Azure Secure & Defend

- Azure Monitor
- Defender for Cloud
- Microsoft Sentinel
- Entra ID Entitlement

Microsoft Applied Skills

brainymotion

Agenda

AZ-1004	Deploy and Configure Azure Monitor
SC-5002	Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls
SC-5001	Configure SIEM security operations using Microsoft Sentinel
SC-5008	Configure and Govern Entitlement with Microsoft Entra ID

Thomas Jäkel

brainymotion

Lead Trainer Cloud Infrastructure

Microsoft Certified Trainer since 1999

github.com/www42/asd

SC-5002

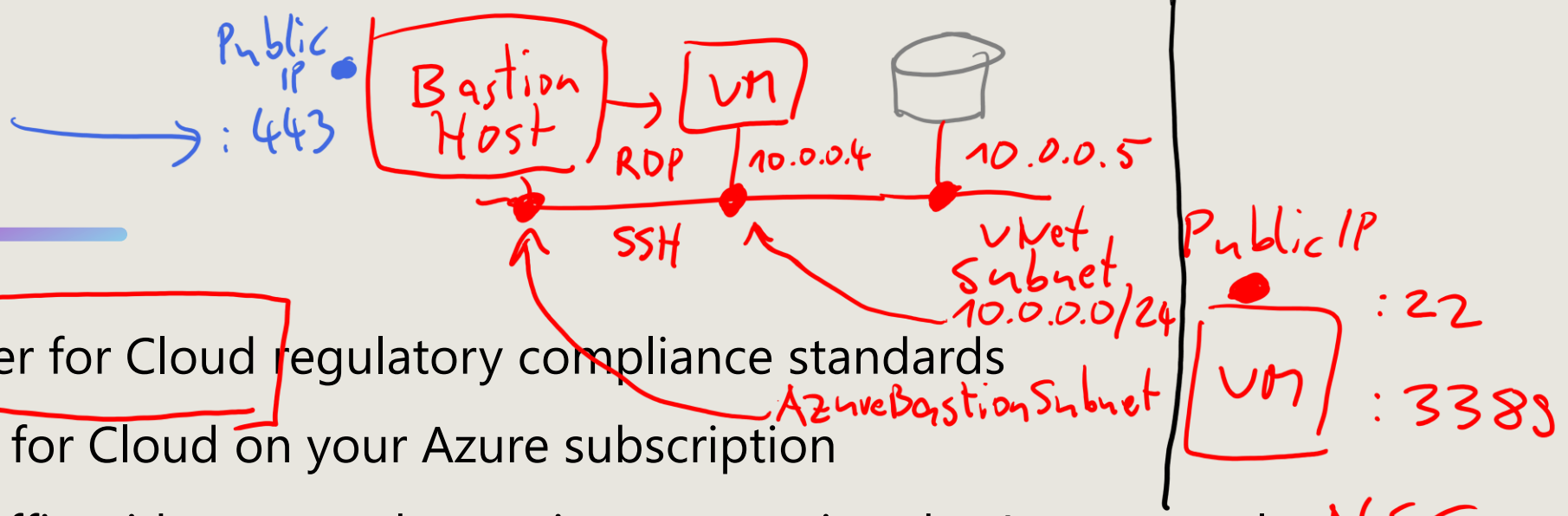
Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls

Introduction

This comprehensive applied skills course for Azure Security Engineers focuses on using Microsoft Defender for Cloud to secure Azure services and workloads. The course provides:

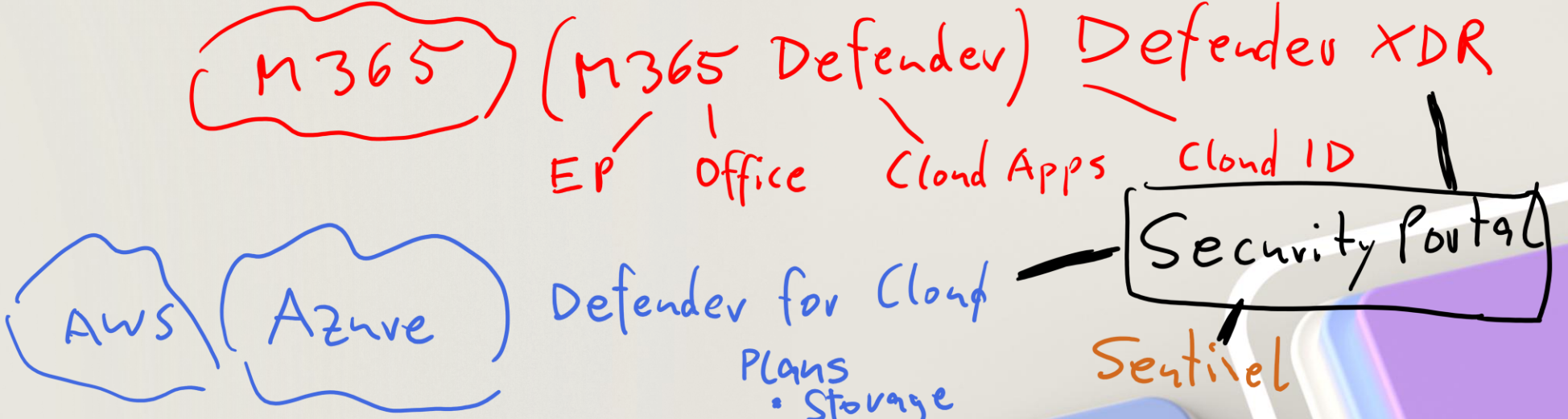
- In-depth understanding of Microsoft Defender for Cloud as a tool for enforcing regulatory compliance in Azure environments.
- Enhanced skills in securing cloud services and workloads against a variety of cyber threats.
- Mastery in applying compliance controls, ensuring adherence to legal and industry-specific security standards.
- The ability to proactively manage and respond to security alerts, maintaining the integrity of Azure cloud infrastructure.

Outline



1. Examine Defender for Cloud regulatory compliance standards
2. Enable Defender for Cloud on your Azure subscription
3. Filter network traffic with a network security group using the Azure portal
4. Create a Log Analytics workspace for Microsoft Defender for Cloud
5. Collect guest operating system monitoring data from Azure and hybrid virtual machines using Azure Monitor
6. Explore just-in-time VM access
7. Configure Azure Key Vault networking settings
8. Connect an Azure SQL server using an Azure Private Endpoint using the Azure portal

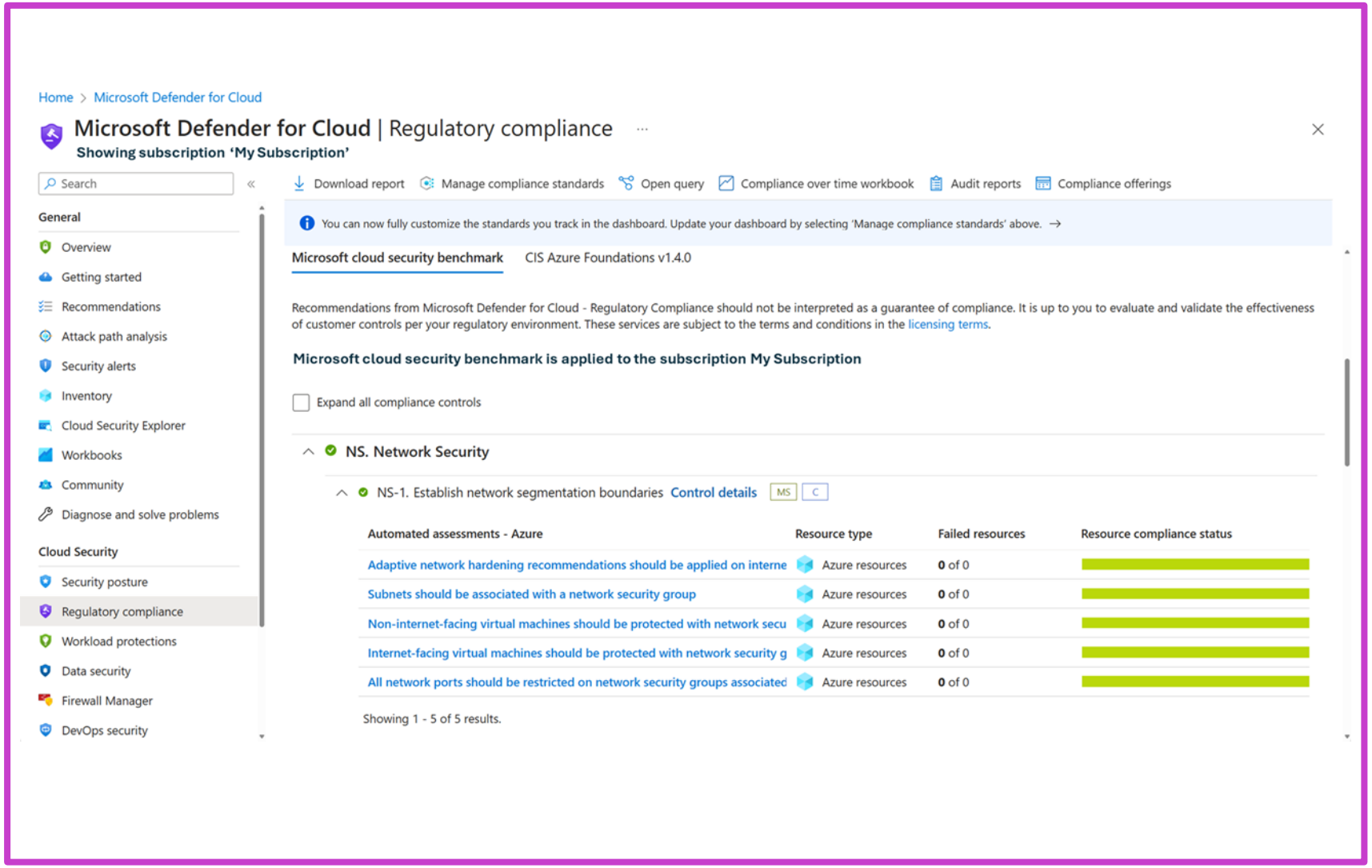
NSG
ASG
LAW
ARC
JIT



1/8 Examine Defender for Cloud regulatory compliance standards

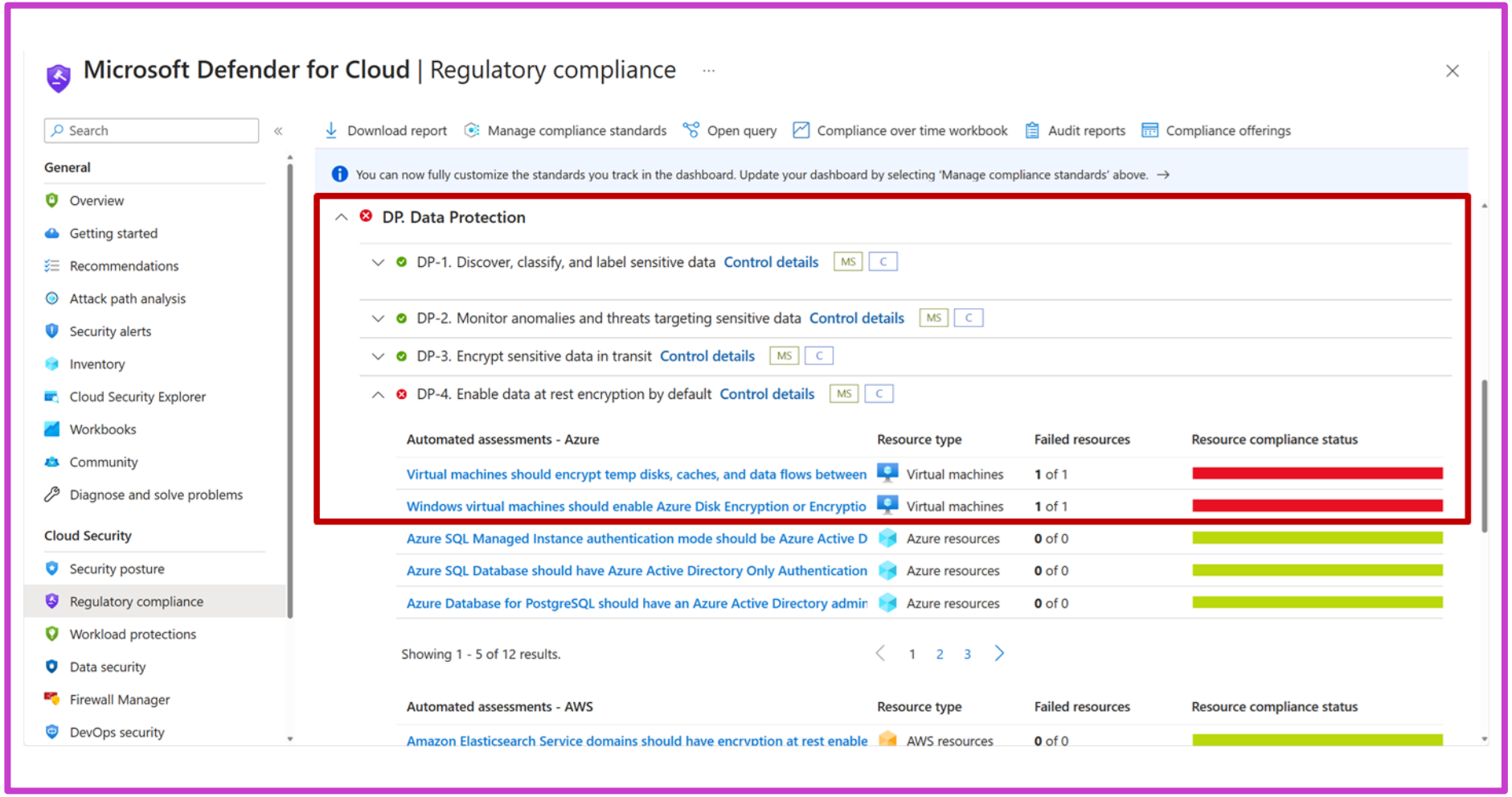
Regulatory compliance standards in Defender for Cloud

- Defender for Cloud identifies issues blocking compliance certification and displays security standards in the Regulatory compliance dashboard.
- Each security standard has multiple compliance controls, with compliant and non-compliant statuses based on assessments.
- The dashboard provides summaries, custom reports, audit downloads, and detailed compliance statuses for standards applied to specific scopes.



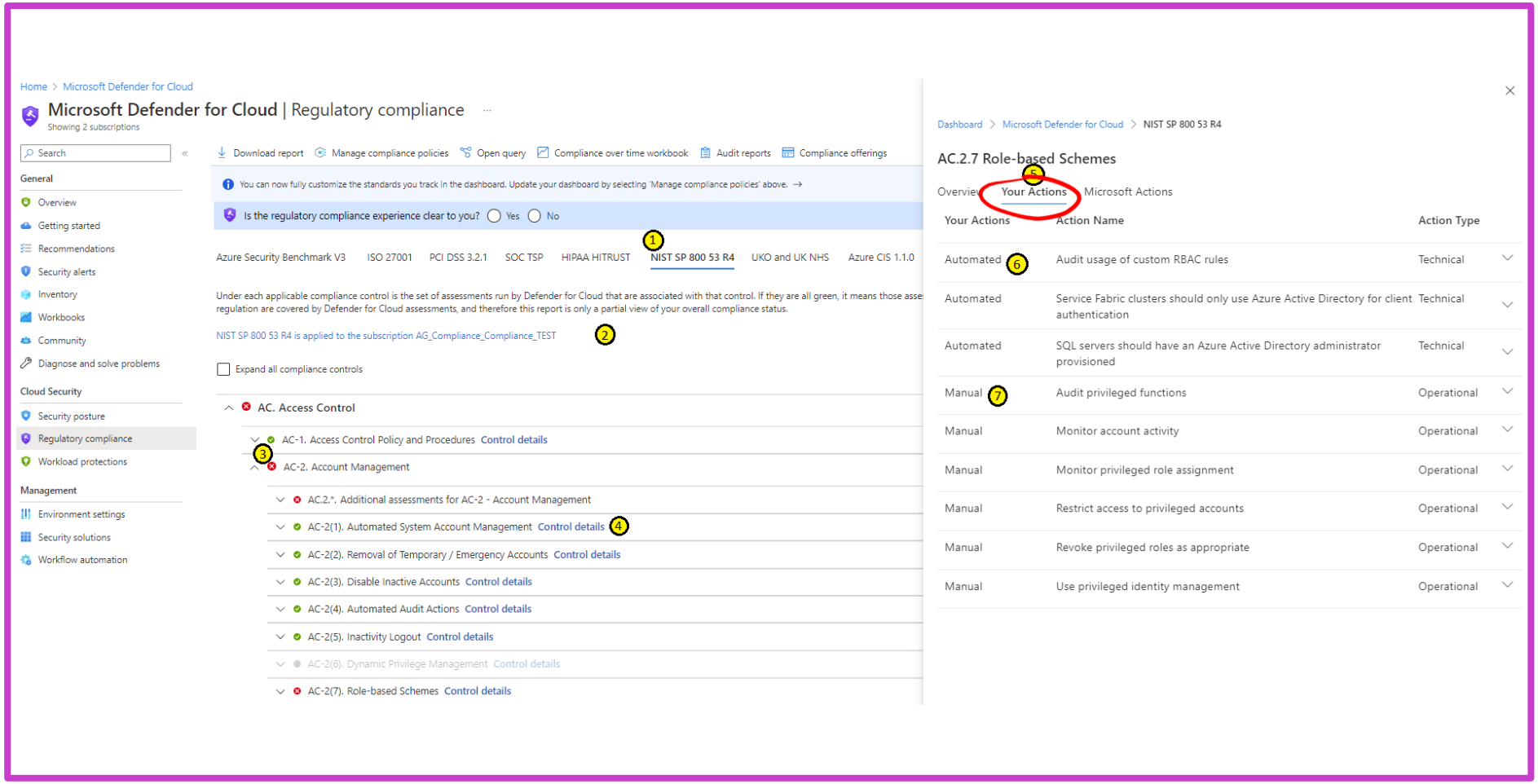
Microsoft cloud security benchmark in Defender for Cloud

- Defender for Cloud assesses hybrid environments against industry standards, regulatory standards, and benchmarks.
- Compliance dashboard provides continuous compliance information for Azure, AWS, and GCP.
- Microsoft cloud security benchmark automatically assesses onboarded subscriptions and accounts.

