Module 04: PART 1

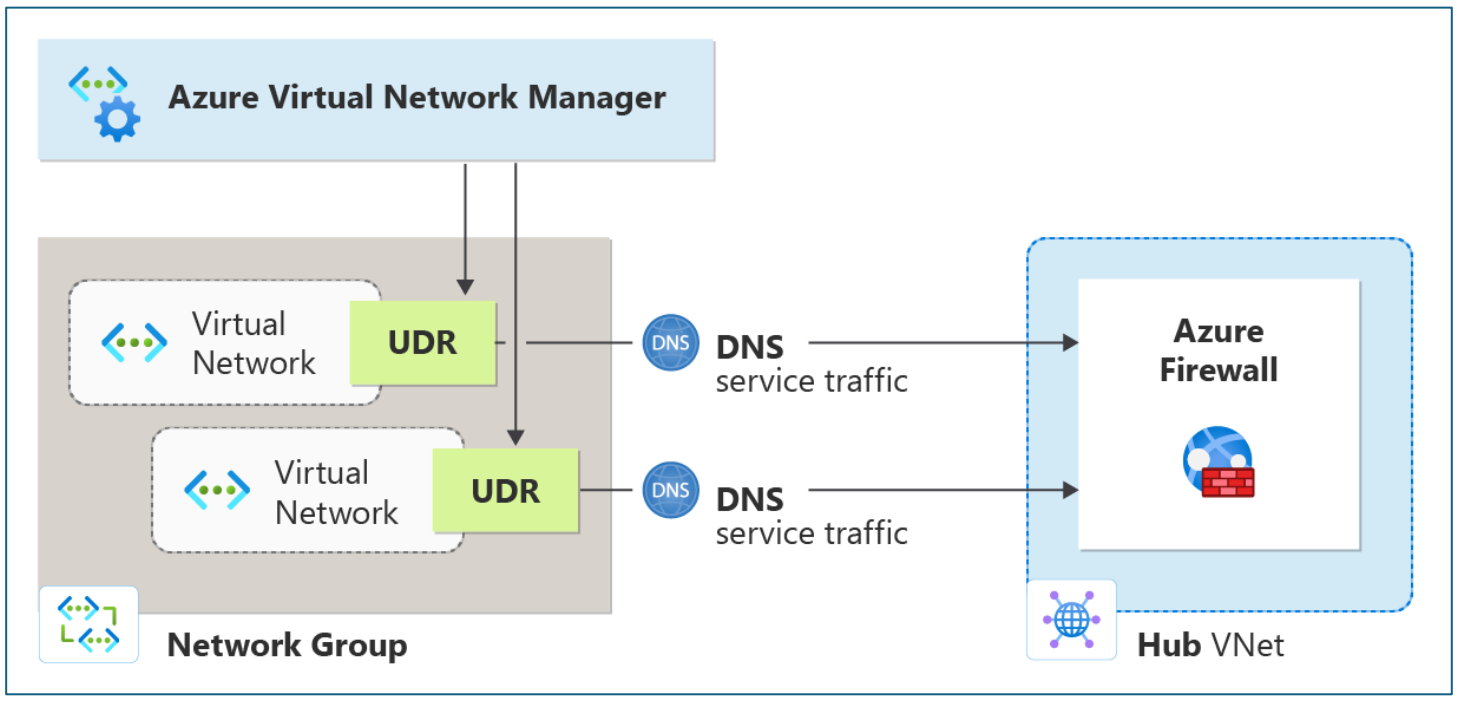
1. Azure Security Features

What is Azure Security Features?

- Azure Security features
- Security Center and resource hygiene
- Key Vault, Sentinel, and Dedicated Hosts
- Azure network security
- Defense in depth
- Network Security Groups and Firewalls

1. What is UDR management?

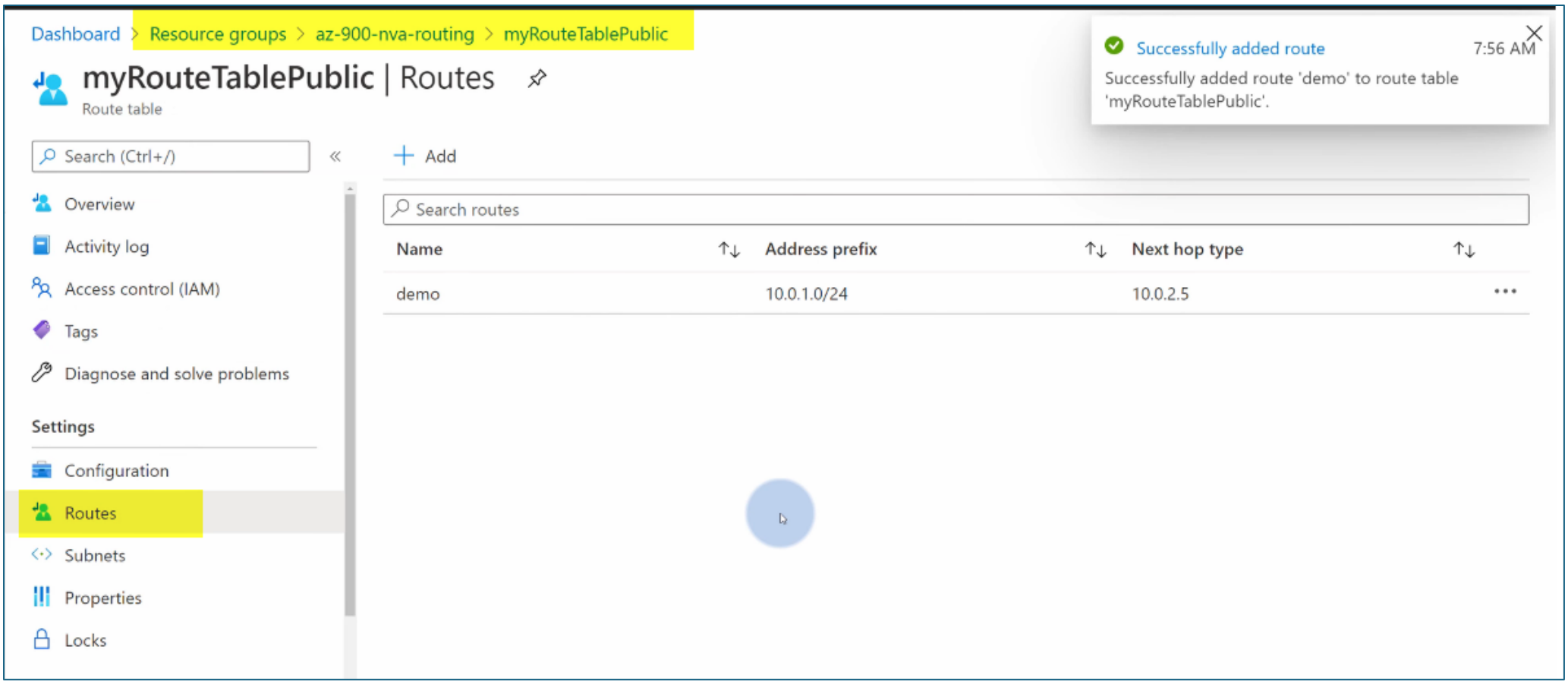
- Azure Virtual Network Manager (AVNM) allows you to describe your desired routing behavior and orchestrate user-defined routes (UDRs) to create and maintain the desired routing behavior.
- User-defined routes address the need for automation and simplification in managing routing behaviors.
- Currently, you'd manually create User-Defined Routes (UDRs) or utilize custom scripts



A. Routing: Process of finding/selecting a path for traffic in one or across multiple networks.

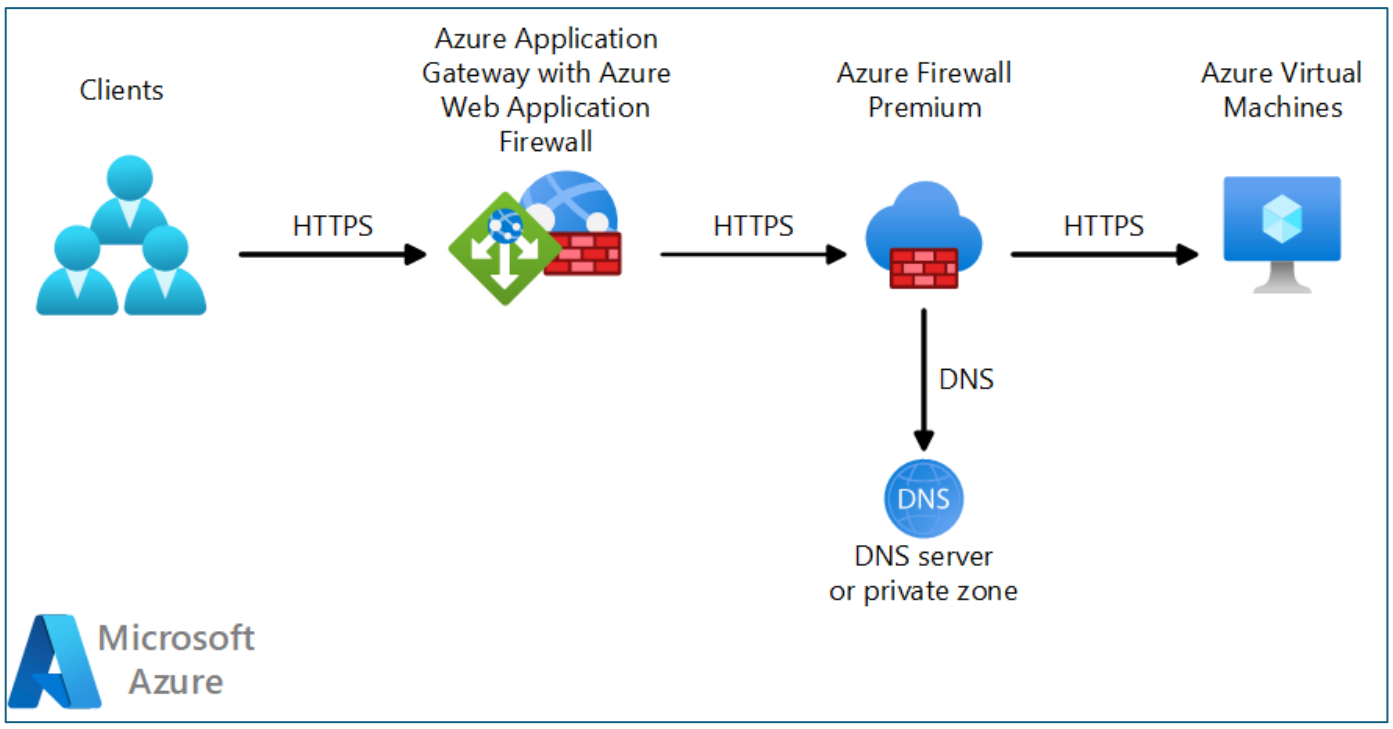
B. User-defined Routes

- Custom (user-defined, static) routes (UDRs)
- Designed to override Azure's default routing or add new routes
- Managed via Azure Route Table resource
- Associated with a zero or more Virtual Network subnets



https://learn.microsoft.com/en-us/azure/virtual-network-manager/concept-user-defined-route

