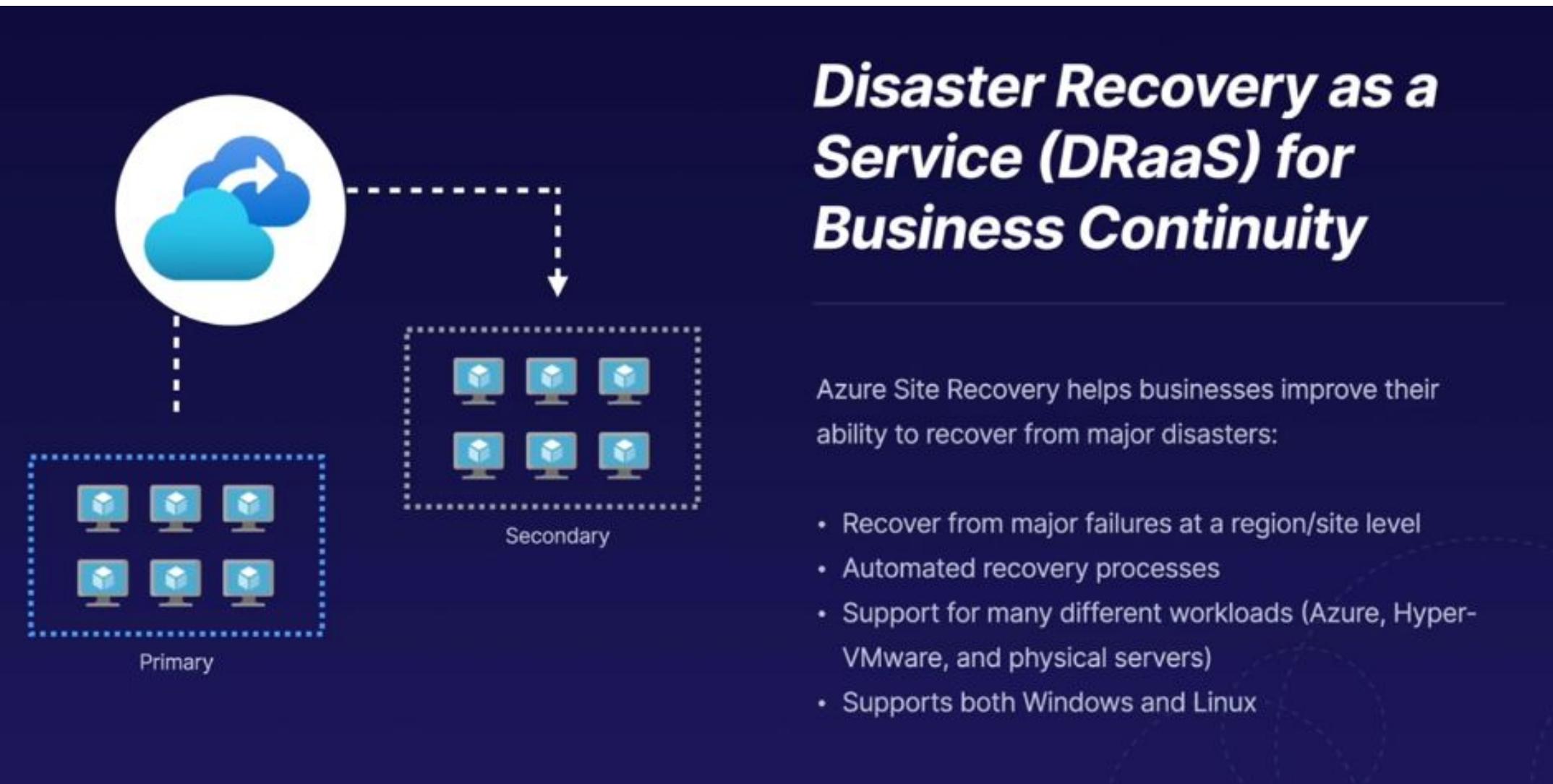
Several backup agents exist to support different backup workloads and scenarios (such as on-premises, within Azure, etc.).



# 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.	<ul style="list-style-type: none"><li>Provides file, folder, and system-state backups for Windows only</li><li>Backs up three times a day</li><li>Restores files to a server</li></ul>
Microsoft Azure Backup Server (MABS)	Backup suite which integrates with Azure backup to support traditional backups.	<ul style="list-style-type: none"><li>Provides file, folder, volume, application, and system state backup</li><li>Protects both Windows and Linux</li><li>Customizable backup frequency</li></ul>
Azure Virtual Machine Backup Extension	Leverages a virtual machine extension to backup a virtual machine within Azure.	<ul style="list-style-type: none"><li>Supports virtual machine-level backups of Windows and Linux</li><li>Only Windows backups are application-consistent</li><li>Backs up once per day</li><li>Restores virtual machines, disks, and files</li></ul>
Microsoft Data Protection Manager (DPM)	Traditional on-premises Microsoft backup solution.	<ul style="list-style-type: none"><li>Used for on-premises backups, but can also integrate with Azure Backup</li><li>Supports tape</li></ul>