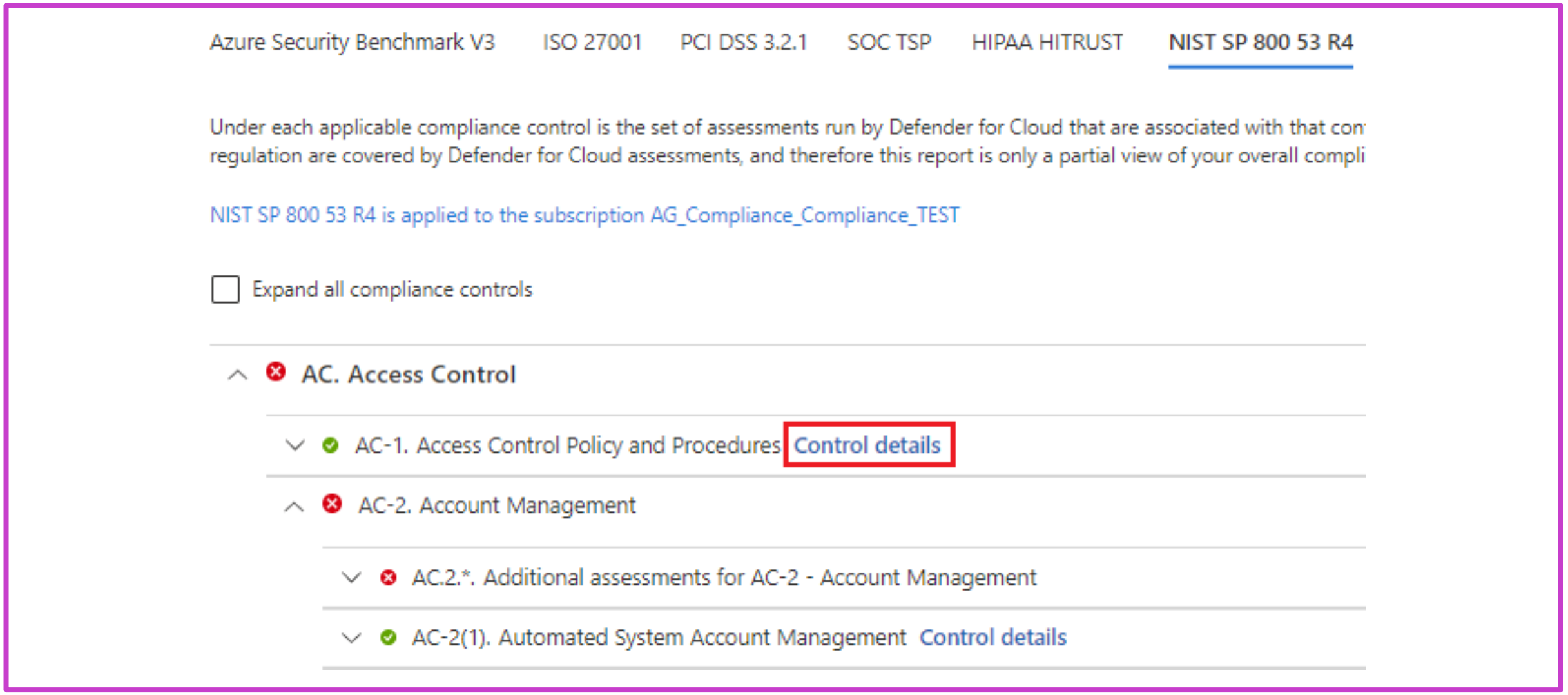


Improve regulatory compliance requirements

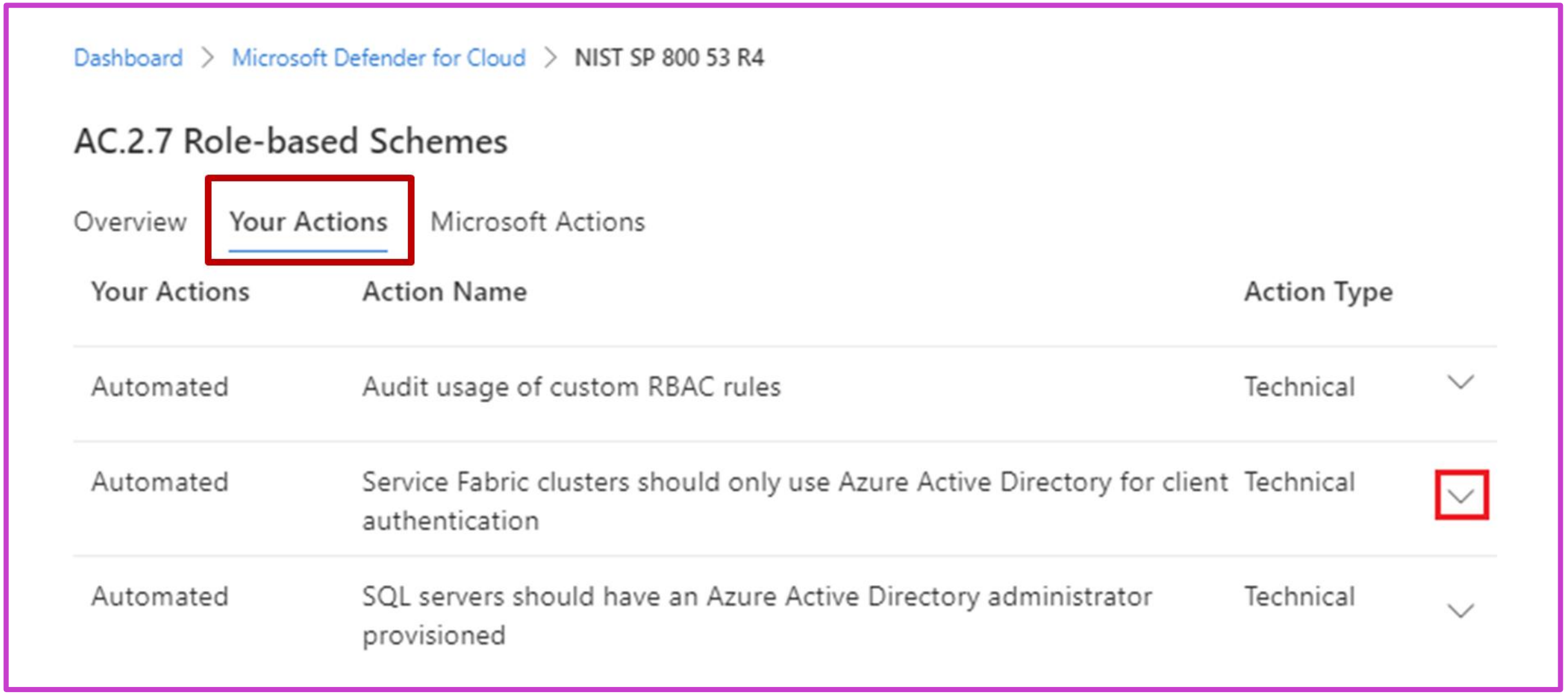
- Defender for Cloud assesses resources for compliance and identifies certification issues.
- Manage and interact with compliance standards in the regulatory compliance dashboard.
- Integrates with Purview Compliance Manager for centralized compliance management across cloud environments.



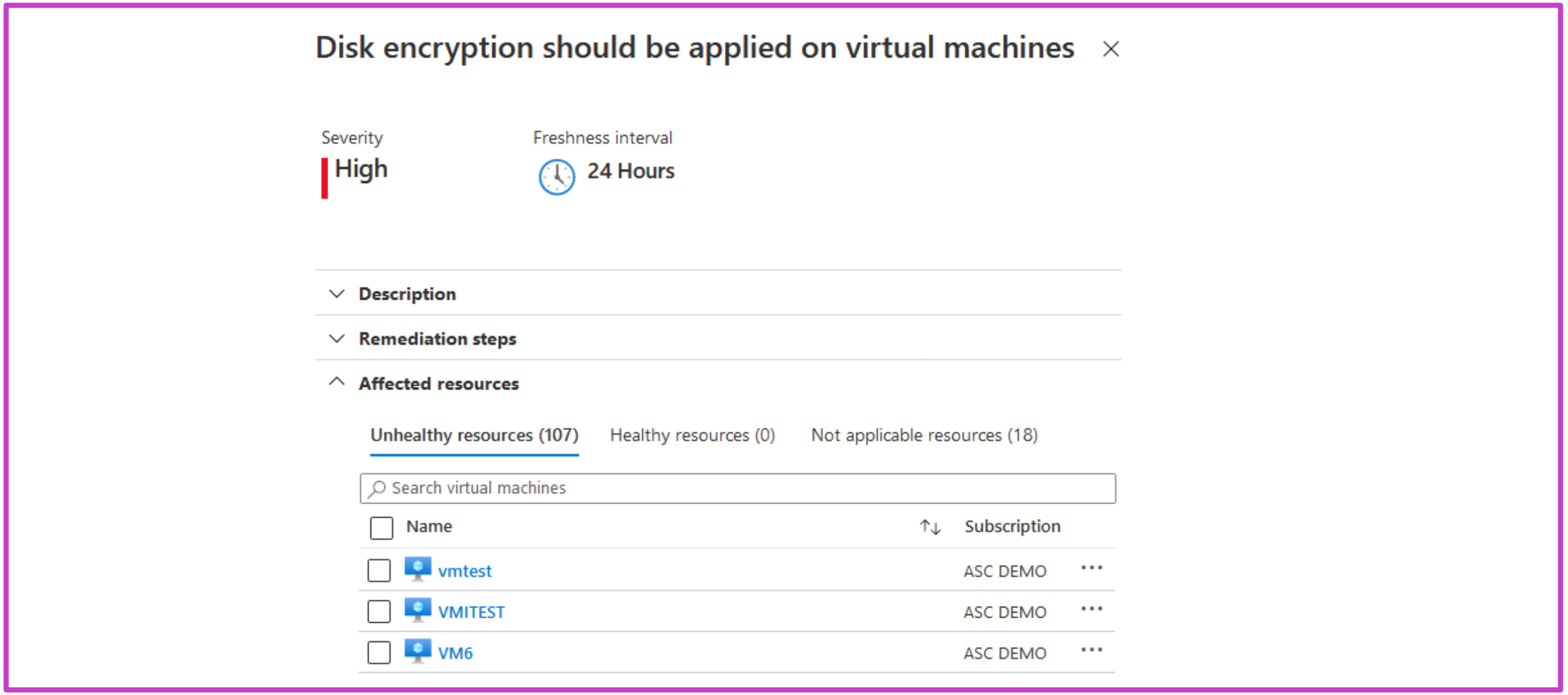
Example - Investigate issues



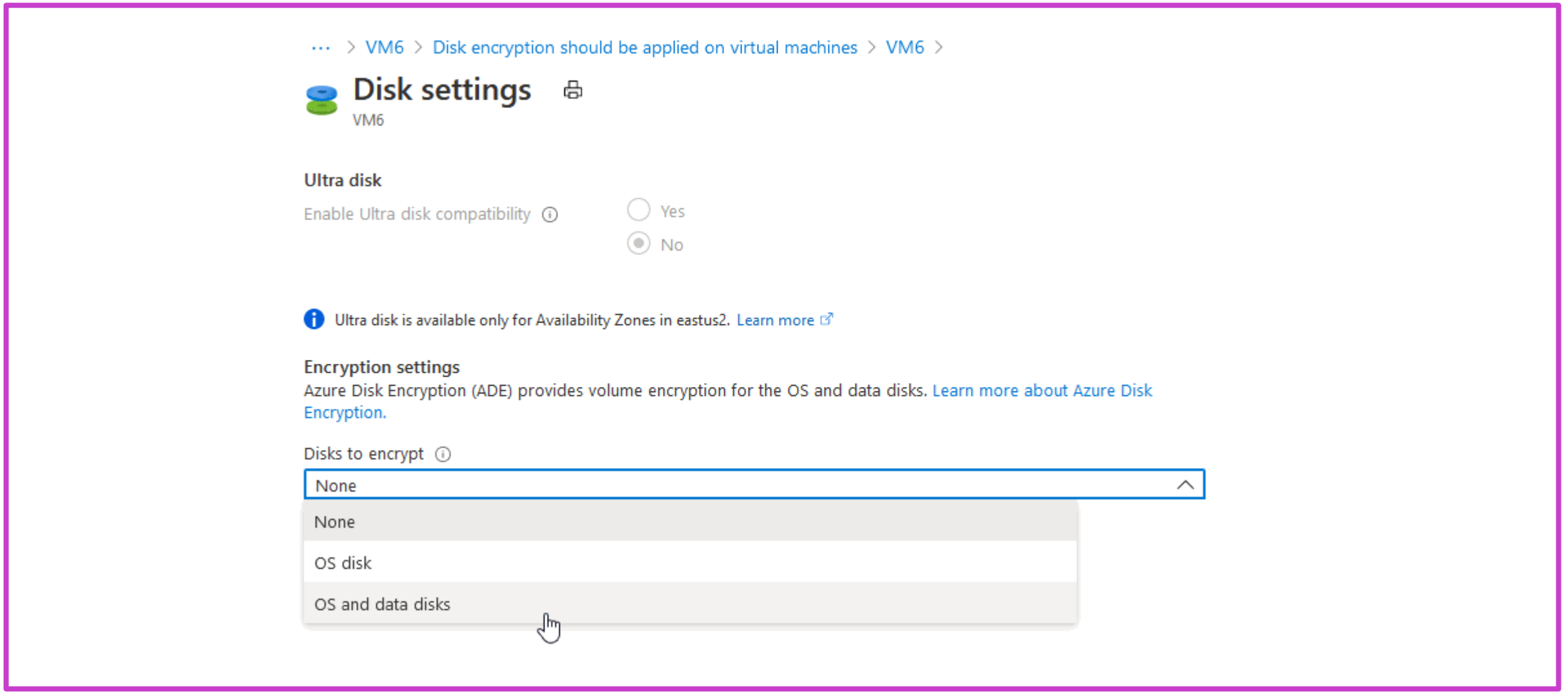
Example - Investigate issues (cont'd)



Example - Remediate an automated assessment



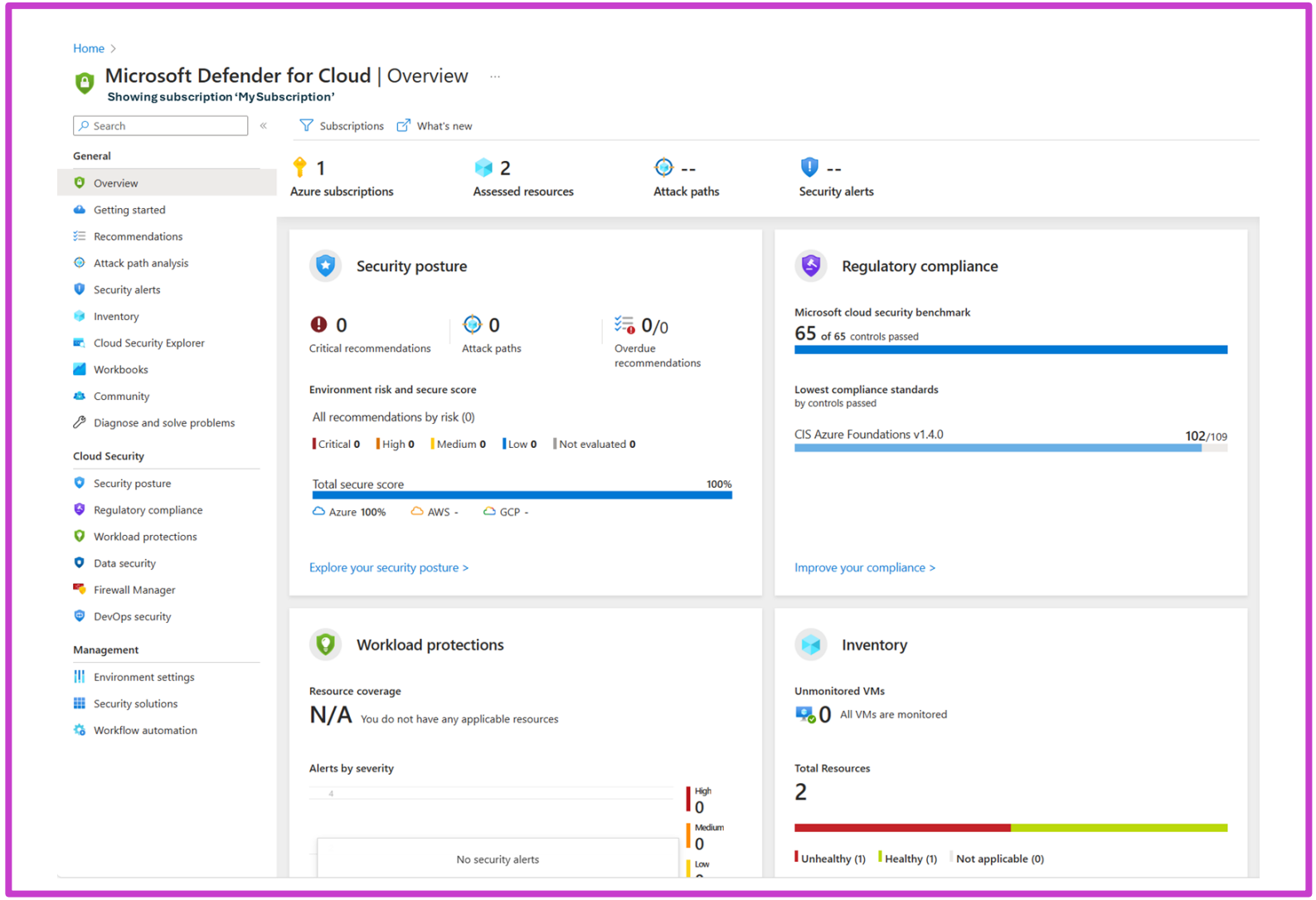
Example - Remediate an automated assessment (cont'd)