2. Azure Firewall Protection:

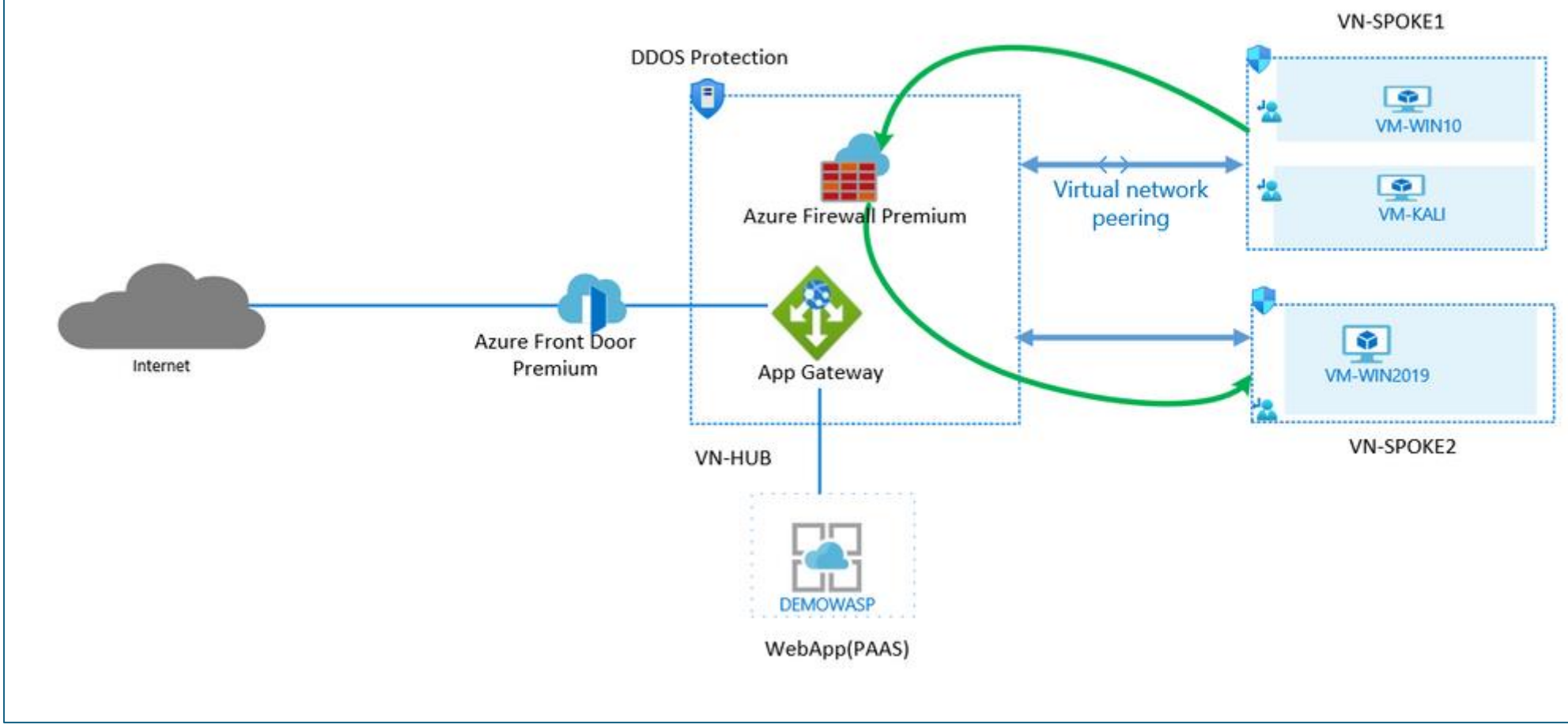


Firewall

A. Firewall is a network security service that monitors and controls incoming and outgoing traffic.

B. Azure Firewall

- Managed, cloud-based firewall service (PaaS, Firewall as a Service)
- Built-in high availability
- Highly Scalable
- Inbound & outbound traffic filtering rules
- Support for FQDN (Fully Qualified Domain Name), ex. microsoft.com
- Fully integrated with Azure monitor for logging and analytics



https://learn.microsoft.com/en-us/azure/firewall/overview

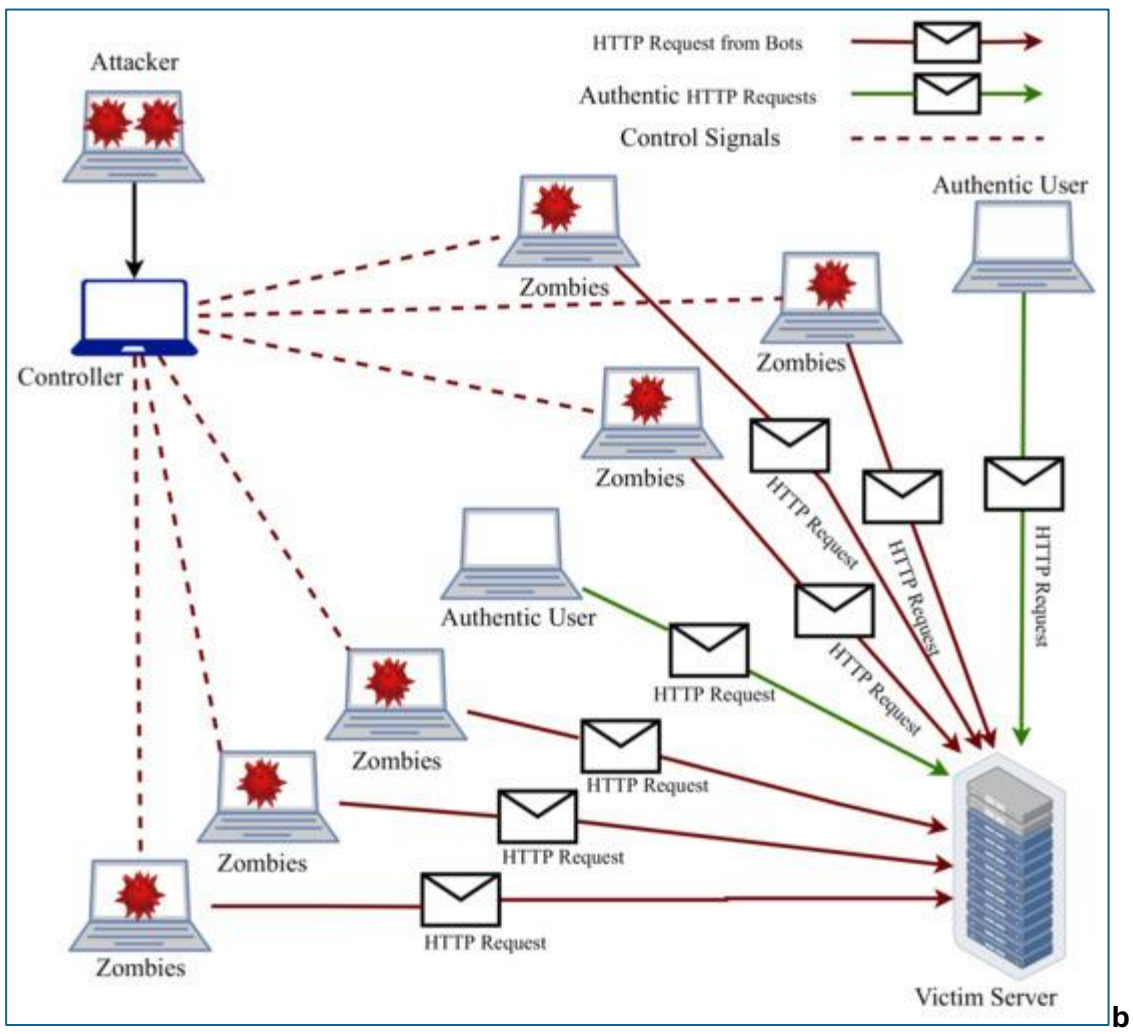
3. DDoS protection:

A. DoS - Denial of Service

Cyber-attack with intent to cause temporary or indefinite disruption of service

B. DDoS - Distributed Denial of Service

DoS attack that is originating from multiple servers

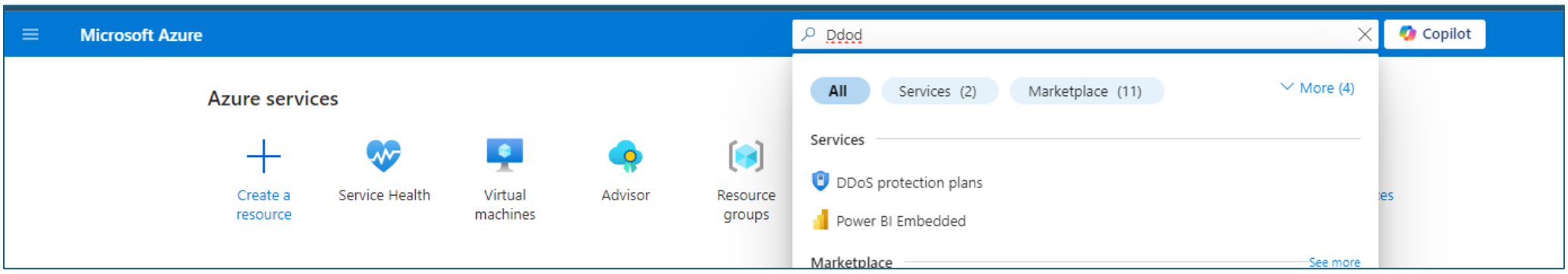


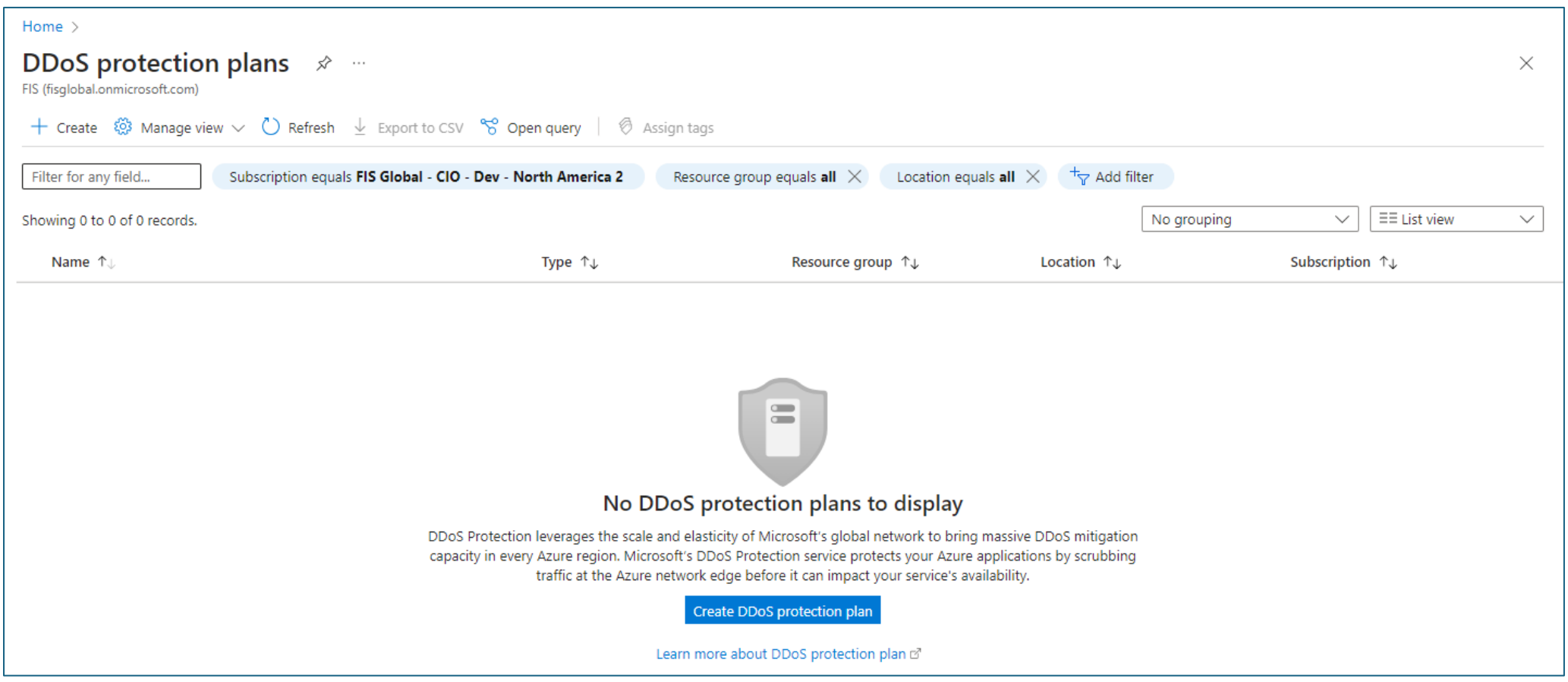
b

C. Azure DDoS Protection

- DDoS protection service in Azure
- Designed to
  - Detect malicious traffic and block it while allowing legitimate users to connect
  - Prevent additional costs for auto-scaling environments