# Azure Site Recovery



# Azure Site Recovery



## Replicated Items

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



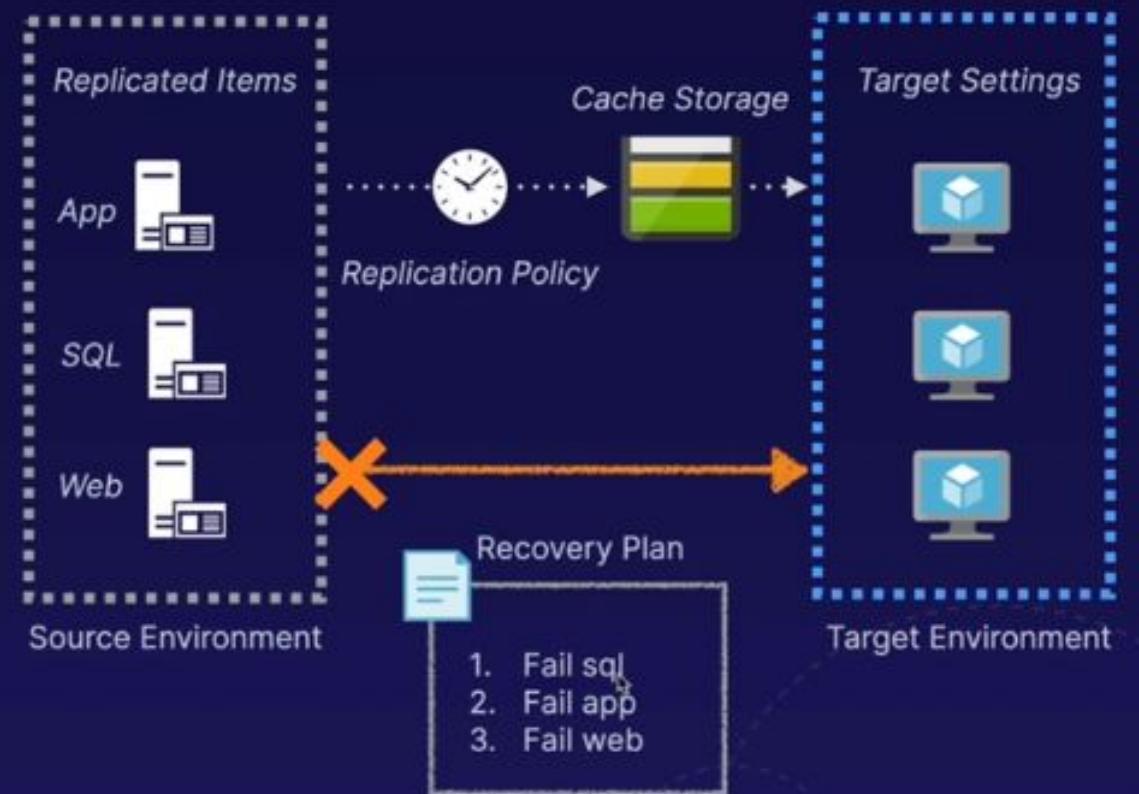
## Replication Policies

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

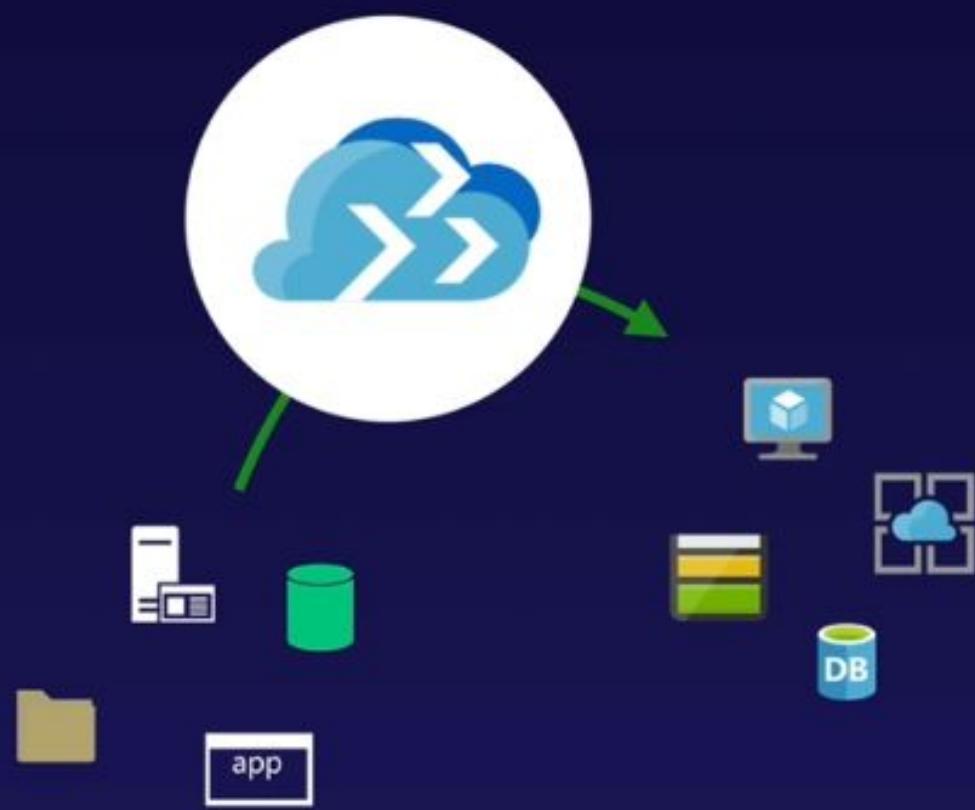


## Recovery Plans

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



# Azure Migrate

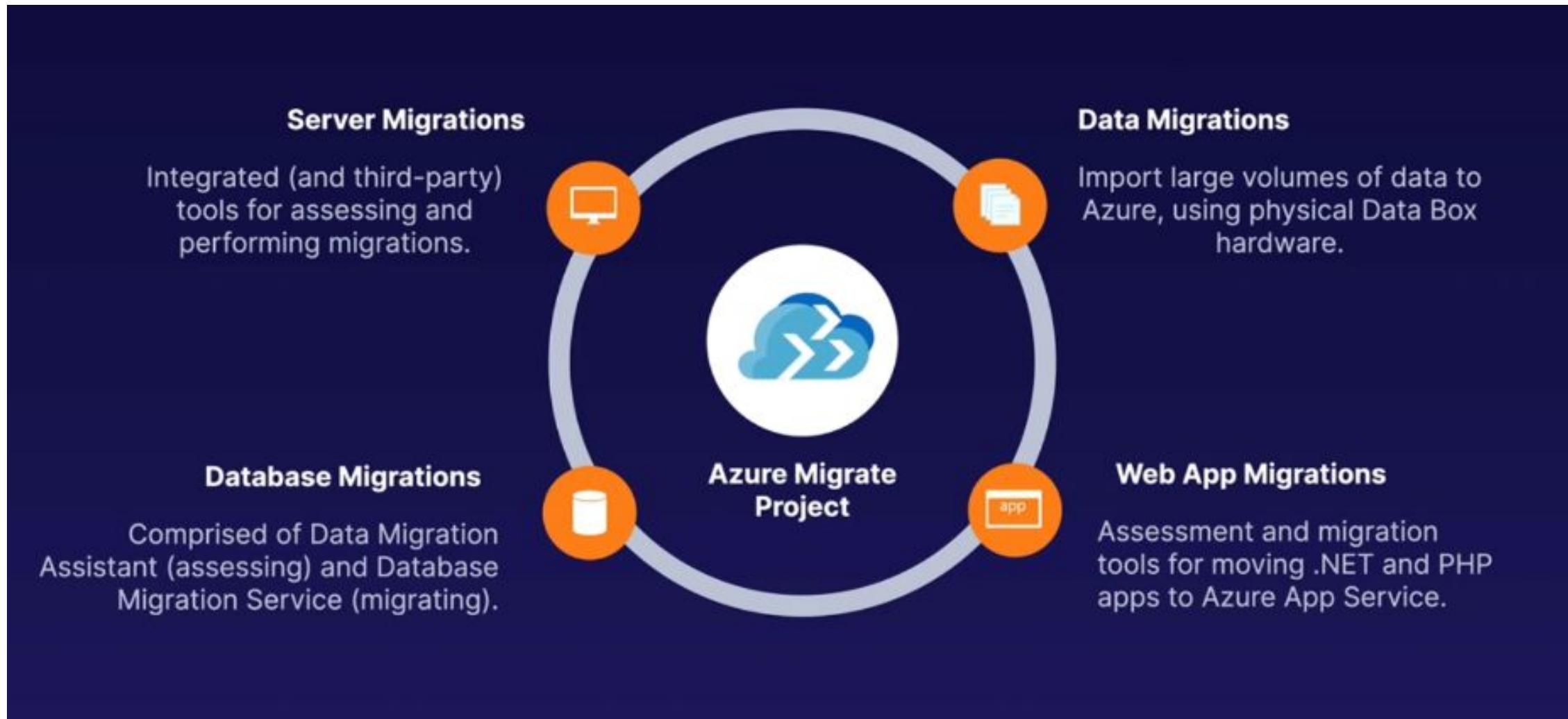


## ***Unified management planning and performing migrations***

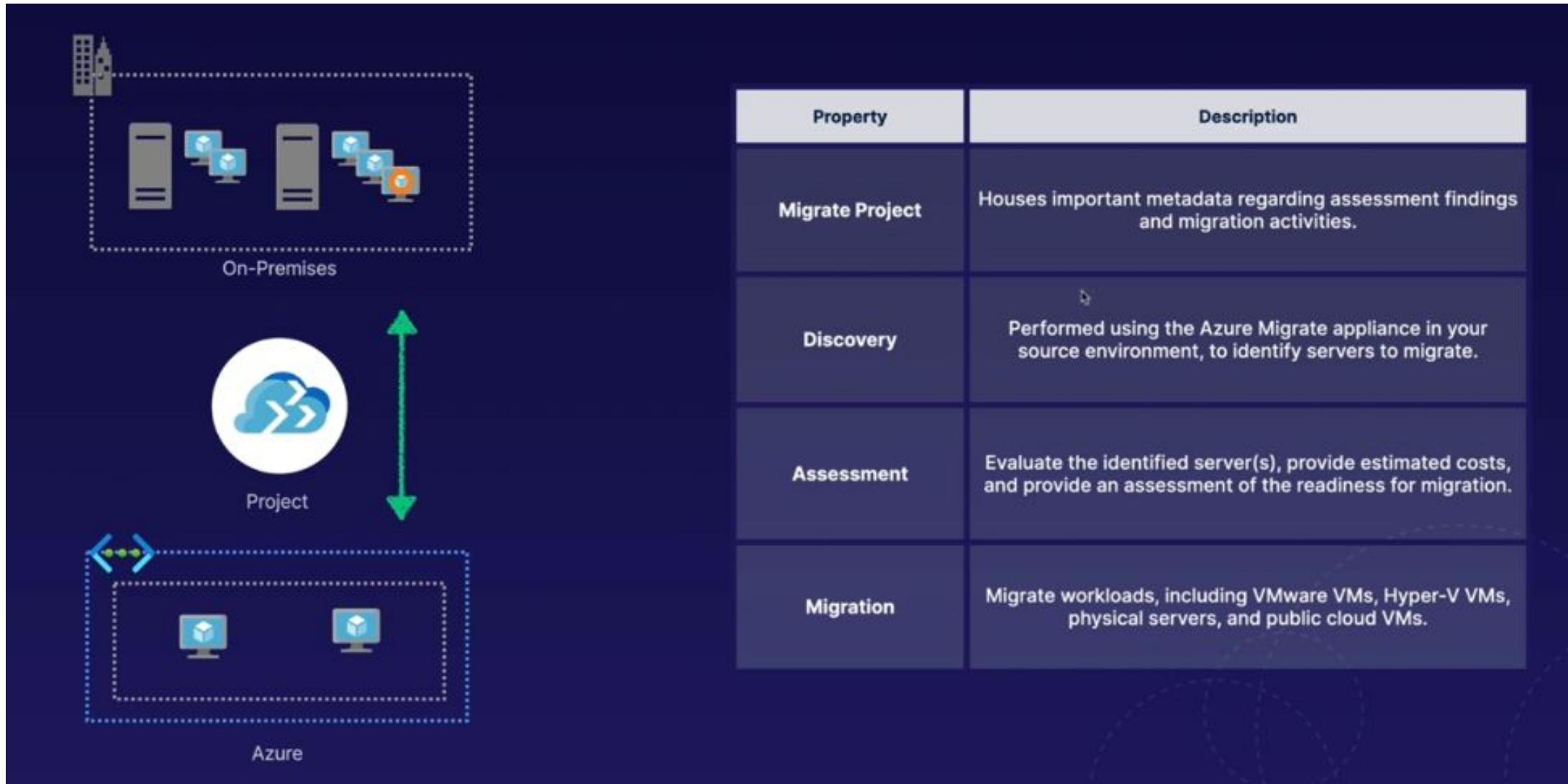
Azure Migrate is a service which provides both Microsoft and third-party migration tools.

- Server migrations (Hyper-V, VMware, physical)
- Database migrations (Database Migration Service)
- Application and data migrations
- Assessment and migration tools

# Azure Migrate



# Azure Migrate For Servers



# Azure Migrate For Databases

The diagram illustrates the Azure Migrate For Databases process flow. It starts with two green cylinder icons labeled "Database Migration Assessment". A green arrow points from these icons to a white circle containing a blue cloud icon with a double-headed arrow, labeled "Project". From the "Project" circle, a green arrow points down to another white circle containing a blue cloud icon with an upward arrow, labeled "Database Migration Service". A green arrow points from this "Database Migration Service" circle down to two blue cylinder icons labeled "DB".

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!**