2/8 Enable Defender for Cloud on your Azure subscription

Connect your Azure subscription

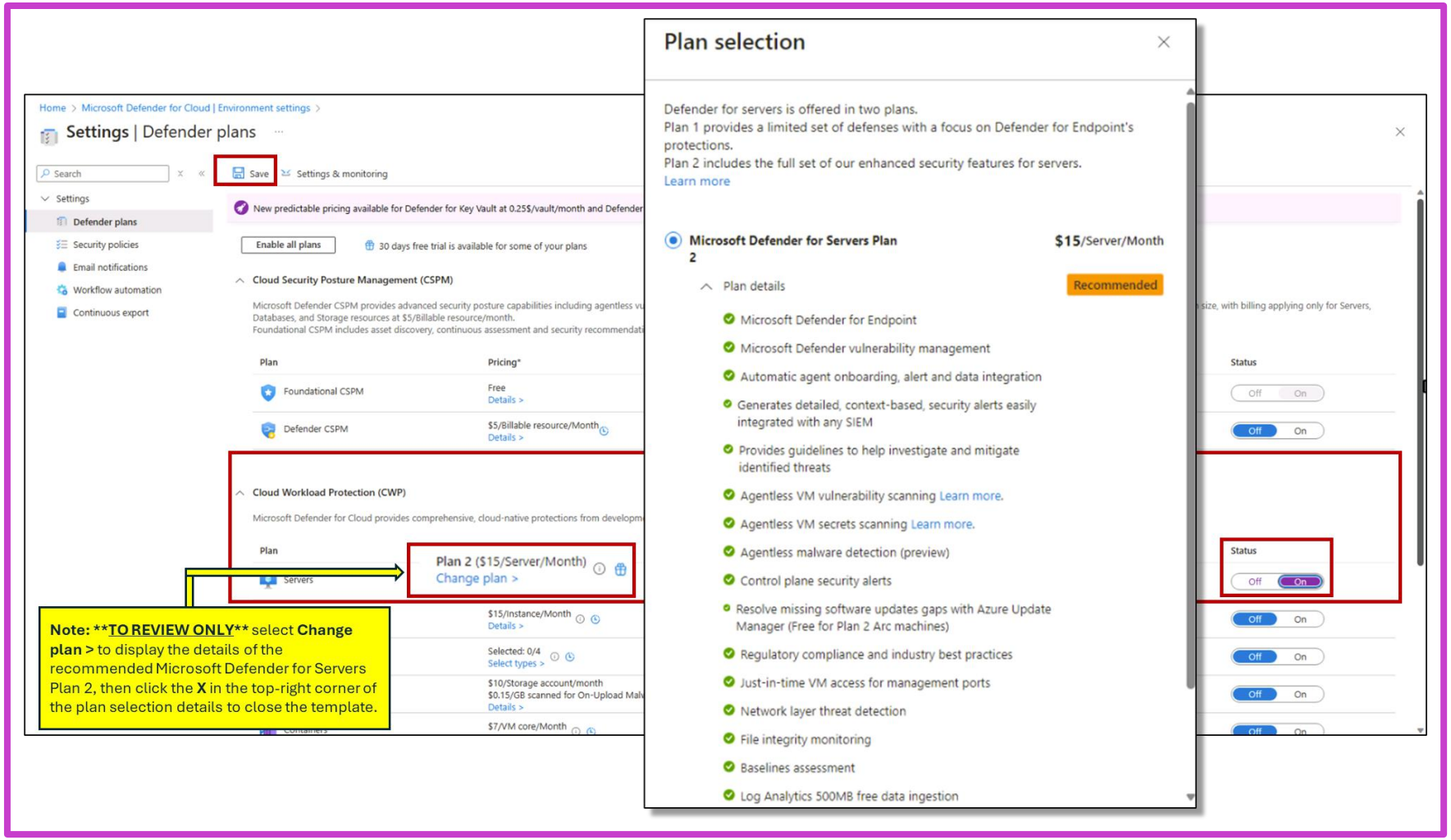
- Microsoft Defender for Cloud offers end-to-end protection for cloud applications with DevSecOps, cloud security posture management (CSPM), and cloud workload protection platform (CWPP) capabilities.
- Free for 30 days, it includes foundational CSPM and Microsoft Defender eXtended detection and response (XDR), with optional paid plans for full protection.
- Provides security recommendations, resource inventory, and a unified security posture view for hybrid cloud workloads.



Exercise – Configuring Microsoft Defender for Cloud Enhanced Security Features for Servers

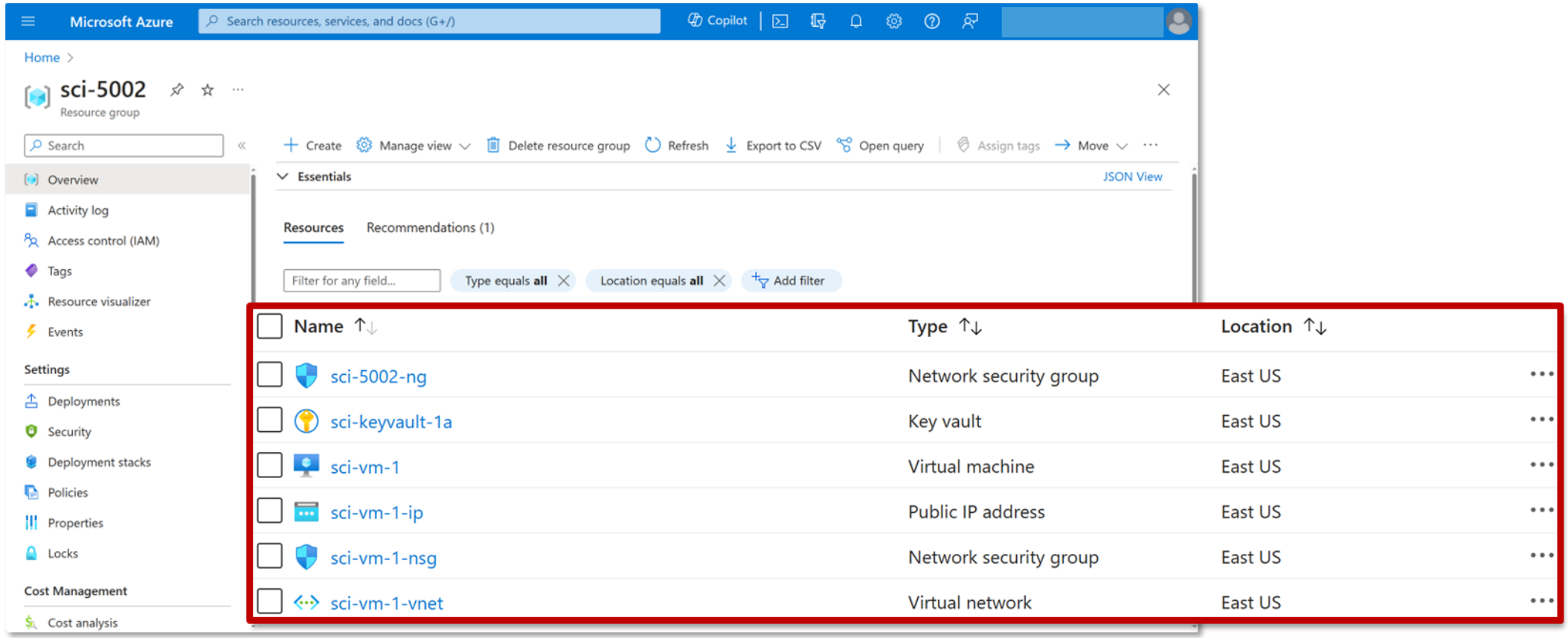
This exercise teaches students how to configure Microsoft Defender for Cloud Enhanced Security Features for Servers Cloud Workload Protection plan.

[Launch this Exercise in GitHub]



3/8 Filter network traffic with a network security group using the Azure portal

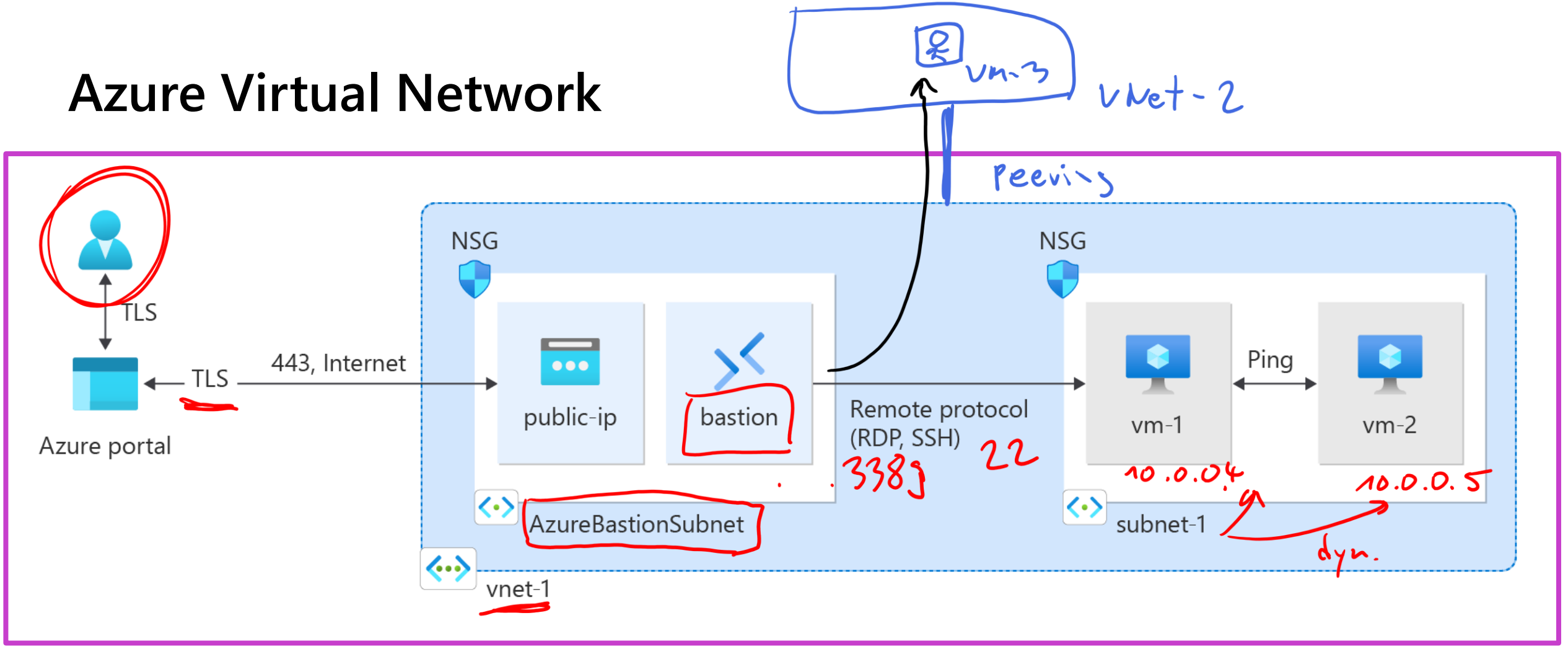
Azure Resource Group



A Resource Group is a container that holds related resources for an Azure solution.

- The resource group can include all the resources for the solution, or only those resources that you want to manage as a group.

Azure Virtual Network

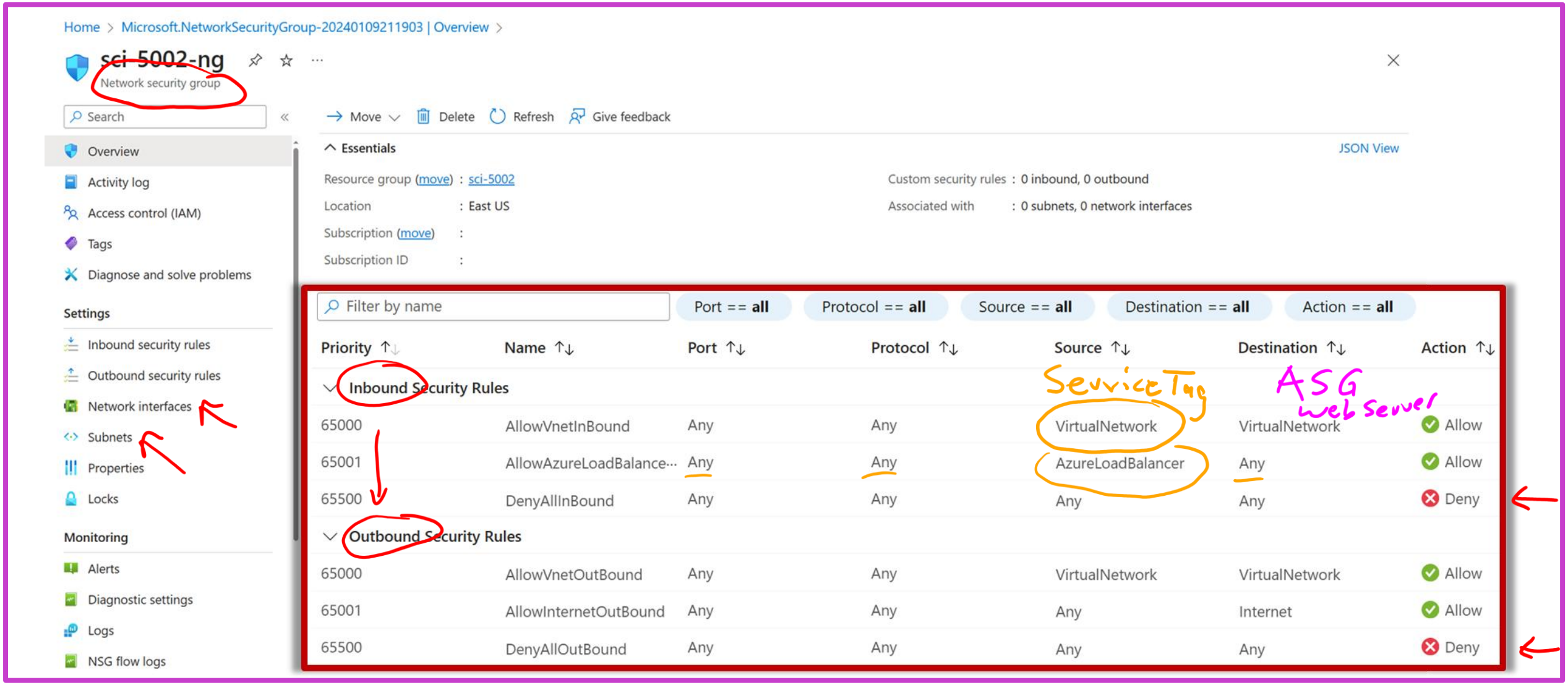


Azure Virtual Network is the fundamental building block for your private network in Azure.

- A virtual network enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks.