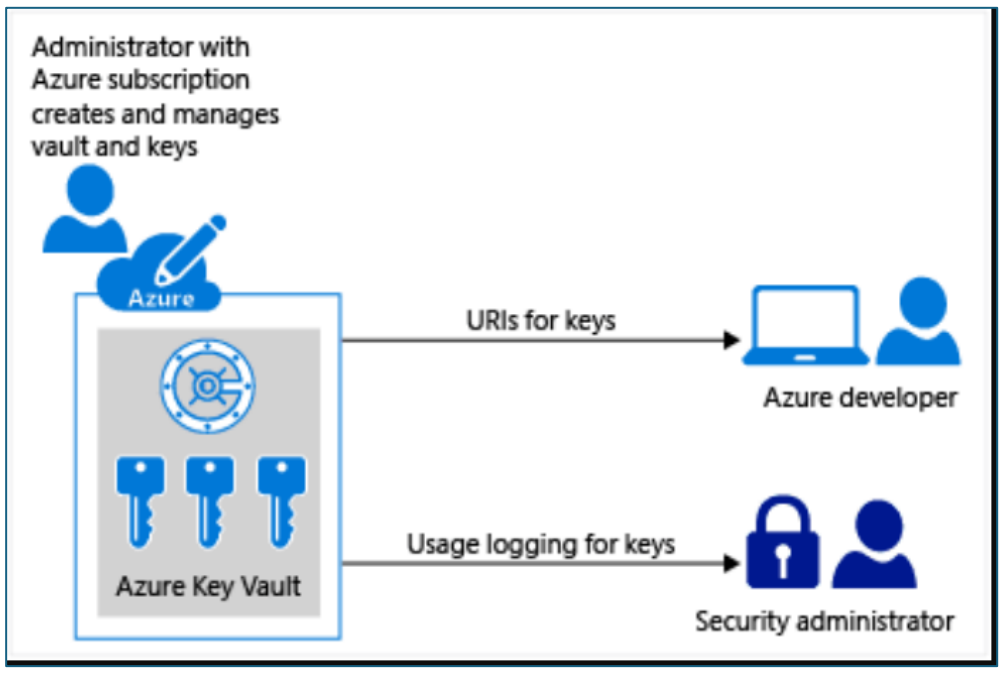
- Two tiers
    - **Basic** – automatically enabled for Azure platform
    - **Standard** – additional mitigation & monitoring capabilities for Azure Virtual Network resources
- Standard tier uses machine learning to **analyze traffic patterns** for better accuracy





4. Azure Key Vault

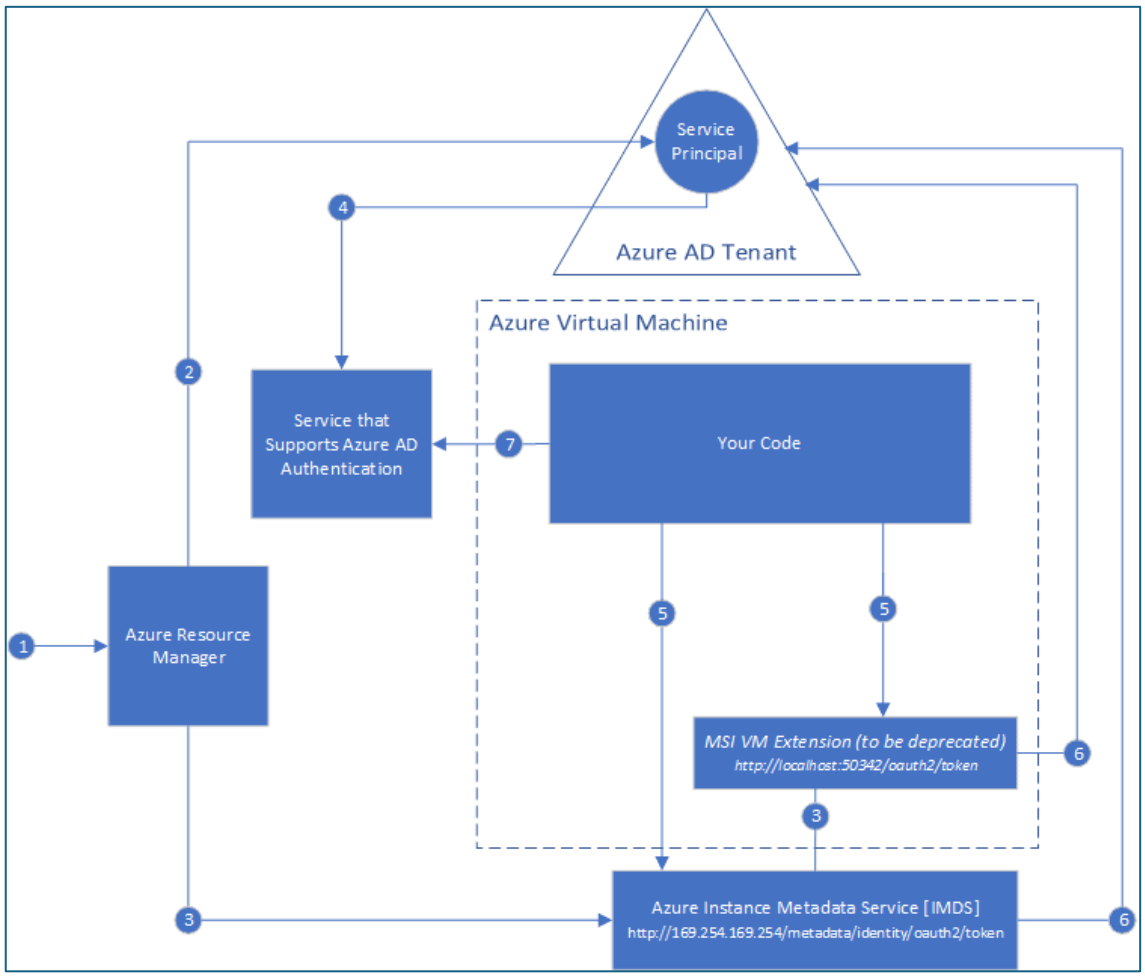
1. **Azure Key Vault** is a cloud service that provides a secure store for secrets. It is a logical group of secrets.
2. It helps you securely store classified information such as keys, passwords, certificates, and other secrets.
3. • Secrets management.
   • Key management.
   • Certificate management
   • Storing secrets backed by hardware security modules (HSMs).



Check out: Microsoft Azure provides governance features and services in order to implement policy-based management for all Azure services available on-cloud and on-premise. In this blog post, we'll cover Topic 3.4 Microsoft Azure Governance which includes Azure Blueprints & Azure Policy.

5. Microsoft Azure Security Center

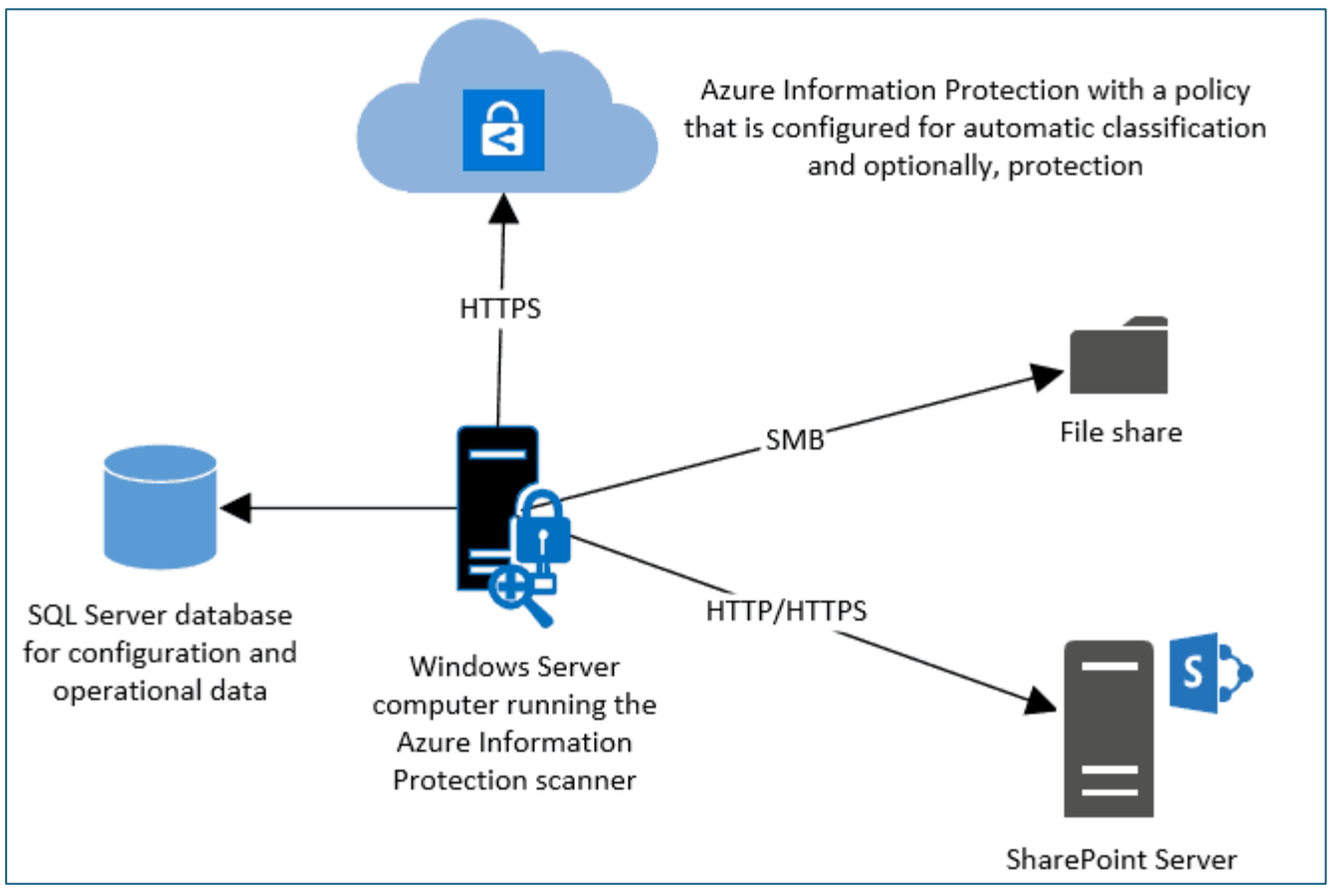
1. **Azure Security Center** provides tools and services across hybrid cloud and on-premise workload to make the cloud more secure.
2. It is a unified infrastructure security management system
3. It **strengthens the security posture**, **protect against threats** by assessing the workloads and raising security alerts and **secure faster** by natively integrating and auto-provisioning Azure security services.



Also Read: Our blog post on **Azure Resource Group**. Click here

6. Azure Information Protection

1. Azure Information Protection(AIP) helps the customer to classify, protect documents and emails by applying labels.
2. Labels can be applied automatically by administrators, manually by users, or by a combination of users.



Check Out: Our blog post on Capex Opex. Click here

7. Azure Advanced Threat Protection

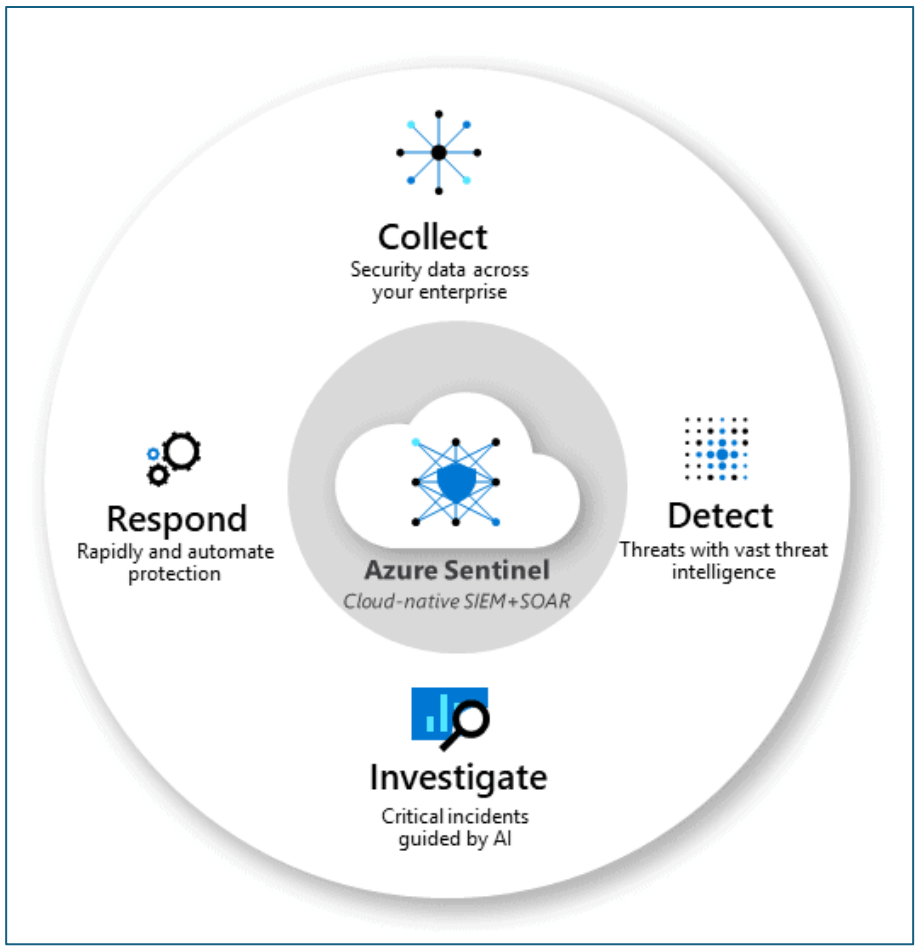
1. Azure ATP is a security service that leverages on-premises Active Directory signals.
2. It monitors users, entity behavior, and activities with learning-based analytics
3. It protects user identities and credentials stored in Active Directory
4. Identify & investigate suspicious user activities and advanced attacks
5. Provide clear incident information on a simple timeline

8. Azure Sentinel

Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution that delivers intelligent security analytics and threat intelligence throughout the enterprise, creating a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Azure Sentinel is your overview of the entire enterprise reducing the stress of increasingly sophisticated attacks, increasing volumes of alerts, and resolution timeframes.

- **Collect data at cloud scale** from all users, devices, applications, and infrastructure, both on-premises as we as on multiple clouds.
- **Detect previously undetected threats** and minimize false positives using Microsoft's analytics and advanced threat intelligence.
- **Investigate threats with artificial intelligence**, and survey for suspicious activities at scale.
- **Respond to incidents rapidly** with built-in orchestration and automation of common tasks.



AZ 900 Exam Questions:

Q 1: Which Azure service should you use to store certificates?

A. Azure Security Center
B. an Azure Storage account
C. Azure Key Vault
D. Azure Information Protection

Correct Answer: C
Explanation: Azure Key Vault securely stores classified information such as keys, passwords, and certificates.

Q 2: Your company plans to automate the deployment of servers to Azure. Your manager is concerned that you may expose administrative credentials during the deployment. You need to recommend an Azure solution that encrypts the administrative credentials during the deployment. What should you include in the recommendation?

A. Azure Key Vault
B. Azure Information Protection
C. Azure Security Center
D. Azure Multi-Factor Authentication (MFA)

Correct Answer: A

Module 05:

1. Azure Identity Services | Authentication, Authorization & Active Directory (AD)

A. Identity

- A user with a username and password.
- Also applications or other servers with secret keys or certificates.
- The fact of being something or someone.

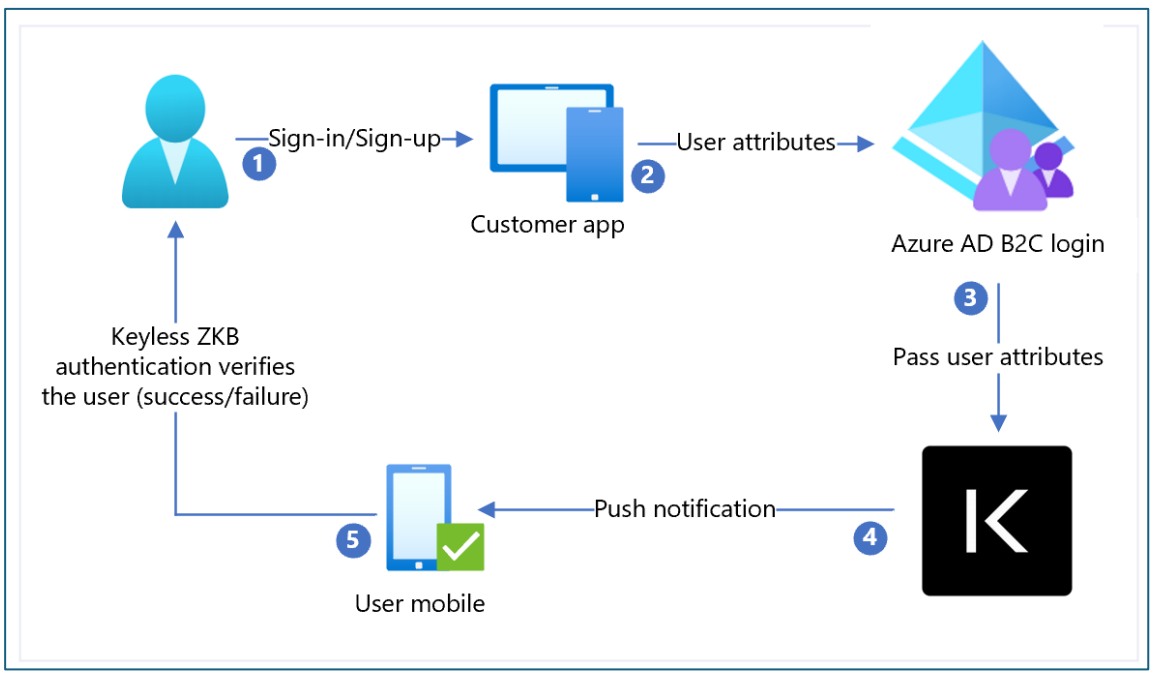
B. Authentication: The process of verification/assertion of identity

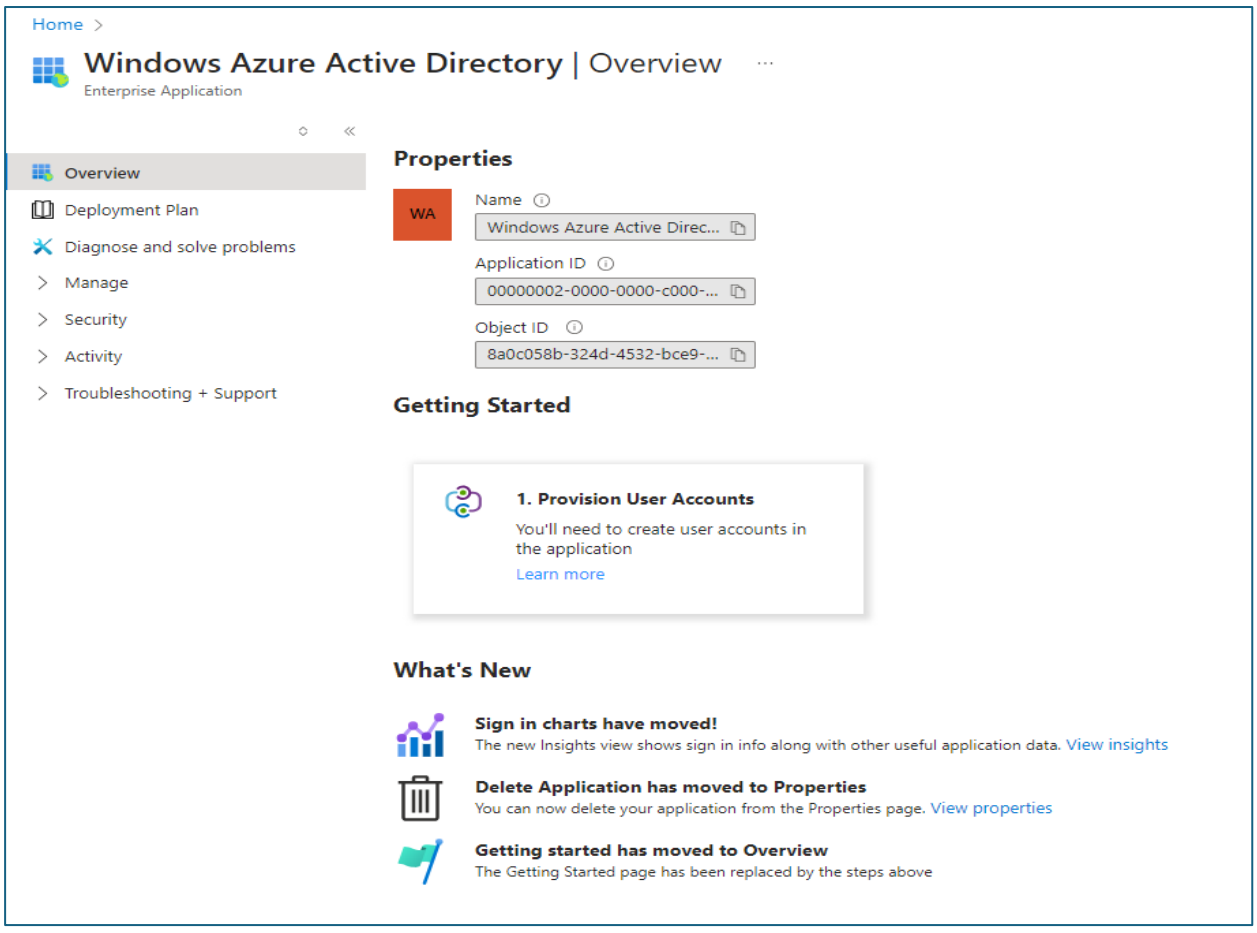
C. Authorization: The process of ensuring that only authenticated identities get access to the resources for which they have been granted access.