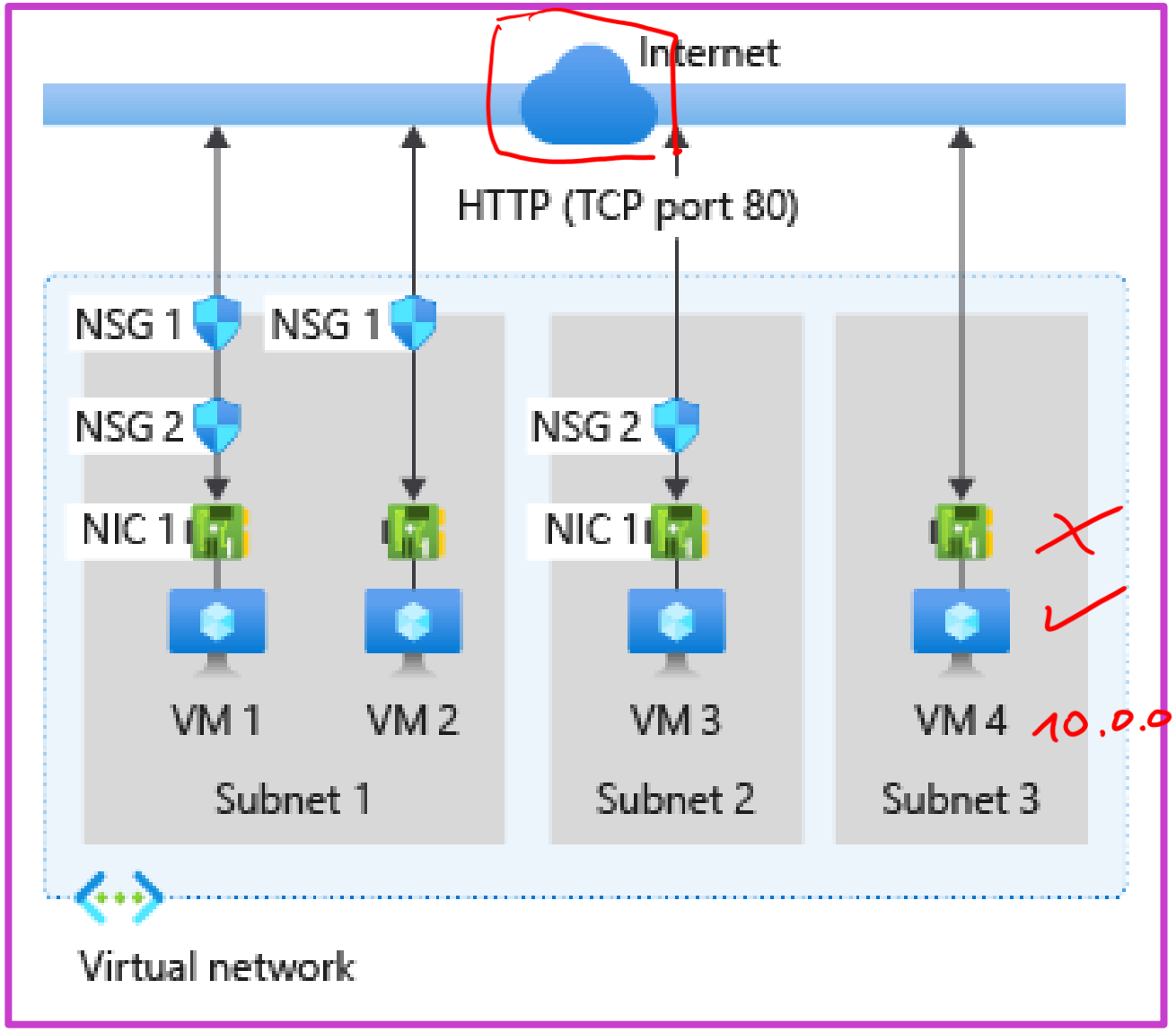
Vint Cerf TCP/IP

How network security groups filter network traffic



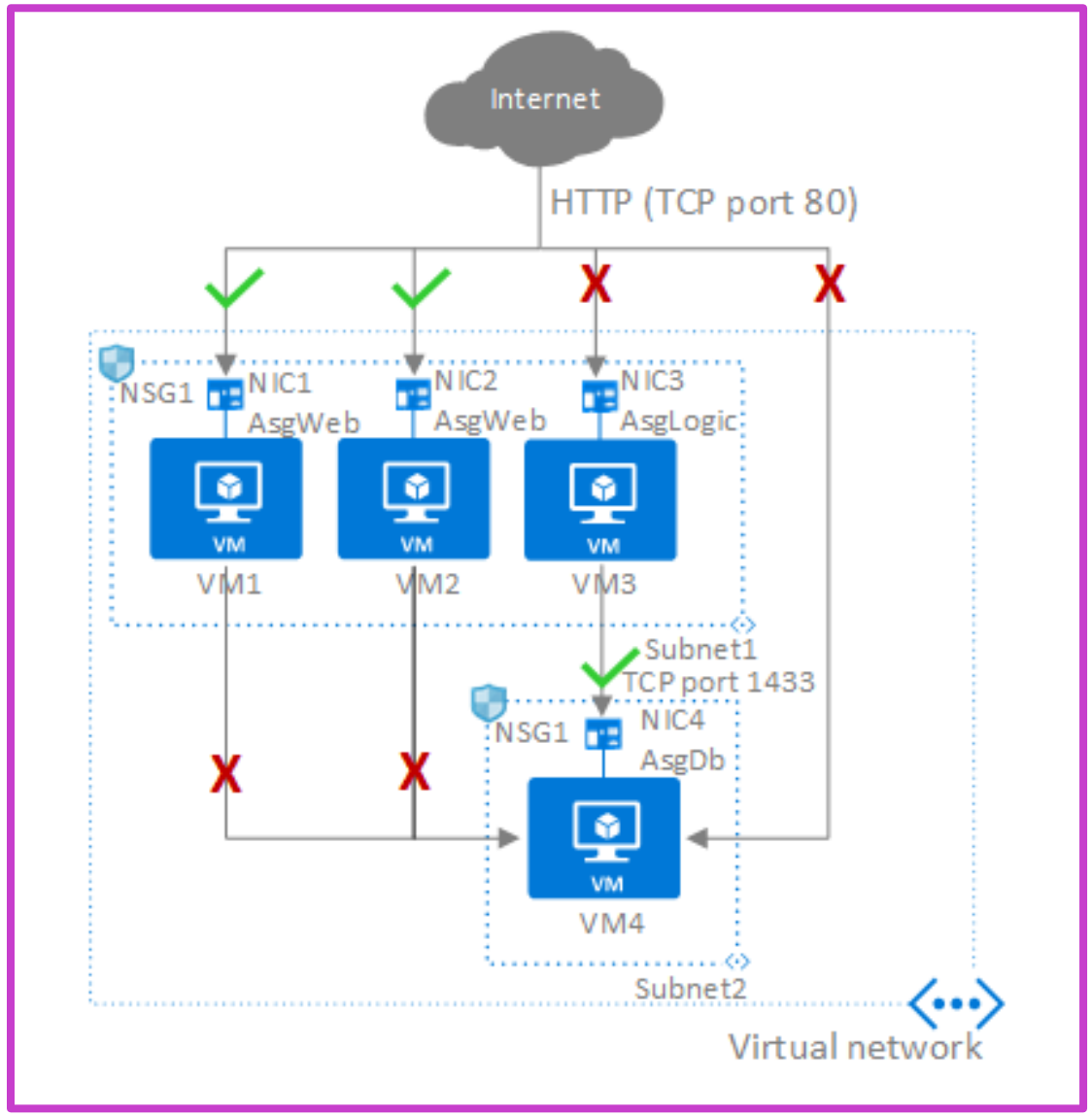
How network security groups filter network traffic (cont'd)

- Azure processes subnet-associated NSG rules first for inbound traffic, then network interface NSG rules; intra-subnet traffic included.
- Outbound traffic is evaluated by network interface NSG rules first, then subnet NSGs, impacting VMs differently based on their NSG associations.
- Intra-subnet traffic can be affected by NSG rules; Azure Network Watcher's IP flow verify helps determine if communication is allowed or denied.



Application security groups

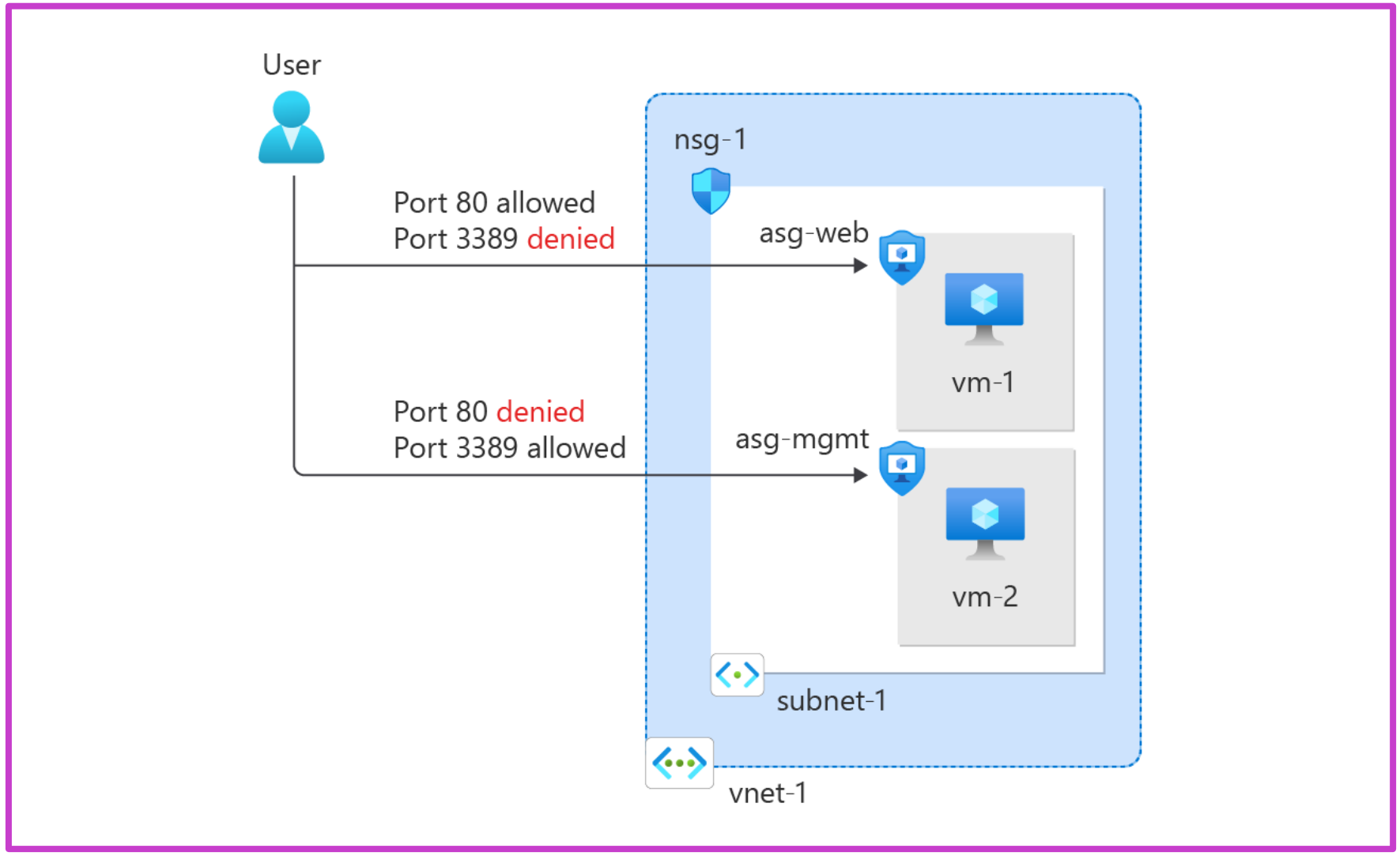
- Application security groups simplify network security for applications by grouping VMs, eliminating manual IP management and focusing on business logic.
- Network interfaces in application security groups apply specific rules; interfaces not in a group are unaffected, even if associated with the same NSG.
- Application security groups require all network interfaces to be in the same virtual network; cross-network group assignment is not allowed.



Exercise – Create a virtual network infrastructure

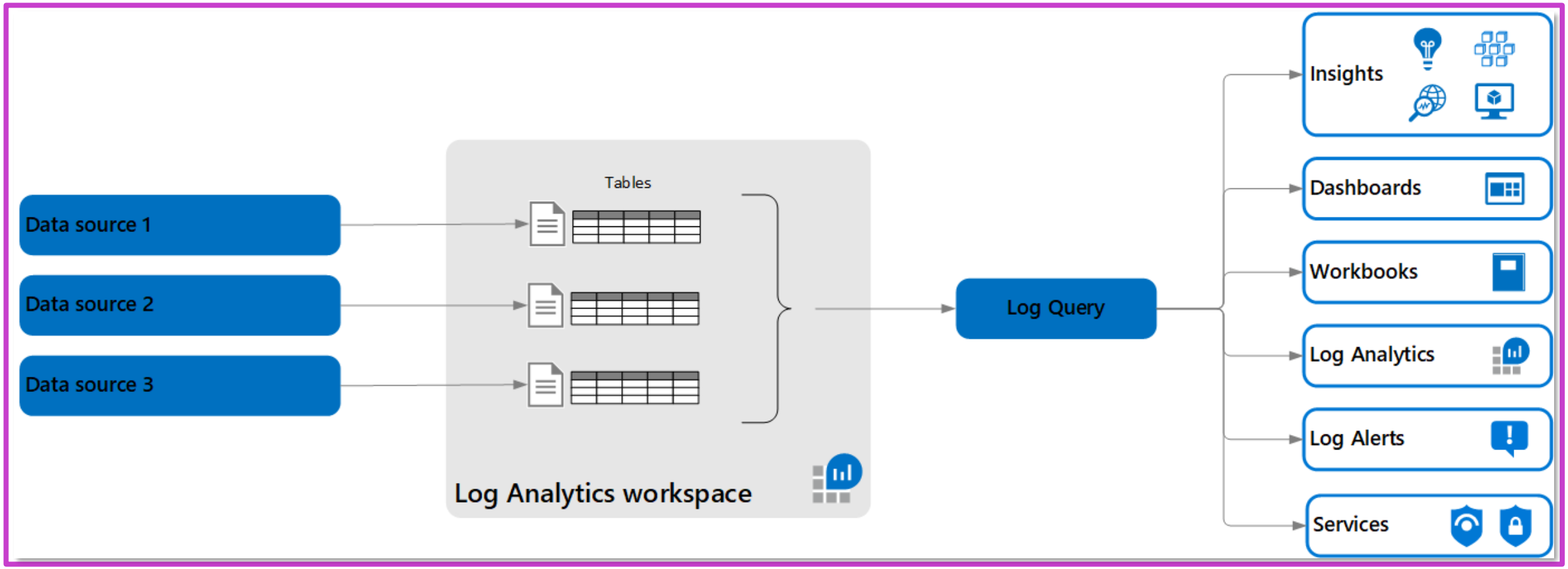
This exercise teaches students how to use a network security group to filter inbound and outbound network traffic to and from Azure resources in an Azure virtual network.

[Launch this Exercise in GitHub]



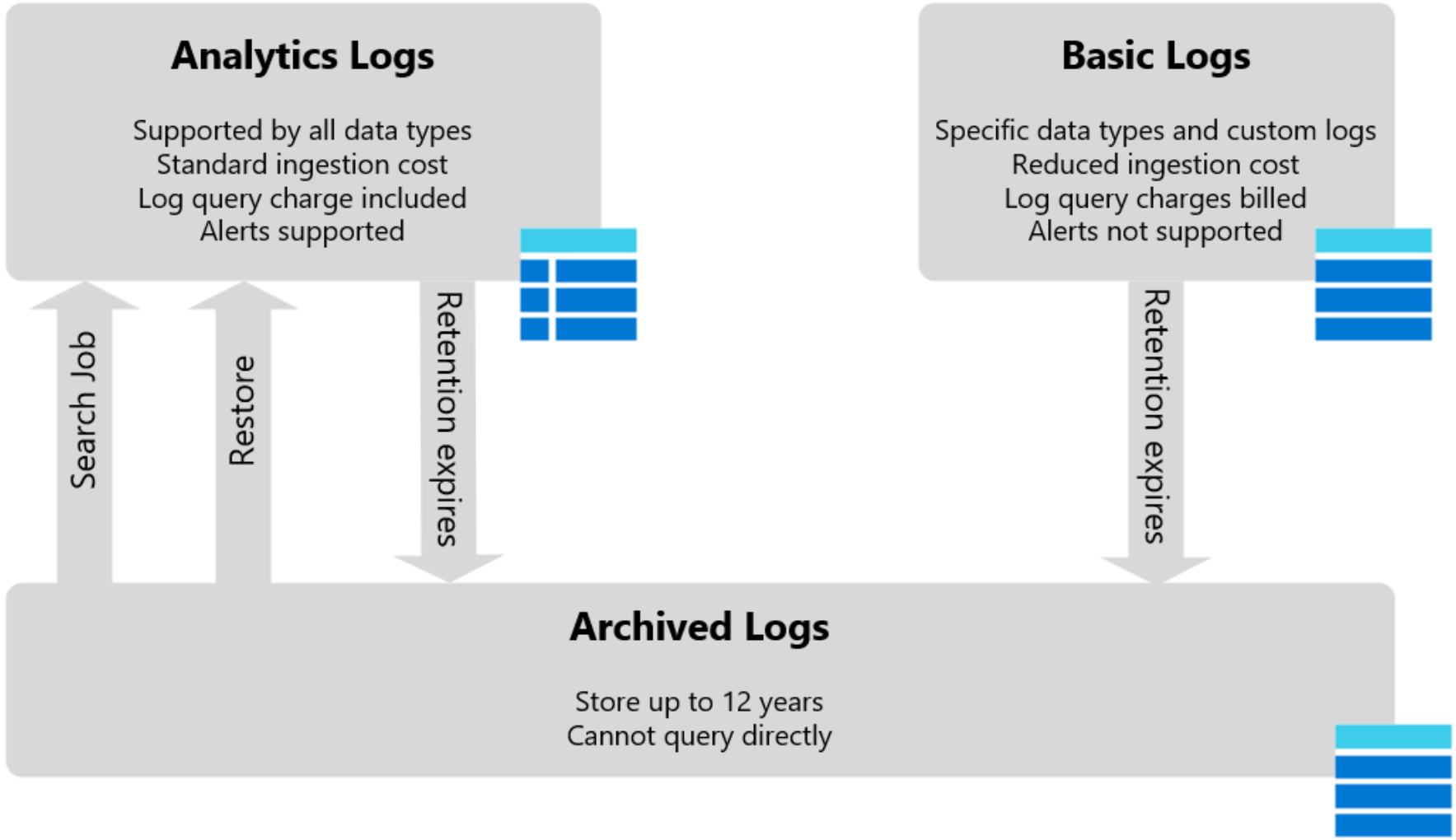
4/8 Create a Log Analytics workspace for Microsoft Defender for Cloud

Log Analytics workspace



- A Log Analytics workspace is a centralized, configurable environment for Azure Monitor log data, allowing data collection and retention management across multiple Azure services.

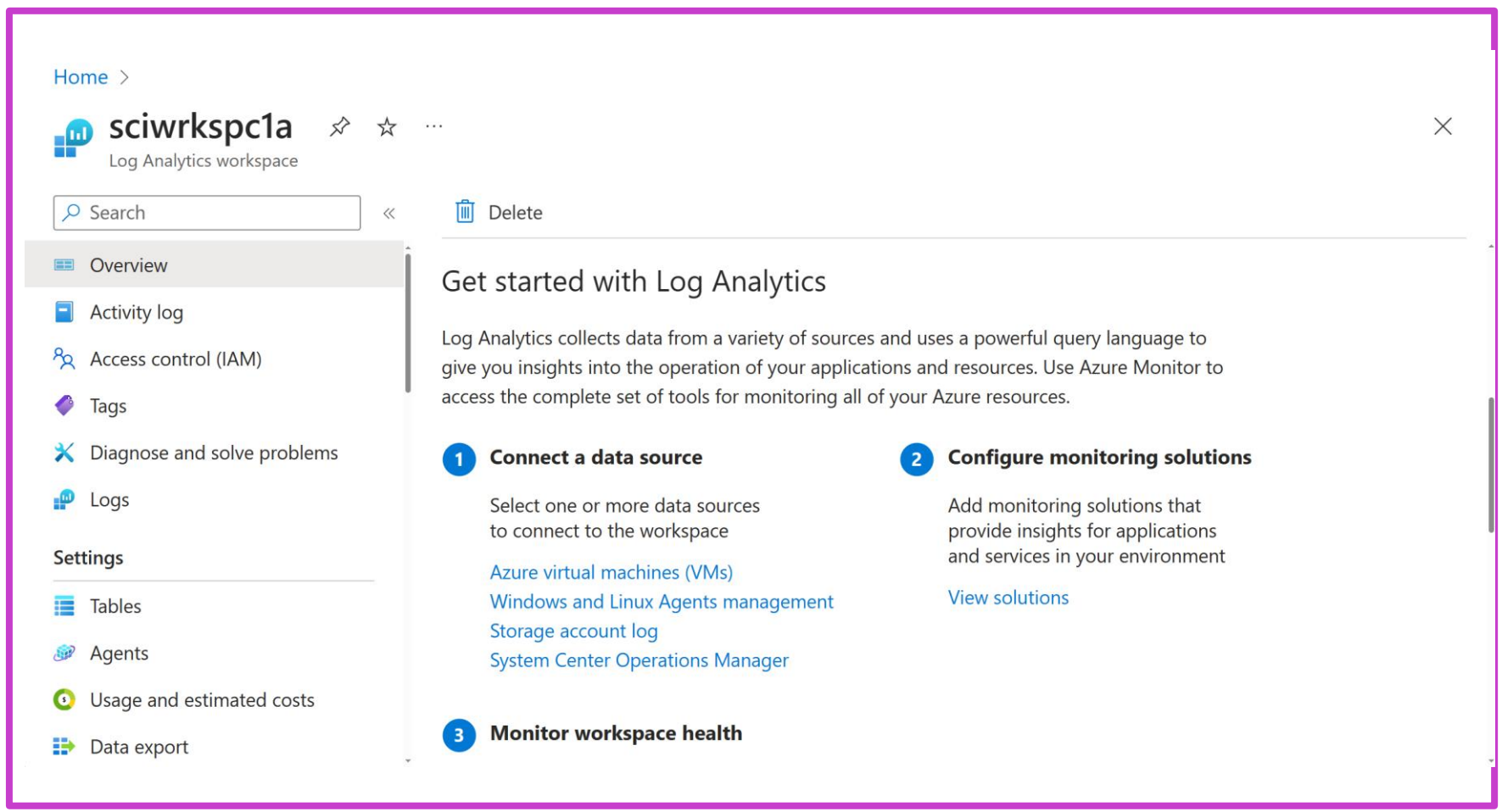
Data retention and archive



Exercise – Create a Log Analytics workspace for Microsoft Defender for Cloud

This exercise teaches students how to create a log analytics workspace to collect logs and data.