D. Access Management: The process of controlling, verifying, tracking and managing access to authorized users and applications.

E. Azure Active Directory

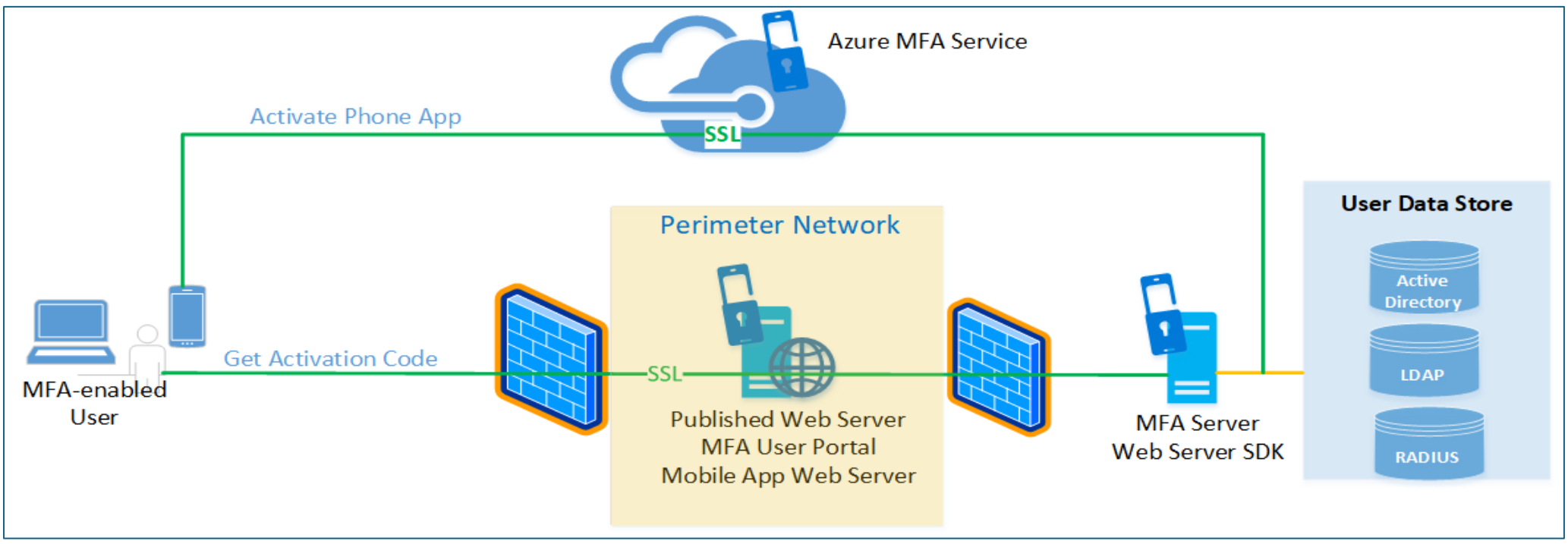
- Identity and Access Management service in Azure
- Identities management – users, groups, applications
- Access management – subscriptions, resource groups, roles, role assignments, authentication & authorization settings, etc.
- Used by multiple Microsoft cloud platforms
    - Azure
    - Microsoft 365
    - Office 365
    - Live.com services (Skype, OneDrive, etc.)





F. Multi-factor Authentication (MFA)

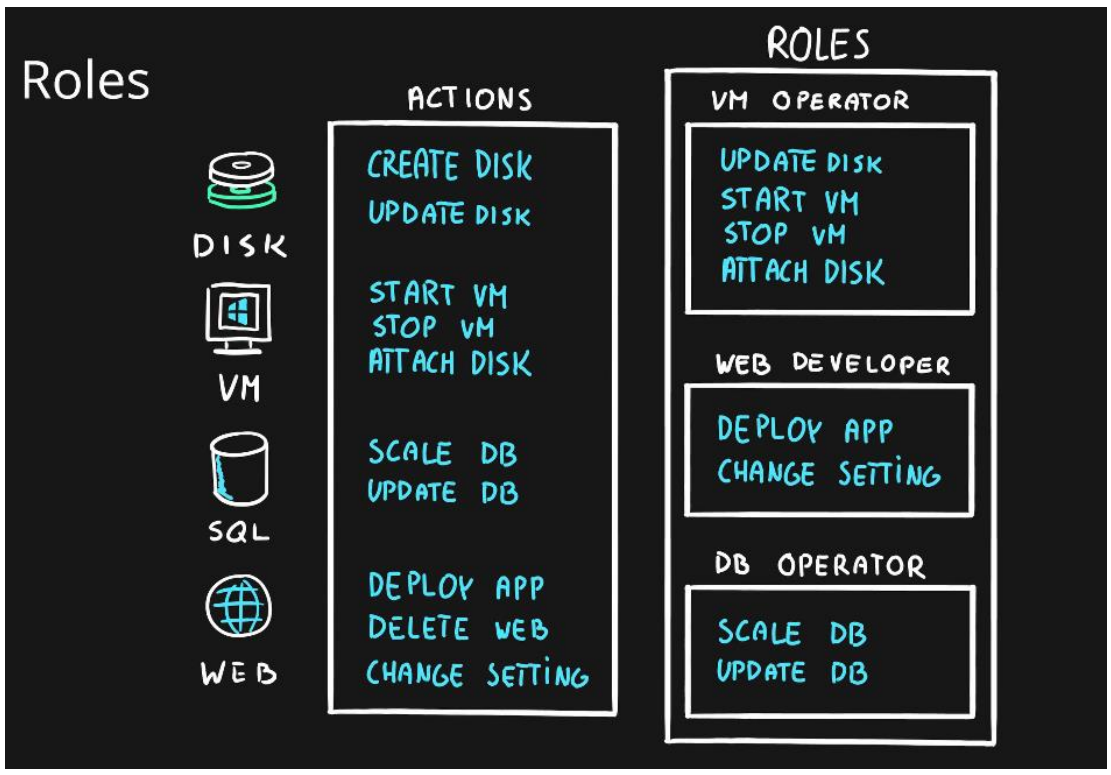
- Process of authentication using more than one factor (evidence) to prove identity
- Factor types
  - **Knowledge Factor** – "Something you know", ex. password, pin
  - **Possession Factor** – "Something you have", ex. phone, token, card, key
  - **Physical Characteristic Factor** – "Something you are", ex. fingerprint, voice, face, eye iris
  - **Location Factor** – "Somewhere you are", ex. GPS location
- Supported by Azure AD by default (simple on-off switch)



2. Role-Based Access Control (RBAC)

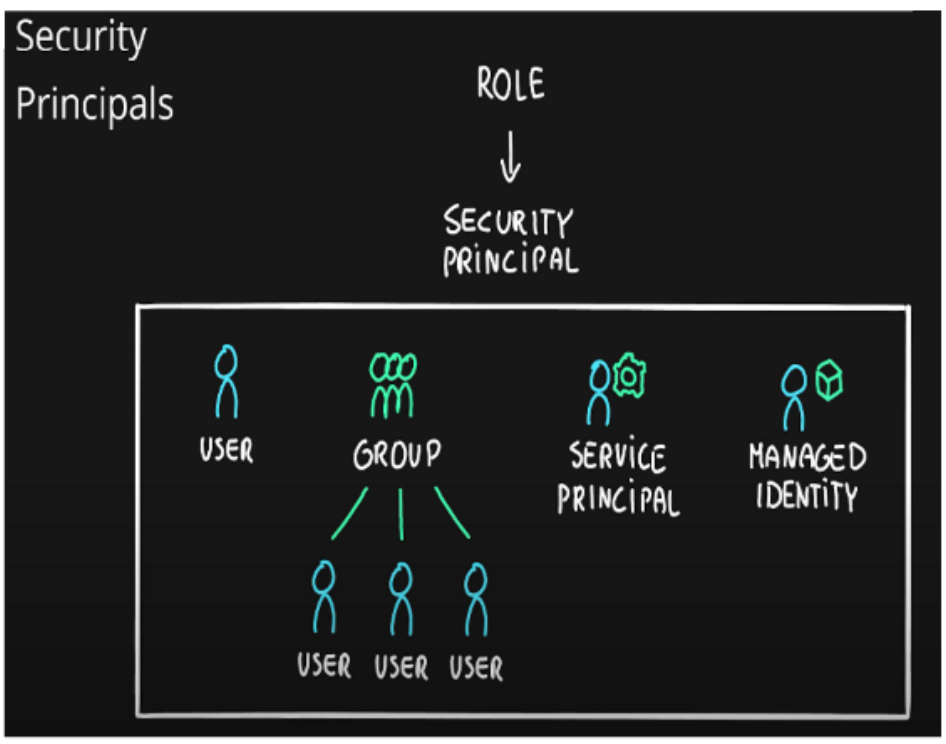
A. What is a Role?

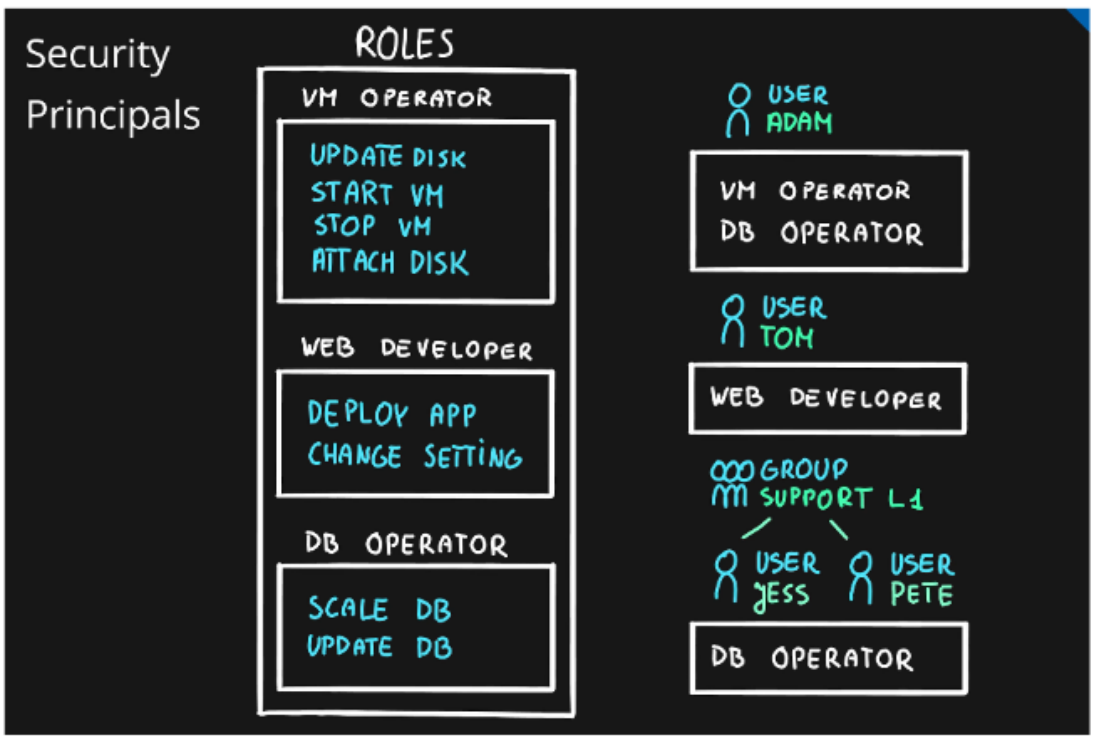
- **Role** (role definition) is a collection of actions that the assigned identity will be able to perform.
- Role definition is an answer to a question "What can be done?"



B. What is a Security Principal?

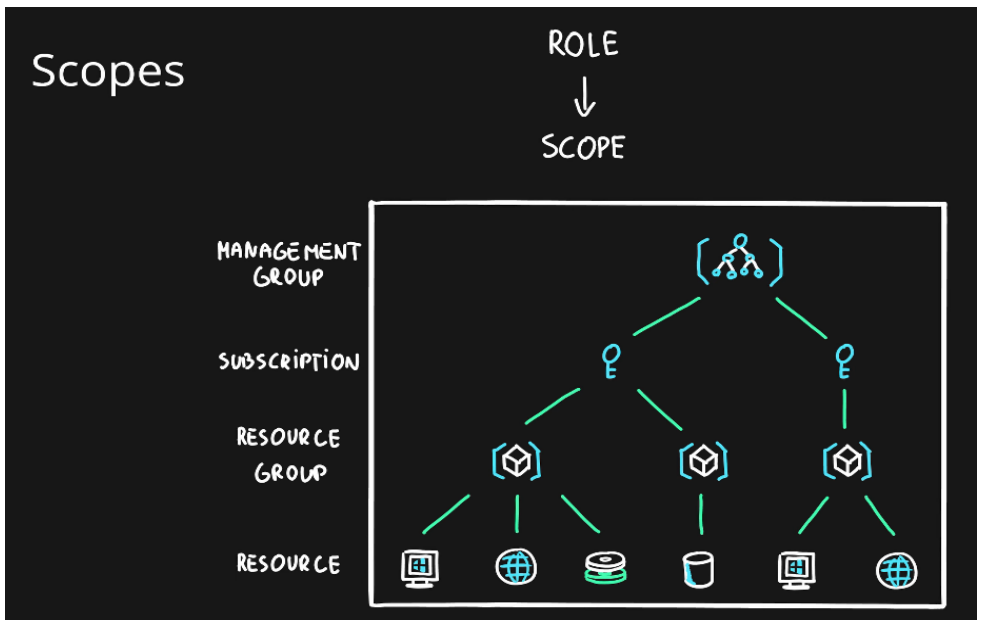
- **Security Principal** is an Azure object (identity) that can be assigned to a role (ex. users, groups or applications).
- **Security Principal assignment** is an answer to a question "Who can do it?"





C. What is a Scope?

- **Scope** is one or more Azure resources that the access applies to.
- Scope assignment is an answer to a question "Where can it be done?"

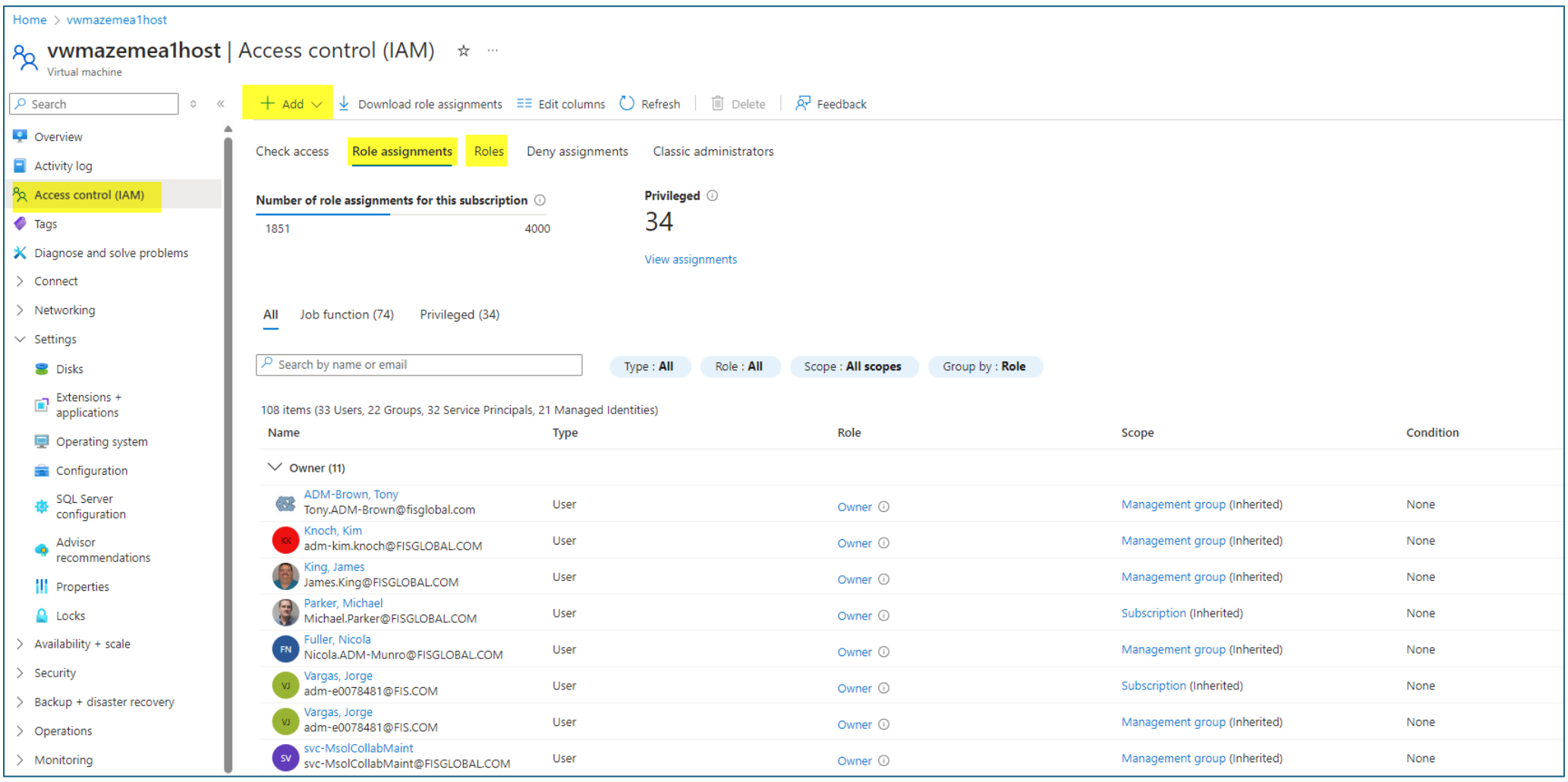


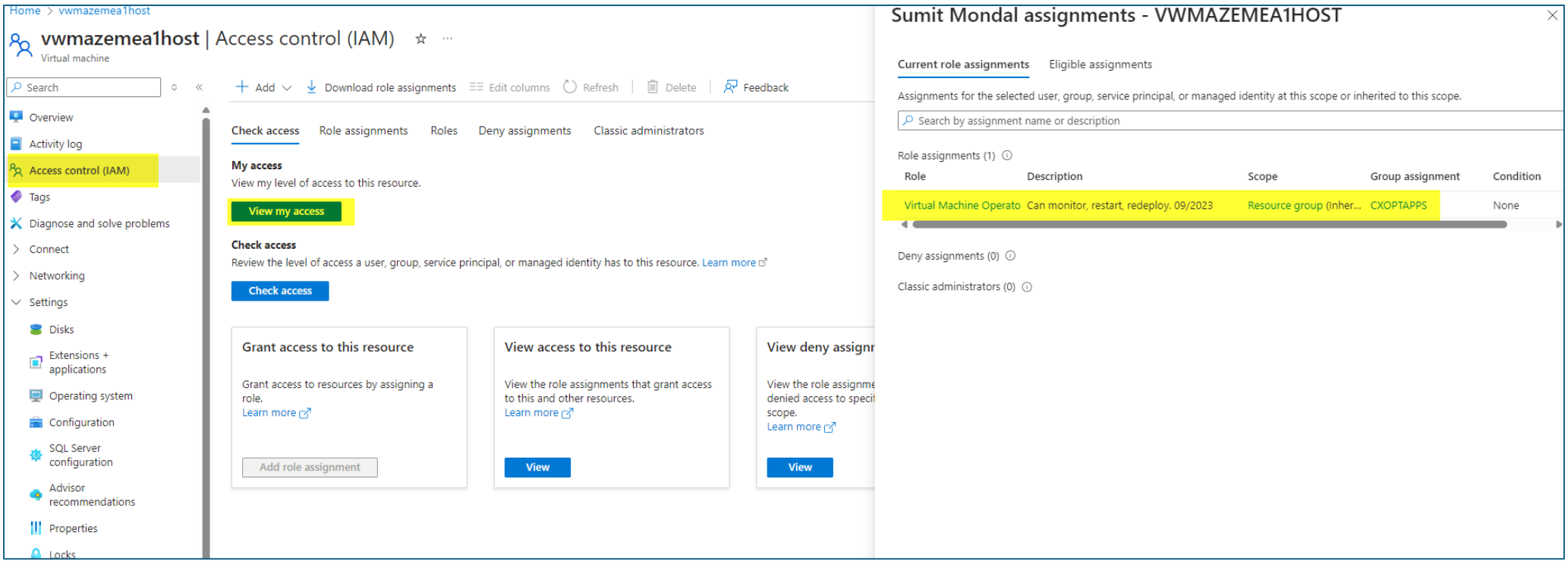
D. What is a Role Assignment?

Role assignment is a combination of the role definition, security principal and scope.

E. Azure Role-based Access Control (RBAC)

- Authorization system built on Azure Resource Manager (ARM)
- Designed for fine-grained access management of Azure Resources
- Role assignment is combination of
  - **Role definition** – list of permissions like create VM, delete SQL, assign permissions, etc.
  - **Security Principal** – user, group, service principal and managed identity
  - **Scope** – resource, resource groups, subscription, management group
- Hierarchical
  - Management Groups > Subscriptions > Resource Groups > Resources
- Built-in and Custom roles are supported