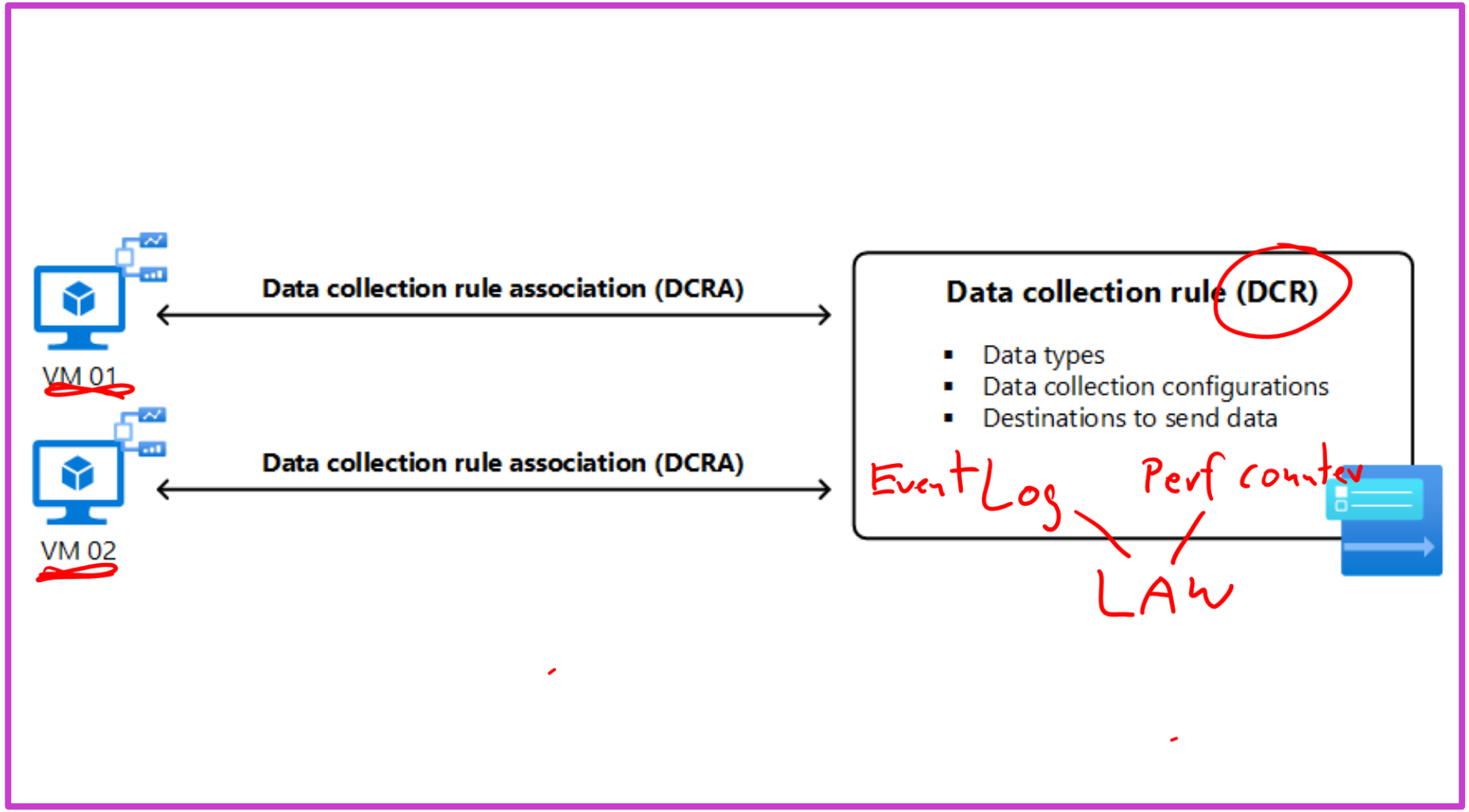
[Launch this Exercise in GitHub]



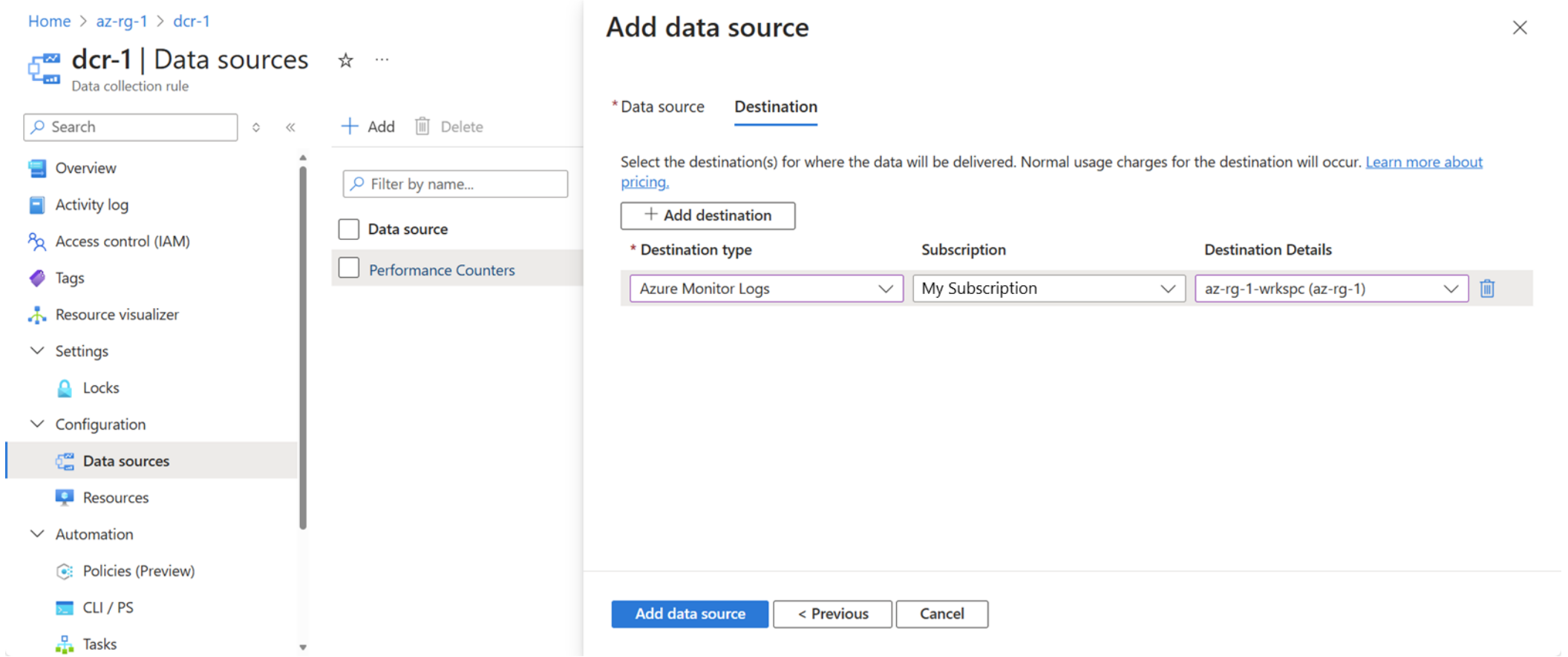
5/8 Collect guest operating system monitoring data from Azure and hybrid virtual machines using Azure Monitor

Deploy the Azure Monitor Agent

- Azure Monitor Agent gathers data from guest operating systems across Azure, hybrid, and on-premises environments.
- Data Collection Rules (DCRs) manage data types, transformations, and destinations for flexible monitoring.
- Supports insights and services like Microsoft Sentinel and Defender for Cloud for enhanced security and compliance.



Collect data with Azure Monitor Agent

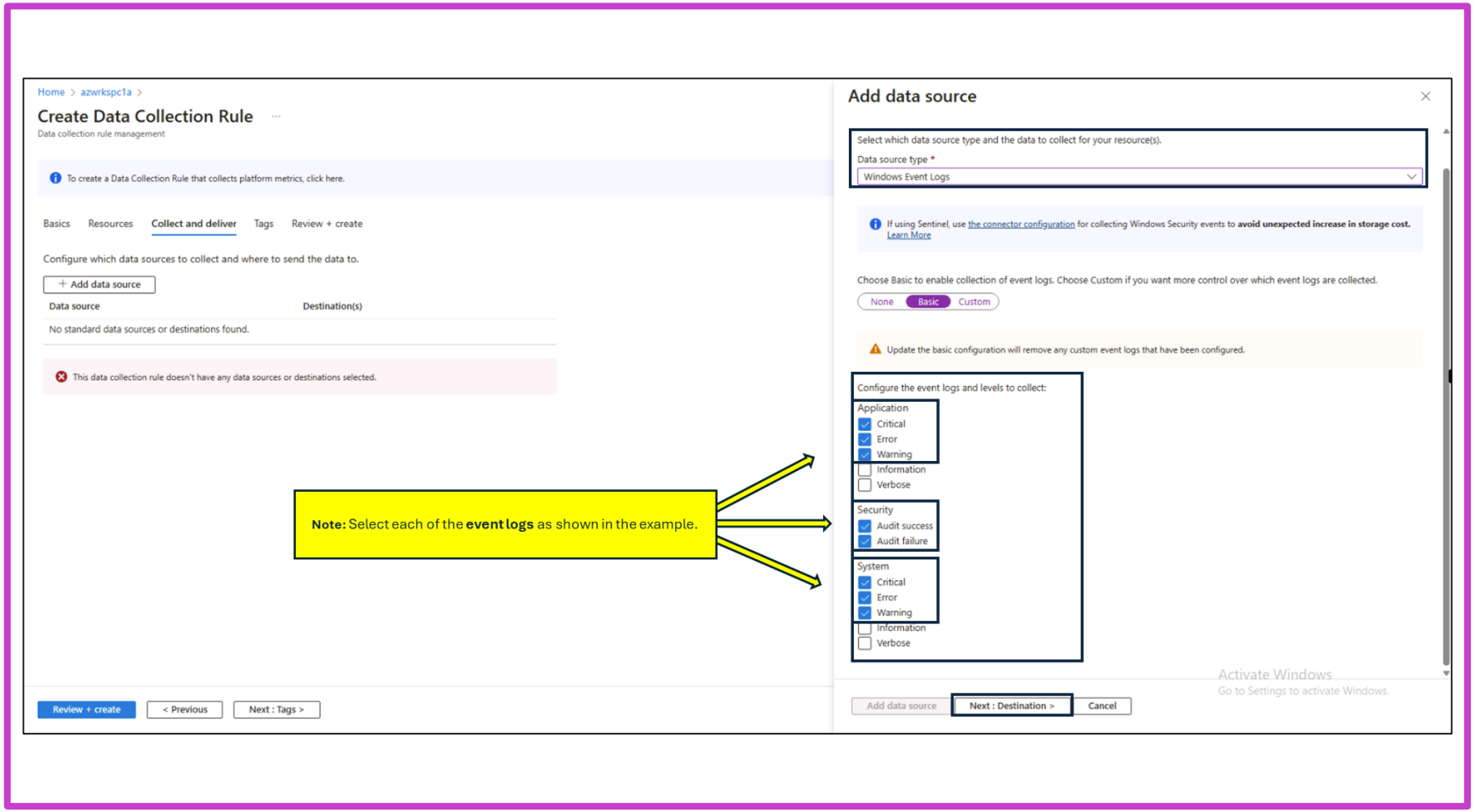


- Collects data from VMs, scale sets, and Arc-enabled servers.
- Uses Data Collection Rules (DCRs) to define and route data.
- Supports deployment via portal, CLI, PowerShell, or ARM templates.

Exercise – Create a data collection rule and install the Azure Monitor Agent

This exercise teaches students how to Create and define a Data Collection Rule and install the Azure Monitor Agent.

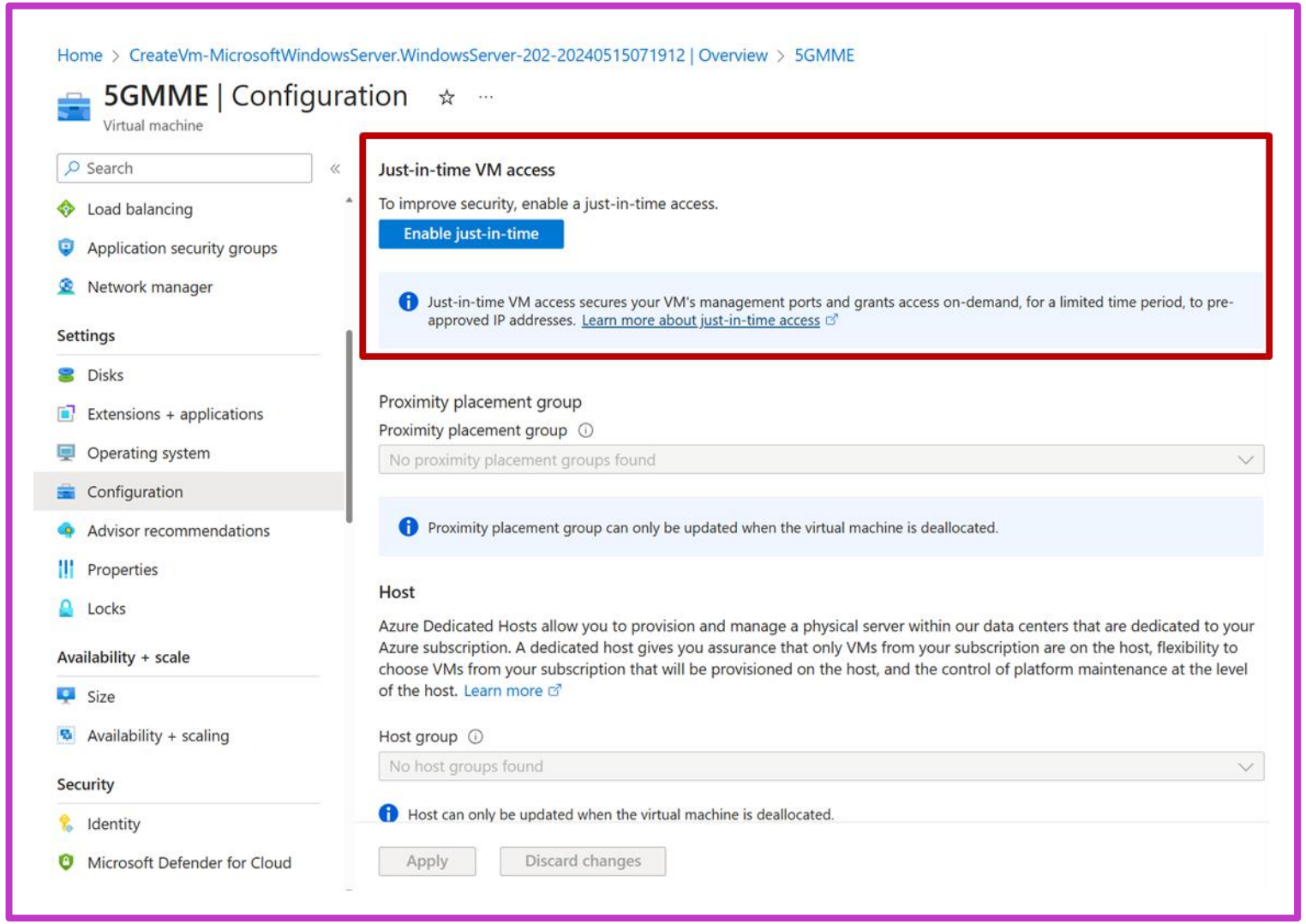
[Launch this Exercise in GitHub]