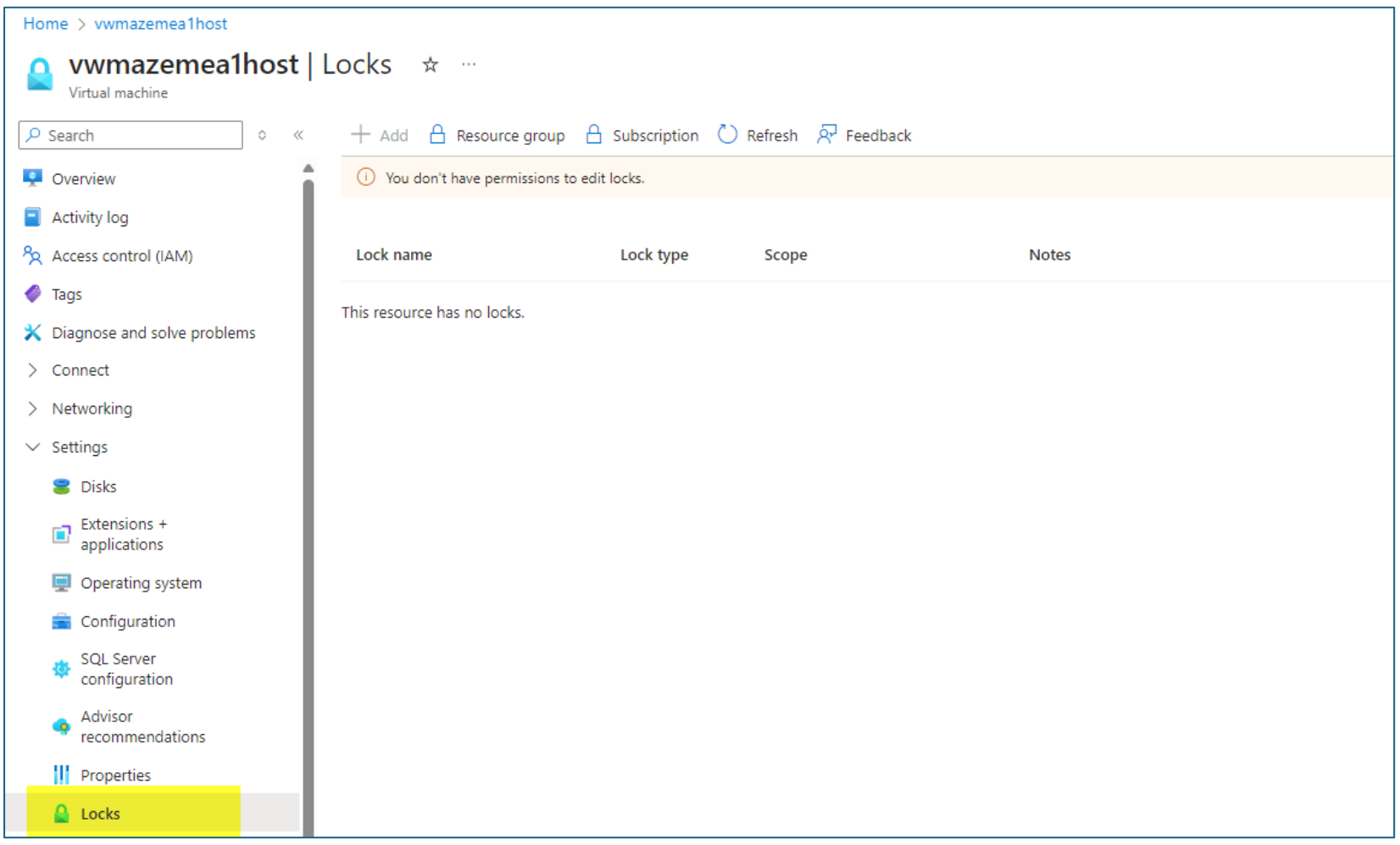


3. Azure Resource Lock

Azure Resource Lock

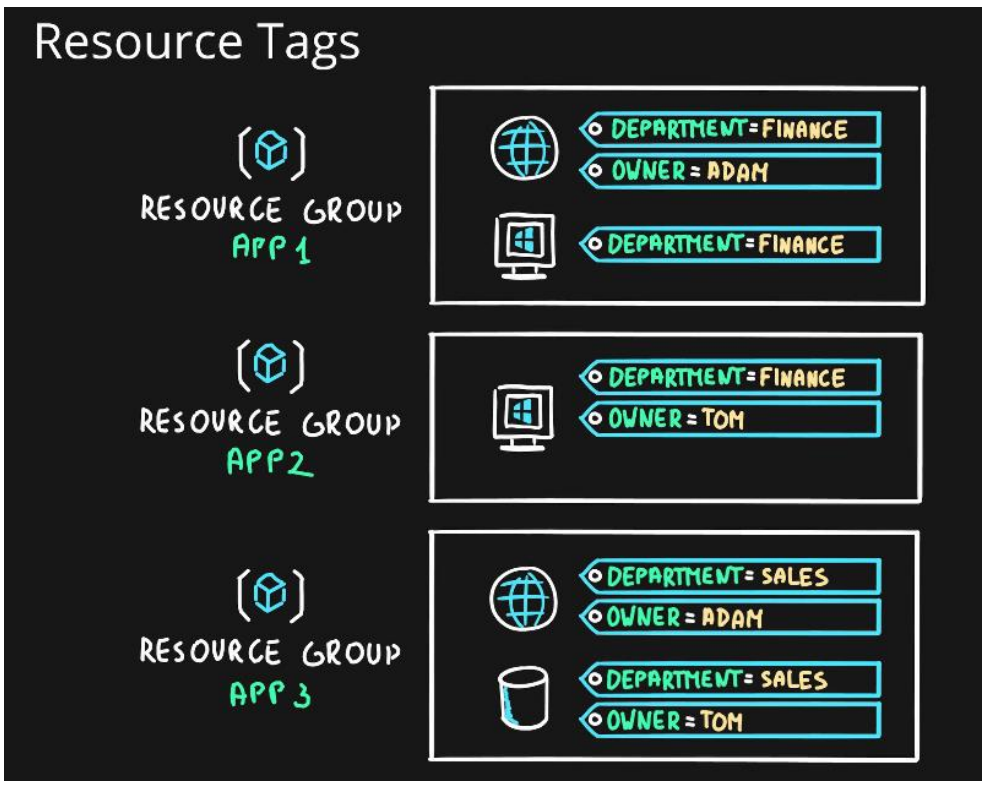
- Designed to prevent accidental deletion and/or modification
- Used in conjunction with RBAC
- Scopes are hierarchical (inherited)
    - Subscriptions > Resource Groups > Resources
- Management Groups can't be locked
- Only Owner and User Access Administrator roles can manage locks (**built-in** roles)

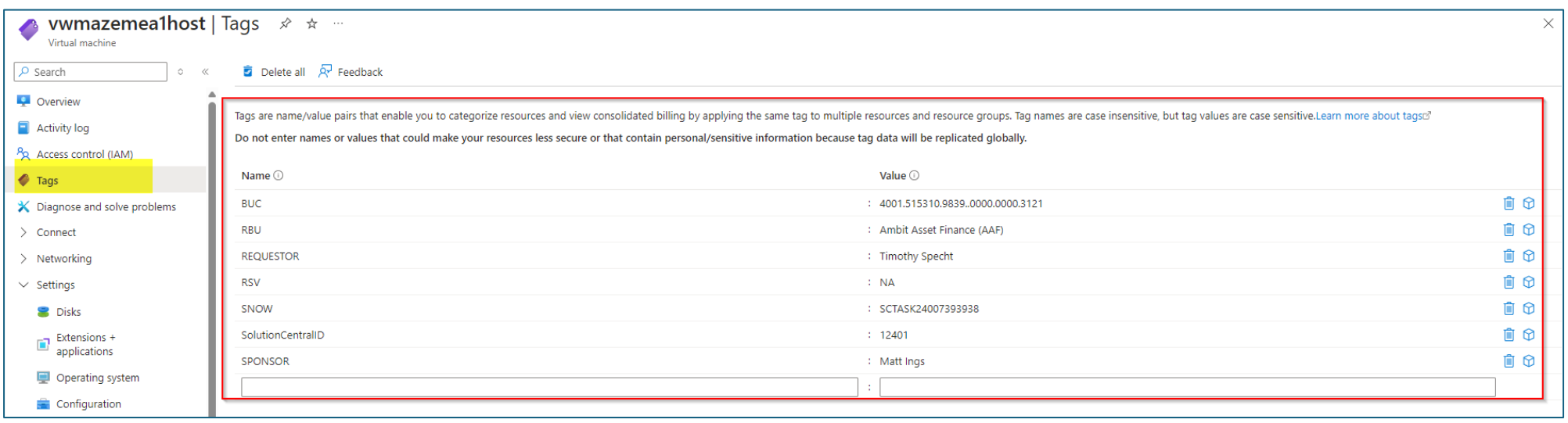
Lock Types	Read	Update	Delete
CanNotDelete	Yes	Yes	No
ReadOnly	Yes	No	No



4. Azure Resources Tags

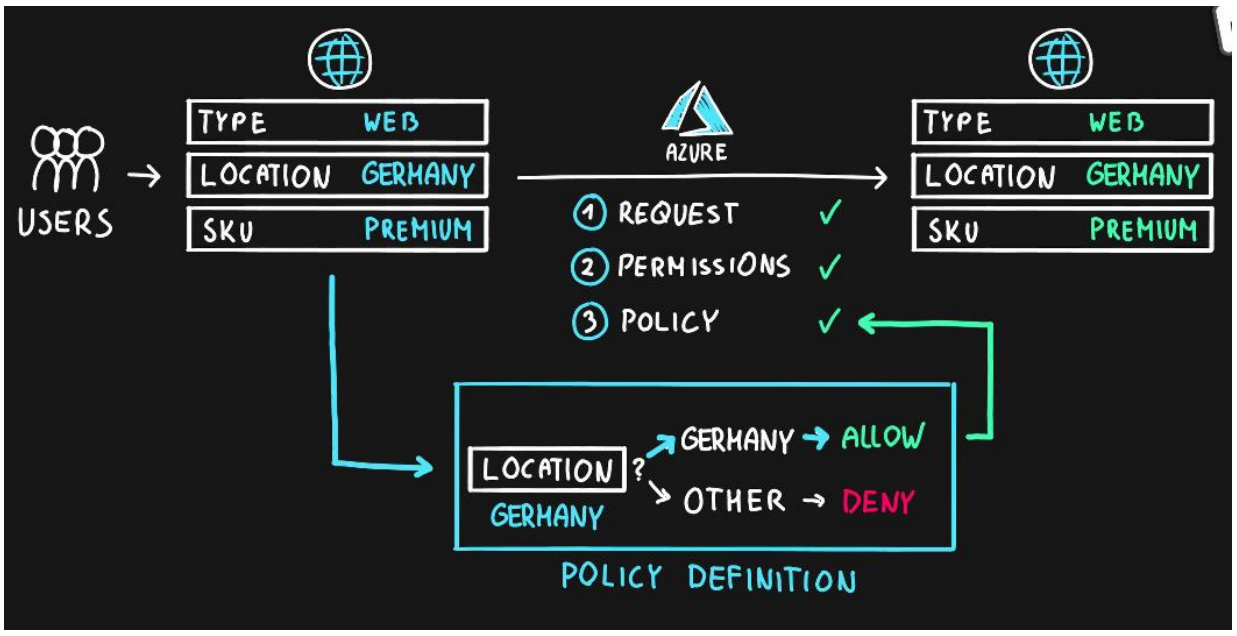
a. Tags are simple Name (key) - Value pairs
b. Designed to help with organization of Azure resources
c. Used for resource governance, security, operations management, cost management, automation, etc.
d. Typical **tagging strategies**
    i. **Functional** – mark by **function** (ex: environment = production)
    ii. **Classification** – mark by **policies used** (ex: classification = restricted)
    iii. **Finance/Accounting** – mark for **billing purposes** (ex: department = finance)
    iv. **Partnership** – mark by **association of users/groups** (ex: owner = adam)
e. Applicable for **resources**, **resource groups** and **subscriptions**
f. NOT inherited by default



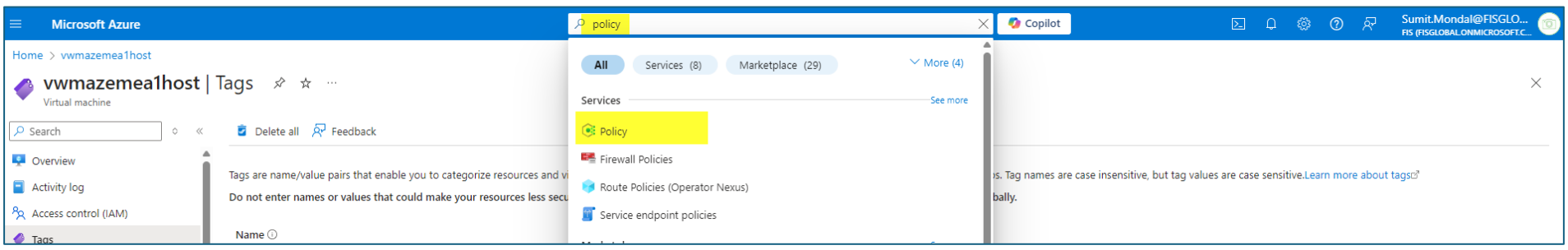


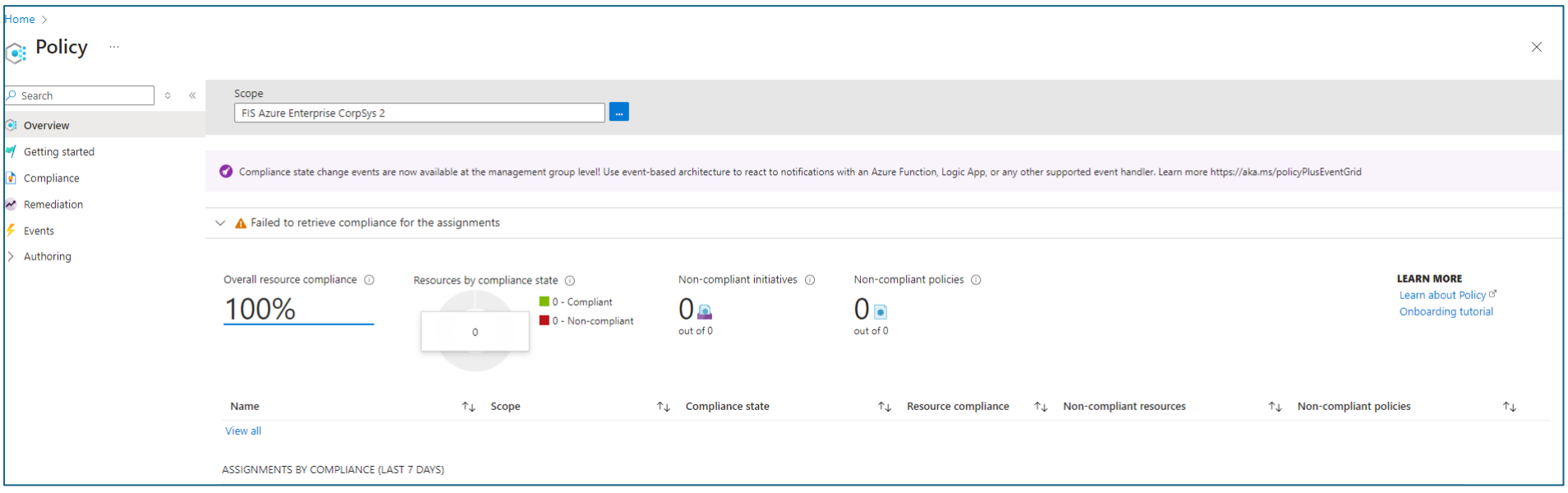
5. Azure Policy:

a. Designed to help with resource governance, security, **compliance**, **cost management**, etc.
b. Policies focus on resource properties (**RBAC** focused on **user actions**)
c. Policy **definition** – Defines what should happen
    i. Define the condition (if/else) and the effect (deny, audit, append, modify, etc.)
        1. Examples include allowed *resource types*, *allowed locations*, *allowed SKUs*, *inherit resource tags*
d. **Built-in** and **custom** policies are supported
e. Policy **initiative** – a **group** of policy definitions
f. Policy **assignment** – assignment of a policy definition/initiative to a scope
    i. Scopes can be assigned to
        1. management groups,
        2. subscriptions,
        3. resource groups, and
        4. resources
g. Policies allow for exclusions of scopes
h. Checked during **resource creation** or **updates** and **existing ones with remediation tasks**



Example:





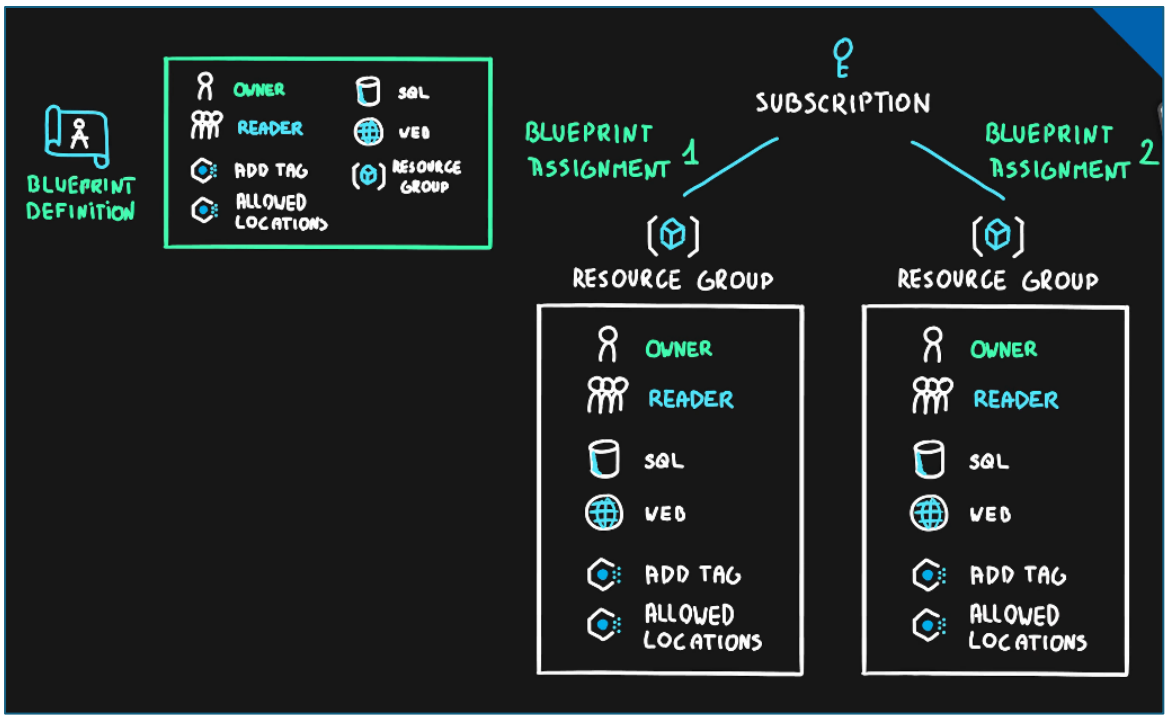
6. Azure BluePrint:

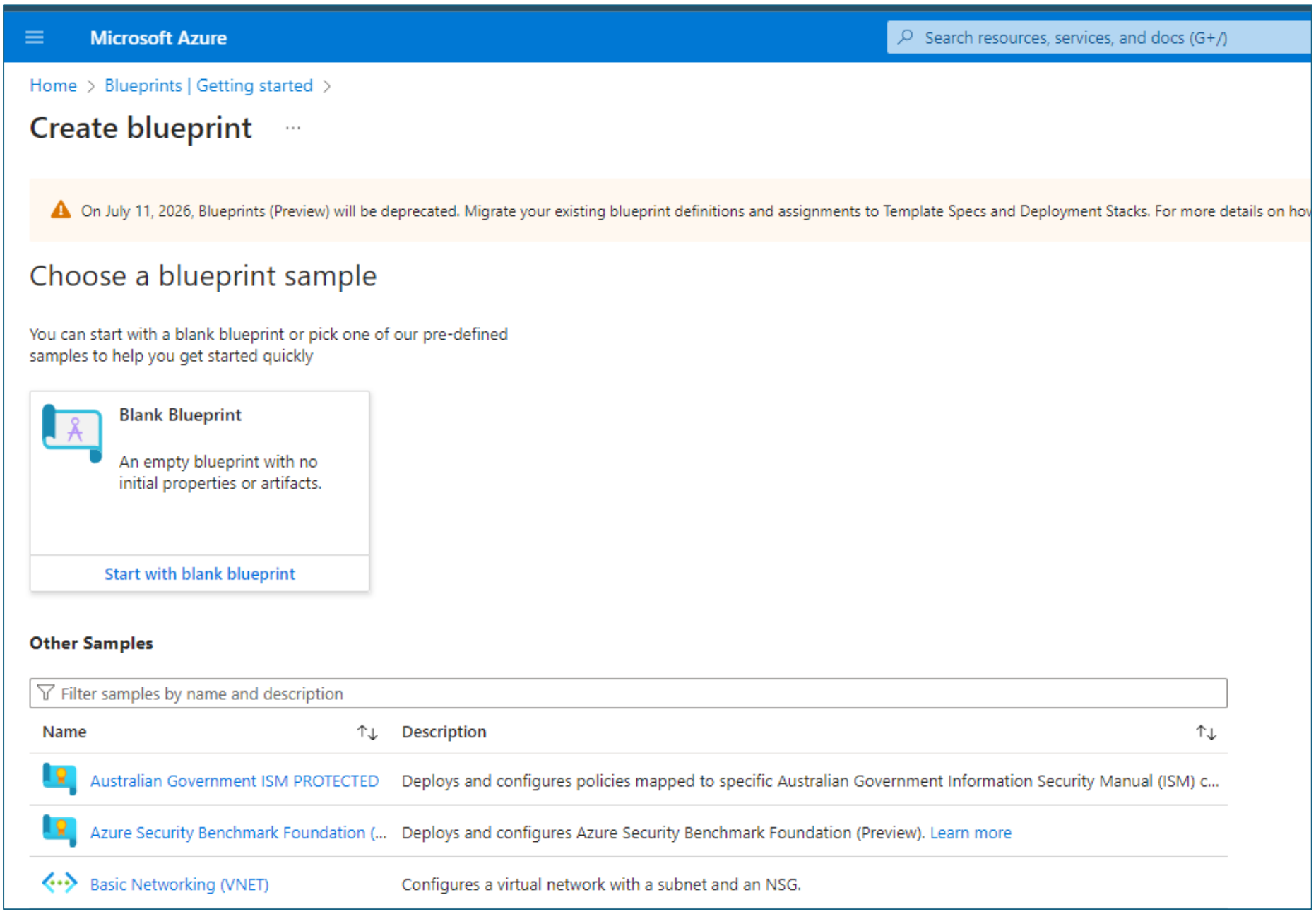
a. **Package** of various Azure components (**artifacts**)
   i. **Resource Groups**
   ii. **ARM Templates**
   iii. **Policy Assignments**
   iv. **Role Assignments**

b. Centralized storage for organizationally approved design patterns

c. Blueprint **definition** – describing what should happen (reusable package)

d. Blueprint **assignment** – describing where it should happen (package deployment)


BLUEPRINT DEFINITION
OWNER
READER
ADD TAG
ALLOWED LOCATIONS
SQL
VED
RESOURCE GROUP
SUBSCRIPTION
BLUEPRINT ASSIGNMENT 1
BLUEPRINT ASSIGNMENT 2
RESOURCE GROUP
RESOURCE GROUP
OWNER
READER
SQL
VED
ADD TAG
ALLOWED LOCATIONS
OWNER
READER
SQL
VED
ADD TAG
ALLOWED LOCATIONS


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Blueprints | Getting started >
Create blueprint
On July 11, 2026, Blueprints (Preview) will be deprecated. Migrate your existing blueprint definitions and assignments to Template Specs and Deployment Stacks. For more details on hov
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
Australian Government ISM PROTECTED
Deploys and configures policies mapped to specific Australian Government Information Security Manual (ISM) c...
Azure Security Benchmark Foundation (...
Deploys and configures Azure Security Benchmark Foundation (Preview). Learn more
Basic Networking (VNET)
Configures a virtual network with a subnet and an NSG.