6/8 Explore just-in-time VM access

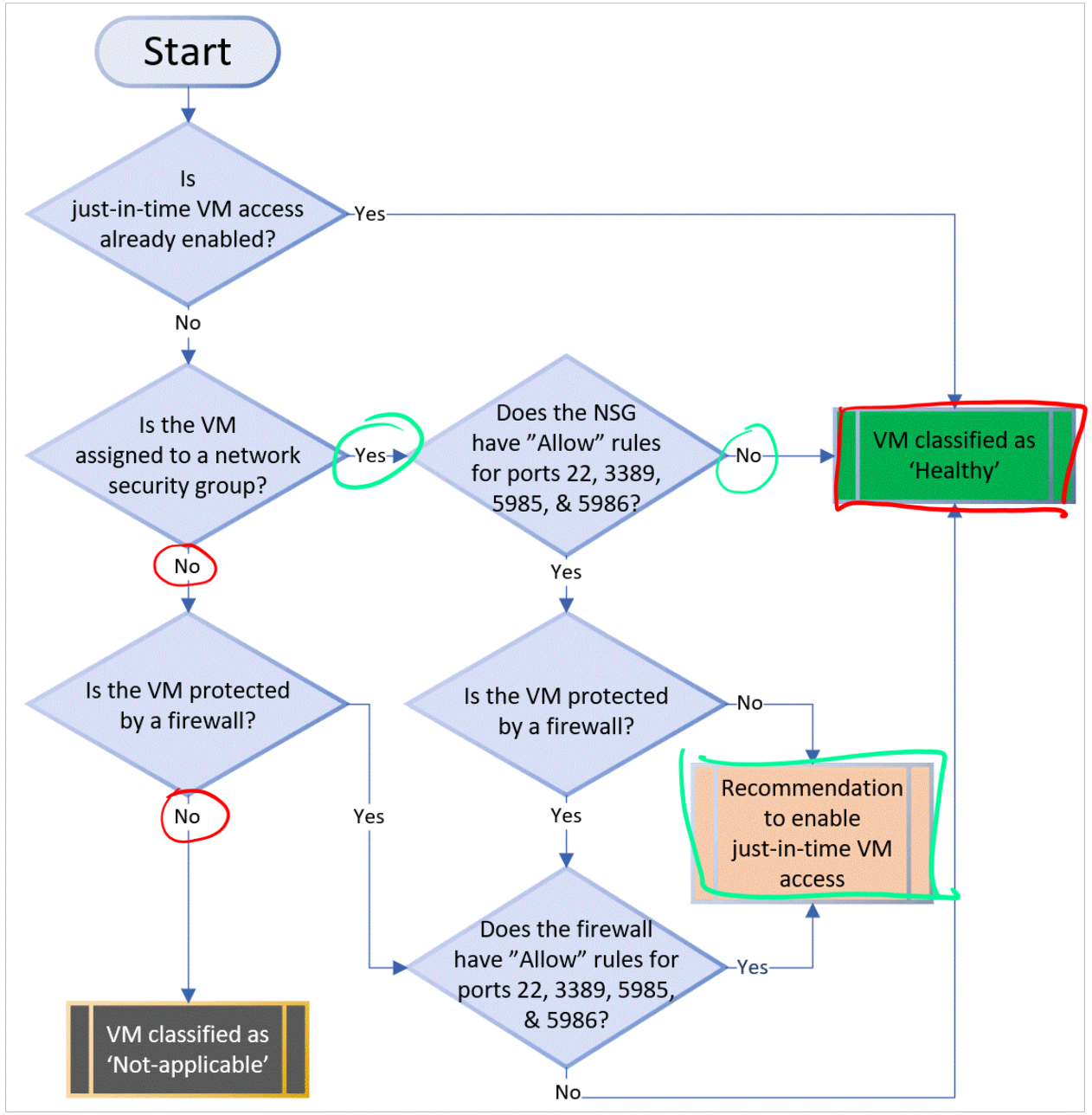
Understanding just-in-time VM access

- Open management ports on VMs are targets for attacks; successful breaches can lead to further resource compromises.
- JIT VM access in Defender for Cloud reduces attack surfaces by limiting open ports while allowing legitimate access when needed.
- JIT manages inbound traffic on Azure and AWS, ensuring security rules are prioritized and access is controlled and temporary.



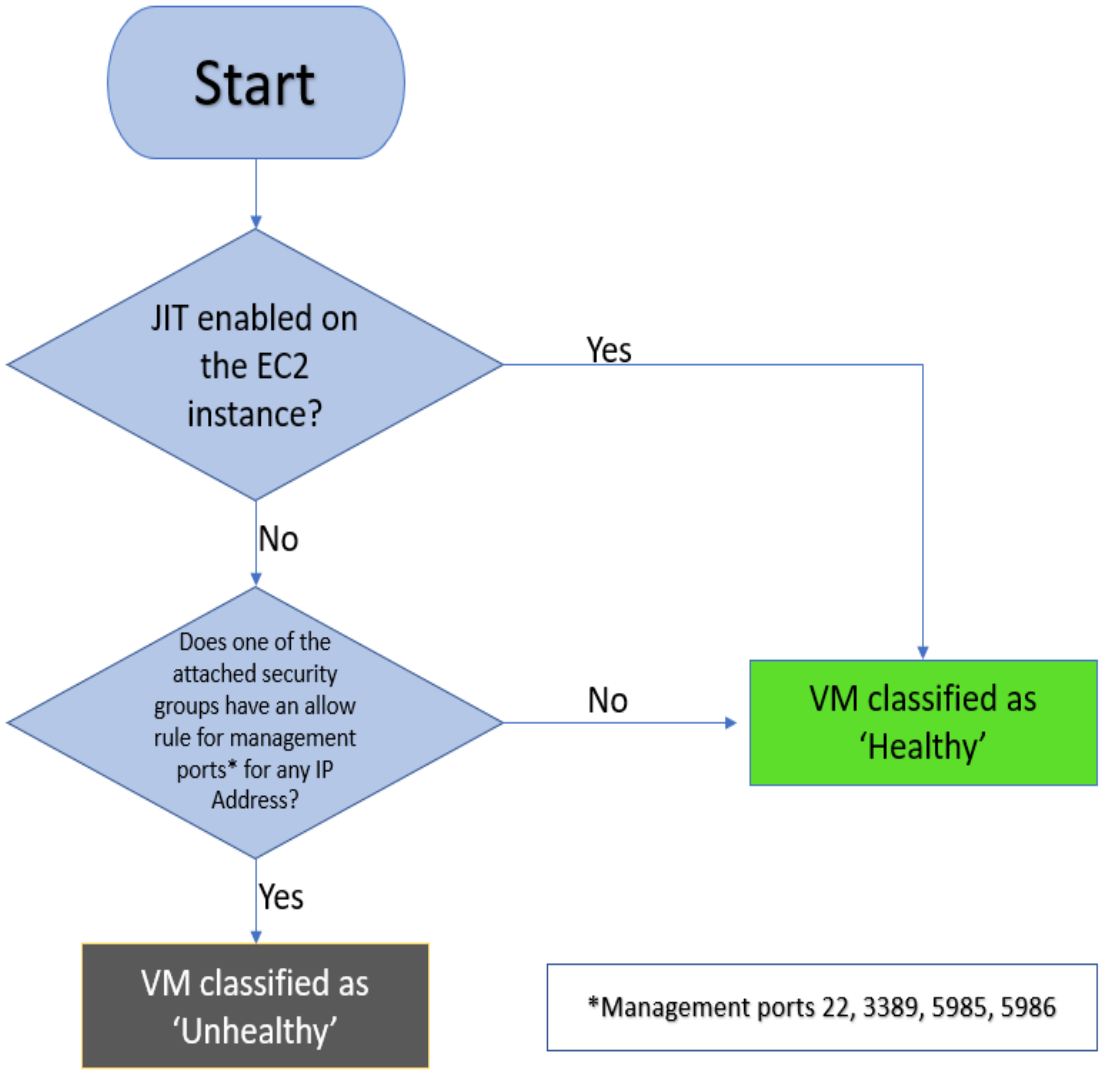
Just-in-time VM is enabled an Azure Virtual Machine

Example: Azure Virtual Machine



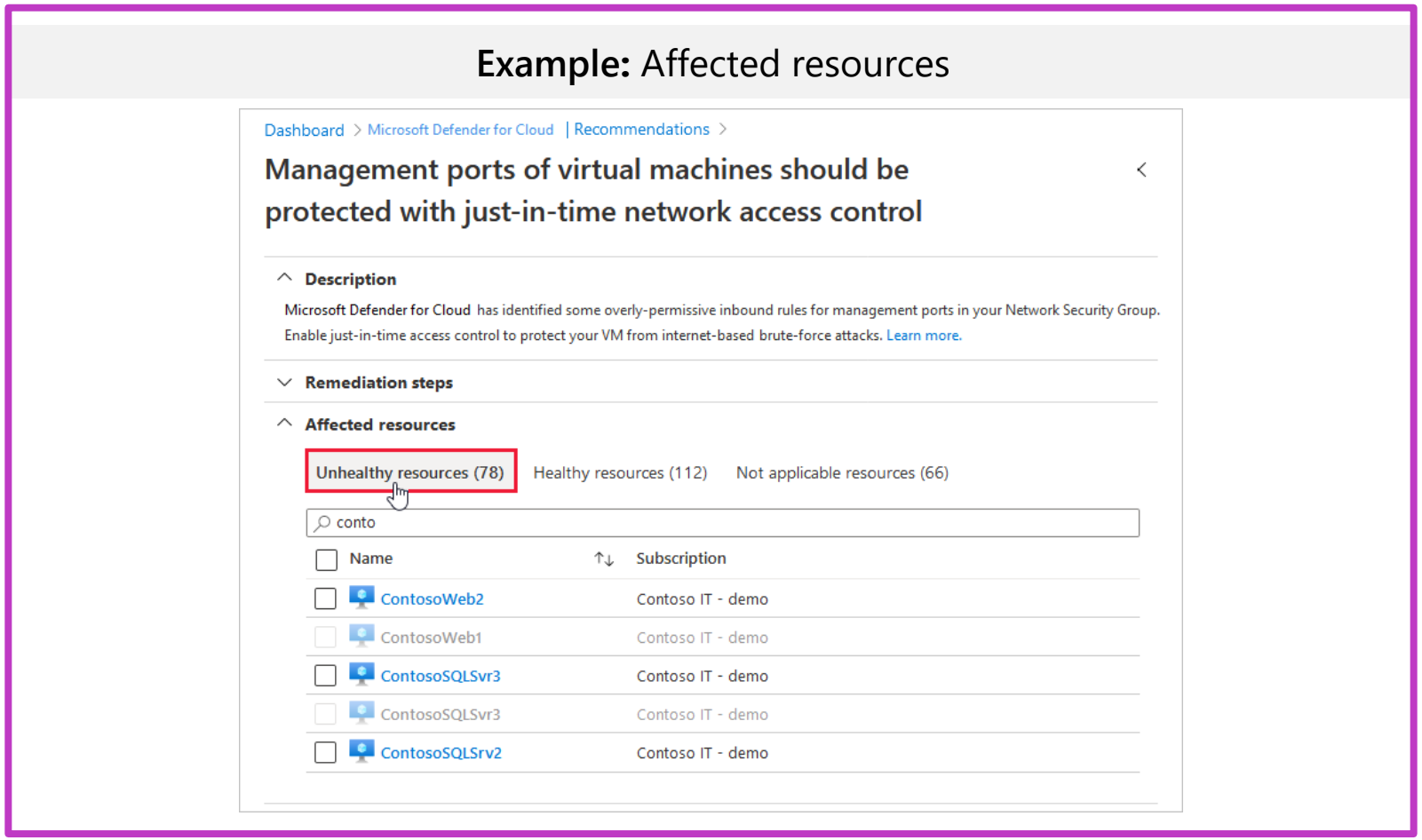
Just-in-time VM is enabled on the AWS EC2 Instance

Example: AWC EC2 Instance



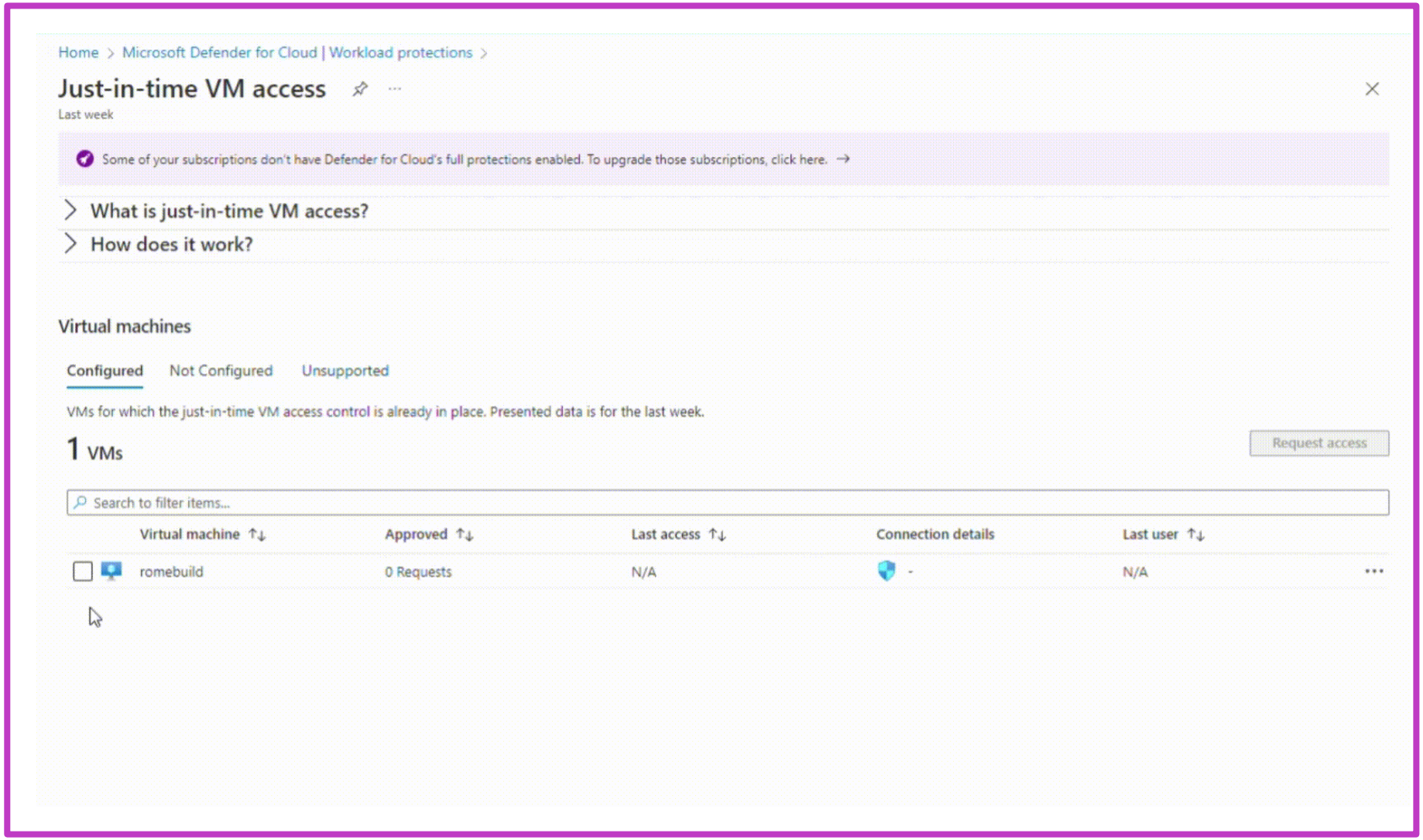
Added to the recommendation's Unhealthy resources tab

When Defender for Cloud finds a machine that can benefit from JIT, it adds that machine to the recommendation's Unhealthy resources tab.



Enable just-in-time access on VMs

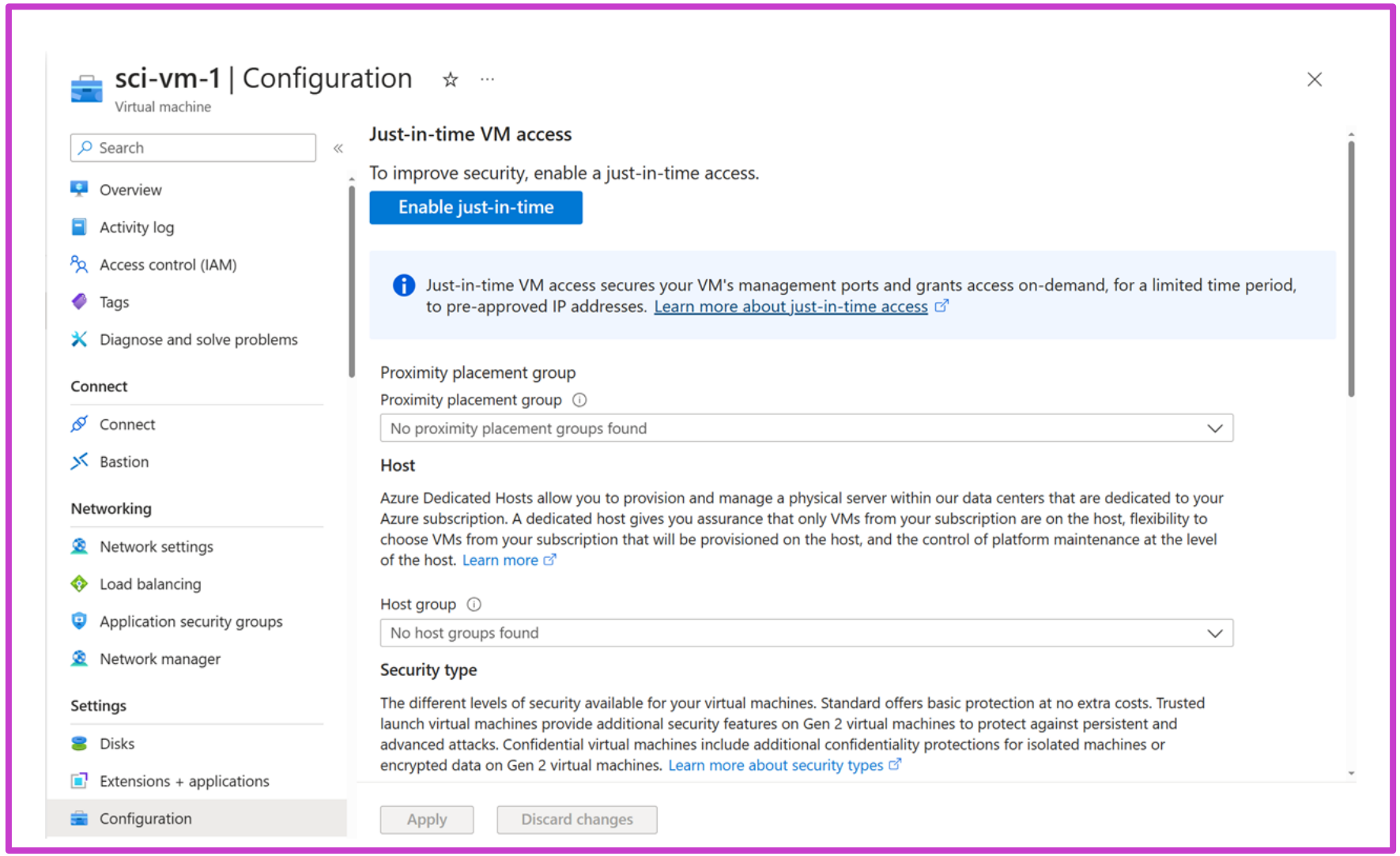
- Protect Azure VMs from unauthorized access using JIT in Defender for Cloud.
- Enable and manage JIT via Defender for Cloud, Azure portal, PowerShell, or REST API.
- Prerequisites: Microsoft Defender for Servers Plan 2, Reader/Security Reader roles.

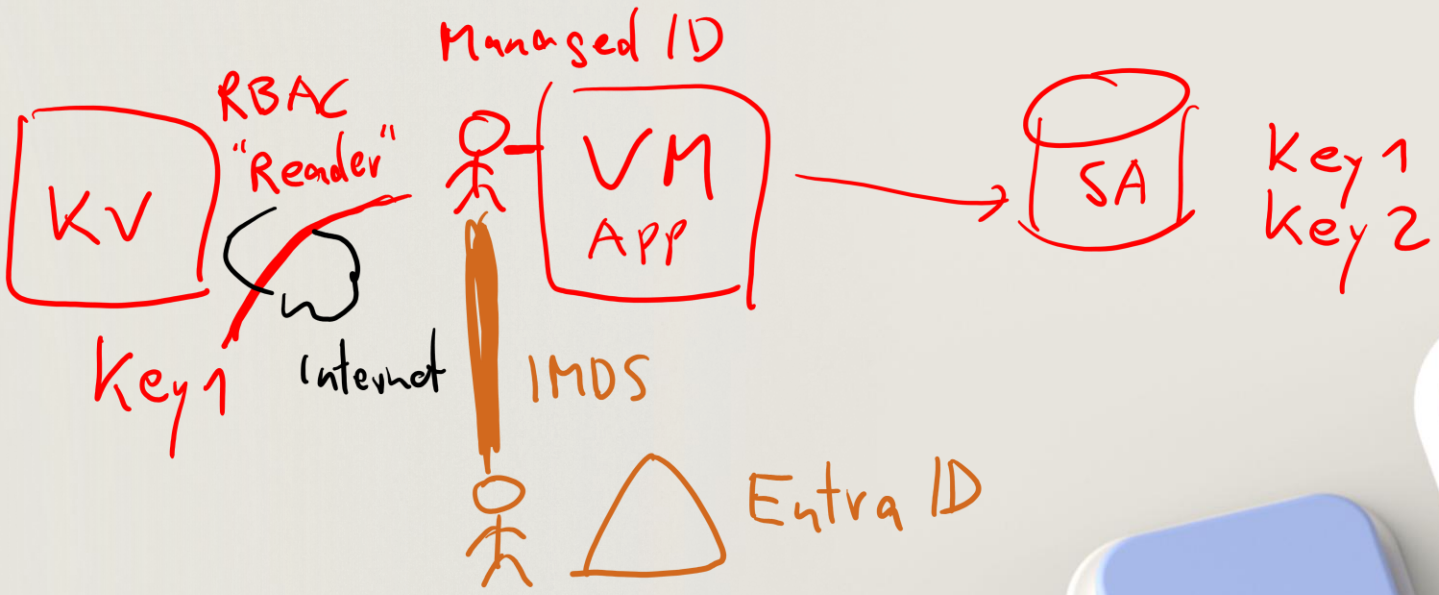


Exercise – Enable just-in-time access on VMs

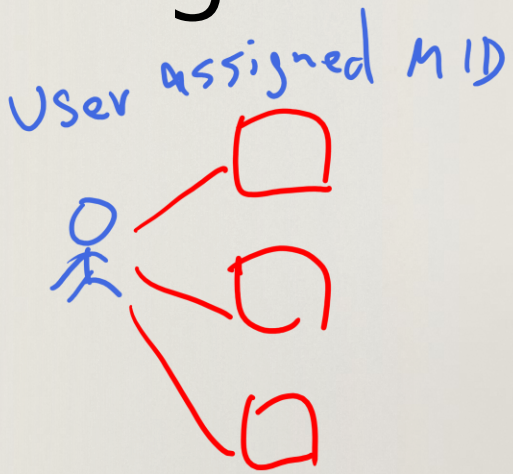
This exercise teaches students how to use Microsoft Defender for Cloud's just-in-time (JIT) access to protect your Azure virtual machines (VMs) from unauthorized network access.

[Launch this Exercise in GitHub]





7/8 Configure Azure Key Vault networking settings



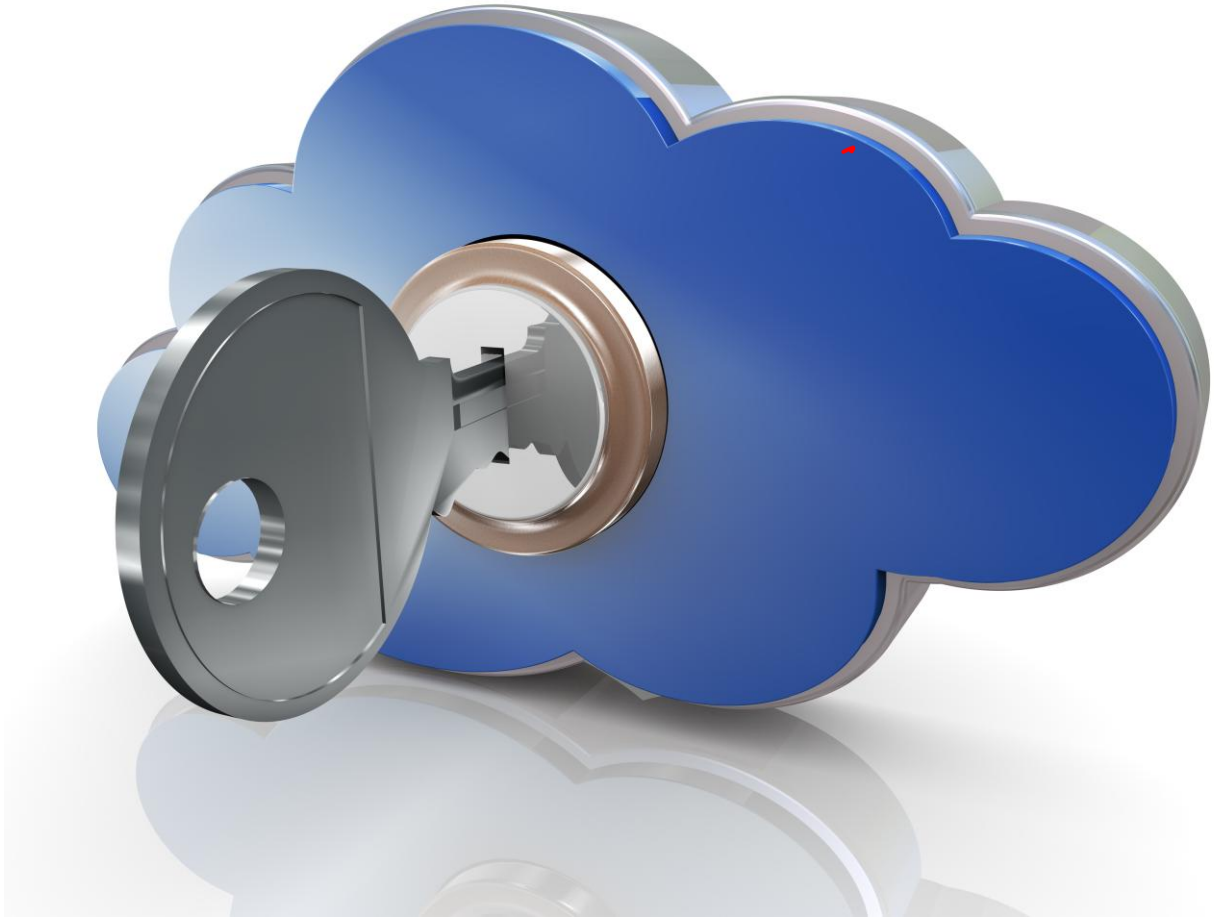
Azure Key Vault basic concepts

RSA 2048 Bit
3 · 5 = 15
15 = ?

- Azure Key Vault: A cloud service for secure storage and access of secrets like API keys, passwords, and certificates. Supports vaults and hardware security module (HSM)-backed containers.

- Roles and Tenants: Involves tenant organizations, vault owners/administrators managing access and key lifecycles, and vault consumers using granted permissions.

- Authentication and Security: Key Vault requires authentication, recommends managed identities for Azure resources, enforces transport layer security (TLS) for data transit security, and supports Perfect Forward Secrecy.



Best practices for Azure Key Vault

- Use Separate Key Vaults: Recommended to use a vault per application, environment, and region to prevent secret sharing and reduce breach impact.

- Control Access: Secure key vaults by restricting access through role-based control, least privilege access policies, firewalls, and data protection features.

- Backup and Multitenancy: Implement logging, alerts, and purge protection for security. For multitenant solutions, backup vault objects in Software as a Service (SaaS) architectures.

Azure Key Vault network security

- Network Security: Restrict vault access by IP address or virtual network, using Azure Key Vault service endpoints and Azure Private Link Service.
- TLS and HTTPS: Key Vault employs TLS and HTTPS for secure communication, with the client participating in TLS negotiation to enforce the latest protocol version.
- Access and Authentication: Control Key Vault access through management and data planes using Microsoft Entra ID, with options for application-only, user-only, or application-plus-user access.

Configure Azure Key Vault firewalls and virtual networks

- Default Firewall Setting: Newly created Azure Key Vaults have the firewall disabled, allowing all applications and Azure services to access it.

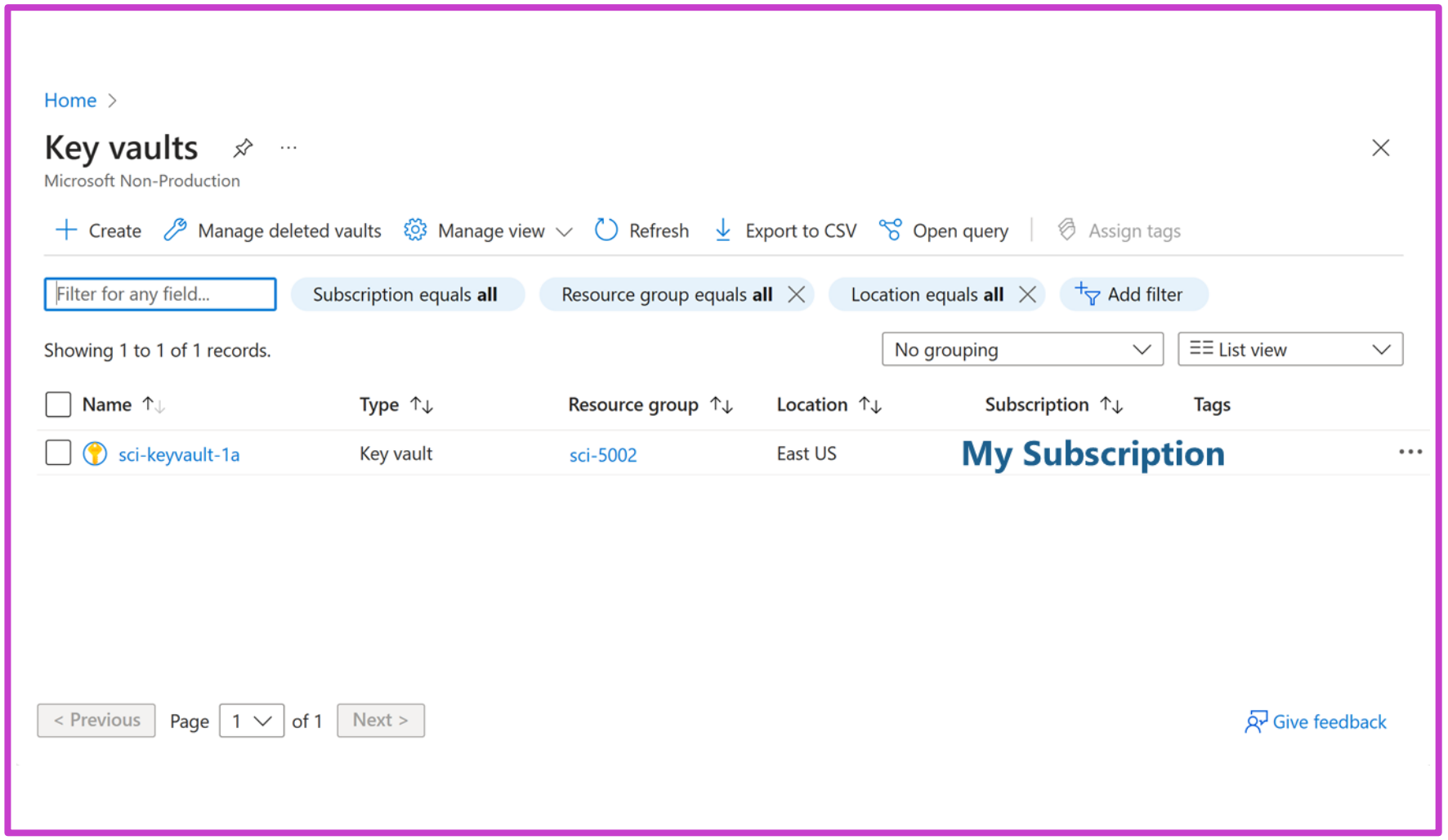
- Access Restrictions: Despite the disabled firewall, operations on the key vault require Microsoft Entra authentication.

- Access Policy Permissions: Key vault secures secrets, keys, and certificates with specific access policy permissions, even with the firewall turned off.

Exercise – Configure Key Vault networking settings

This exercise teaches students how to use the Azure portal to configure the Azure Key Vault networking settings to work with other applications and Azure services.

[Launch this Exercise in GitHub]

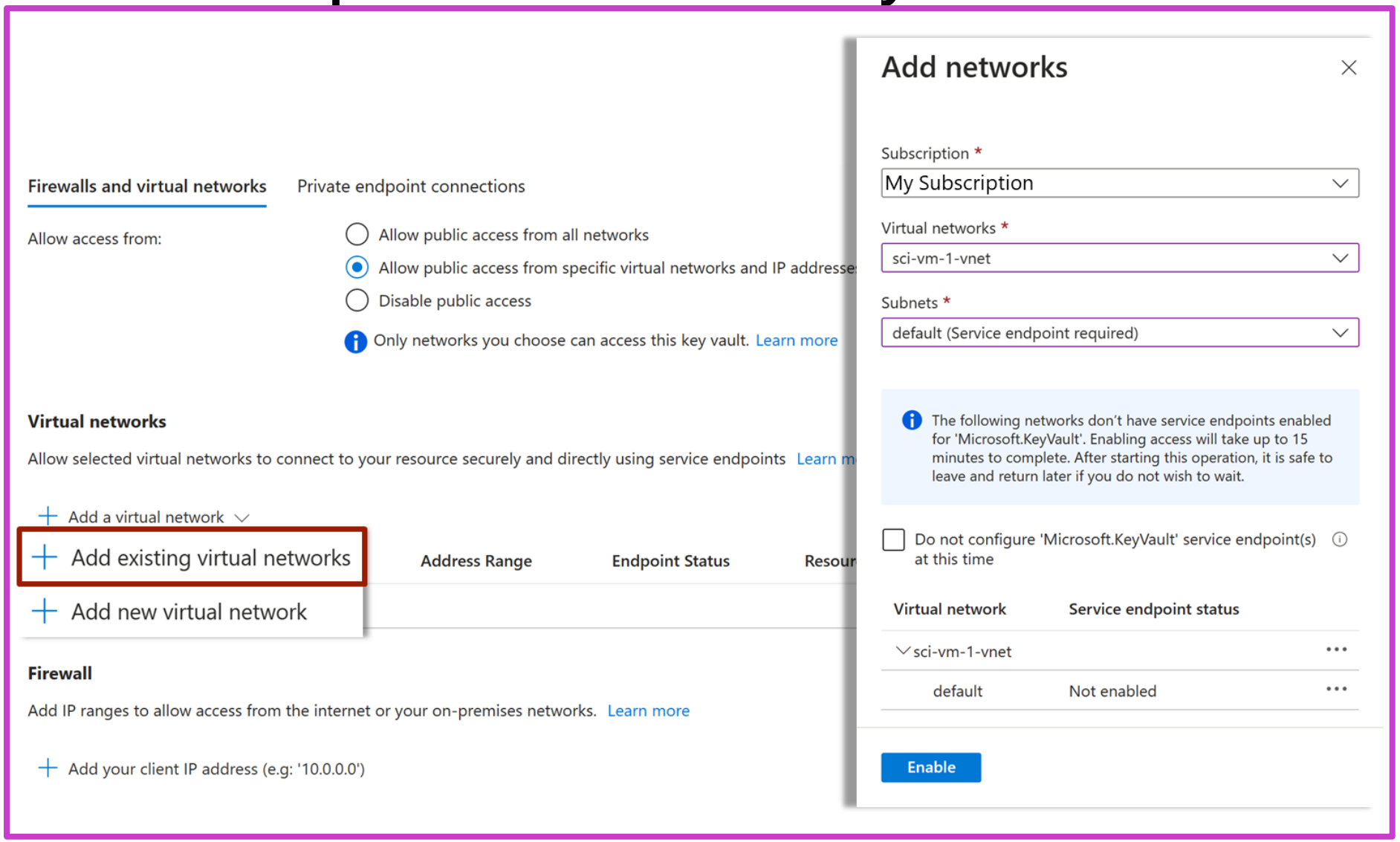


Azure Key Vault soft delete

- Soft-Delete Feature: Key Vault's soft-delete allows recovery of deleted vaults and objects (keys, secrets, certificates) for 7-90 days, with 90 days as the default.
- Purge Protection and Recovery: Purge protection is optional, preventing permanent deletion until the retention period ends. Recovery requires specific permissions and doesn't restore integrated services.
- Billing and Application Implications: Purge and recovery actions are billed; HSM-keys incur charges. Soft-delete, by default, affects application logic for reusing names of deleted vaults/objects.

Virtual network service endpoints for Azure Key Vault

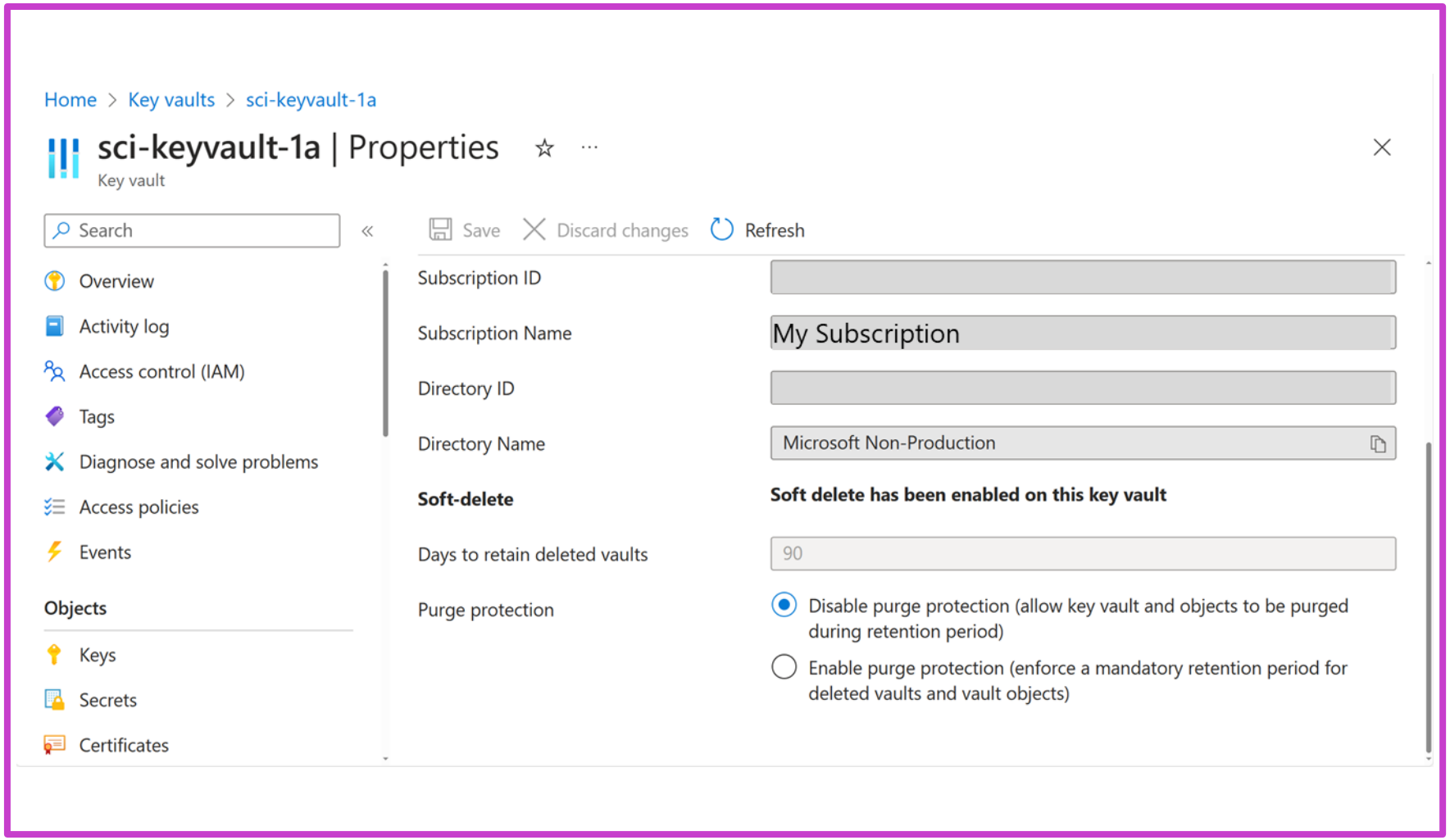
- Access Control: Restrict Key Vault access to specific virtual networks and IP ranges; outsiders denied unless allowed.
- Firewall Exceptions: Trusted Microsoft services can bypass firewall restrictions, still requiring Microsoft Entra token and access policies.
- Operational Scope: Firewall and network rules affect Key Vault's data plane only, not control plane operations like creating or modifying vaults.



Exercise – Perform soft-delete and purge protection key vault recovery

This exercise teaches students how to use purge protection to prevent the deletion of your key vault, keys, secrets, and certificates by a malicious insider.

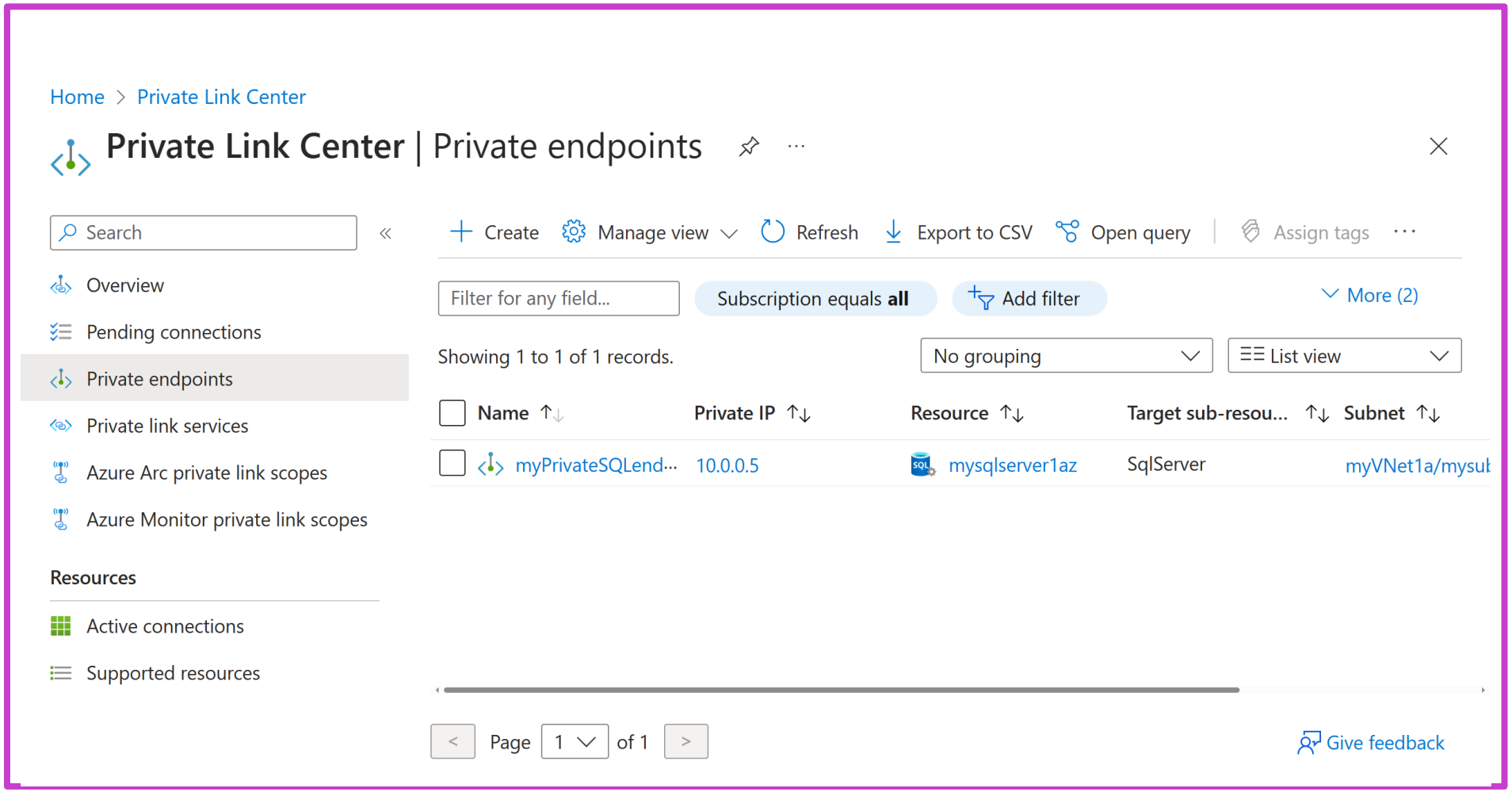
[Launch this Exercise in GitHub]



8/8 Connect an Azure SQL server using an Azure Private Endpoint using the Azure portal

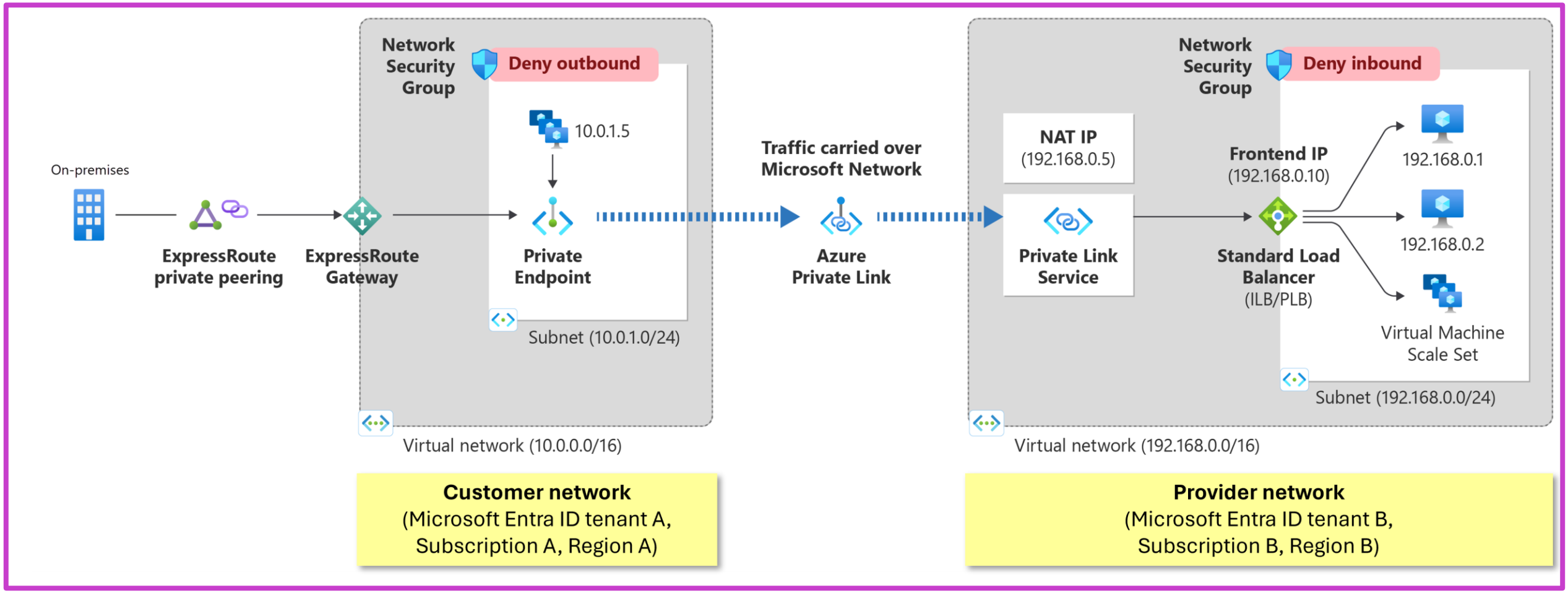
Azure Private Endpoint

- Private Endpoint Function: Connects virtual networks to Azure services securely using Azure Private Link.
- Deployment Considerations: Supports one-way connections, maintains static IP, allows multiple endpoints across regions/subscriptions.
- Network Security Features: Secures traffic, supports network policies like *UDRs, NSGs, and *ASGs.



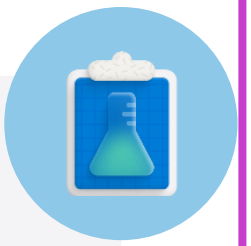
*User-Defined Routes *Network Security Groups *Application Security Groups

Azure Private Link Service



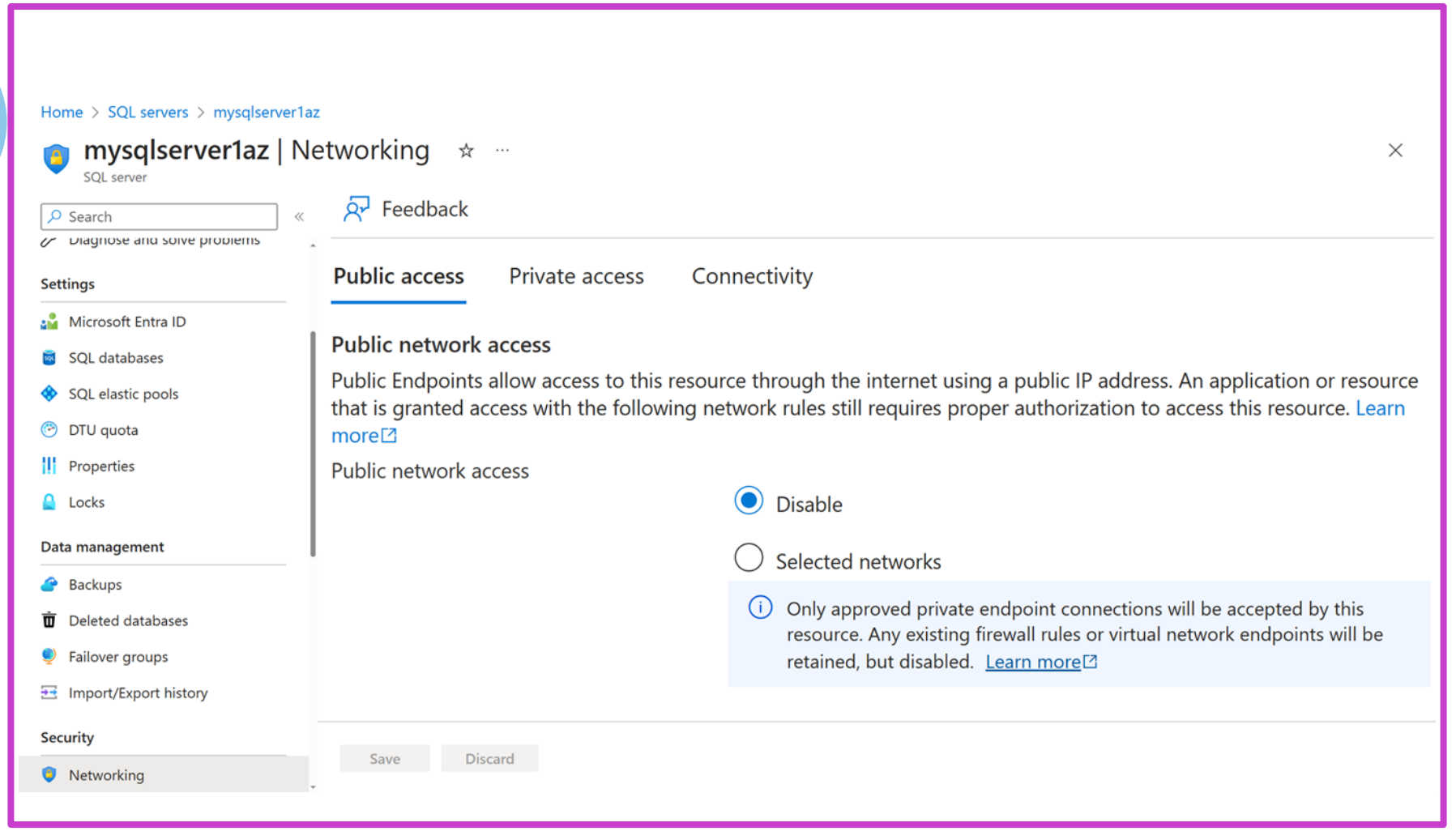
- Azure Private Link: Facilitates secure, private access to Azure Platform-as-a-Service (PaaS) and partner services globally, reducing public internet exposure and data leakage risks, enhancing connectivity and security.

Exercise – Connect to an Azure SQL server using an Azure Private Endpoint using the Azure portal



This exercise teaches students how to enable Azure resources, like virtual machines (VMs), to privately and securely communicate with Private Link resources such as Azure SQL server.

[Launch this Exercise in GitHub]



Knowledge check

1 **What is the primary function of a Network Security Group (NSG) in Azure?**

- ☐ To provide data encryption services.
- ☐ To automate network configuration.
- ☐ To filter network traffic based on IP address, port, and protocol.

2 **What is the first step in creating a Log Analytics workspace for Microsoft Defender for Cloud?**

- ☐ Configuring Microsoft Entra ID
- ☐ Navigating to the Microsoft Defender for Cloud in the Azure portal and selecting “Create workspace.”
- ☐ Open Azure Monitor and select Alerts to start workspace creation.

3 **What is a critical step in connecting an Azure SQL server using an Azure Private Endpoint?**

- ☐ Installing a local SQL server instance.
- ☐ Setting up an Azure Private Endpoint in the networking settings of the SQL server.
- ☐ Configuring a public IP address for the SQL server.

Knowledge check

1 **What is the primary function of a Network Security Group (NSG) in Azure?**

- ☐ To provide data encryption services.
- ☐ To automate network configuration.
- ☑ To filter network traffic based on IP address, port, and protocol.

2 **What is the first step in creating a Log Analytics workspace for Microsoft Defender for Cloud?**

- ☐ Configuring Microsoft Entra ID
- ☑ Navigating to the Microsoft Defender for Cloud in the Azure portal and selecting “Create workspace.”
- ☐ Open Azure Monitor and select Alerts to start workspace creation.

3 **What is a critical step in connecting an Azure SQL server using an Azure Private Endpoint?**

- ☐ Installing a local SQL server instance.
- ☑ Setting up an Azure Private Endpoint in the networking settings of the SQL server.
- ☐ Configuring a public IP address for the SQL server.

Learning Path Recap

In this learning path, we:

- Enhanced cloud security posture with Defender for Cloud.
- Investigated and remediated security issues.
- Enabled and configured Defender for Cloud on Azure.
- Managed network traffic and access controls.

End of presentation