

Azure Secure & Defend

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

Microsoft Applied Skills





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



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

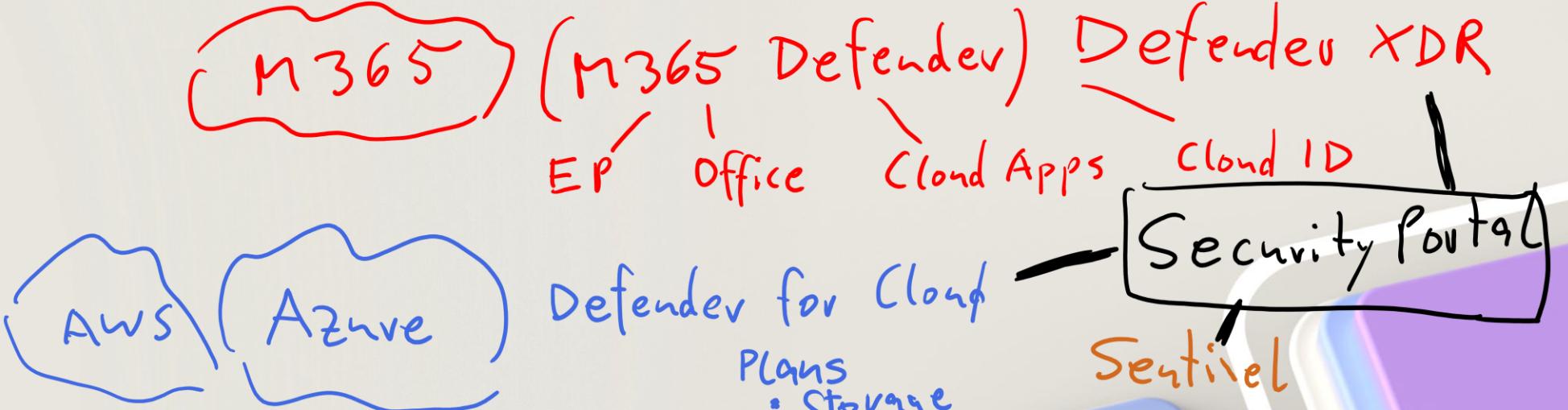
Introduction

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

-
- The diagram illustrates a network architecture. A 'Bastion Host' (red box) has a 'Public IP' (blue dot) and port 443. It connects via RDP to a 'VM' (red box) with IP 10.0.0.4. The 'VM' also connects via SSH to another 'VM' (red box) with IP 10.0.0.5. This second 'VM' is located in a 'vNet Subnet' (red box) with IP range 10.0.0.0/24. A 'Key Vault' icon is connected to the 'VM' at IP 10.0.0.5. A 'Public IP' (blue dot) is associated with the 'vNet Subnet'. A red bracket labeled 'AzureBastionSubnet' covers the 'Bastion Host' and the first 'VM'. A red circle labeled 'NSG ASG' covers the 'vNet Subnet' and the second 'VM'. A red circle labeled 'ARC' covers the 'Bastion Host' and the 'vNet Subnet'. A red circle labeled 'JIT' covers the 'vNet Subnet' and the 'Key Vault'.
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
LAW
 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
ARC
 6. Explore just-in-time VM access
JIT
 7. Configure Azure Key Vault networking settings
 8. Connect an Azure SQL server using an Azure Private Endpoint using the Azure portal



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.

The screenshot shows the Microsoft Defender for Cloud Regulatory compliance dashboard. The left sidebar lists various security categories: General (Overview, Getting started, Recommendations, Attack path analysis, Security alerts, Inventory, Cloud Security Explorer, Workbooks, Community, Diagnose and solve problems), Cloud Security (Security posture, Regulatory compliance, Workload protections, Data security, Firewall Manager, DevOps security). The 'Regulatory compliance' section is currently selected. The main content area displays the 'Microsoft cloud security benchmark CIS Azure Foundations v1.4.0'. It includes a note about customizing standards, the benchmark title, and a statement about its nature. Below this, it says 'Microsoft cloud security benchmark is applied to the subscription My Subscription' and shows an unchecked checkbox for 'Expand all compliance controls'. A section titled 'NS. Network Security' is expanded, showing a control for 'NS-1. Establish network segmentation boundaries' with 'Control details' (MS, C) and five items under 'Automated assessments - Azure': 'Adaptive network hardening recommendations should be applied on interne' (Azure resources, 0 of 0, green bar), 'Subnets should be associated with a network security group' (Azure resources, 0 of 0, green bar), 'Non-internet-facing virtual machines should be protected with network secu' (Azure resources, 0 of 0, green bar), 'Internet-facing virtual machines should be protected with network security g' (Azure resources, 0 of 0, green bar), and 'All network ports should be restricted on network security groups associated' (Azure resources, 0 of 0, green bar). The message at the bottom says 'Showing 1 - 5 of 5 results.'

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.

The screenshot shows the Microsoft Defender for Cloud | Regulatory compliance dashboard. The left sidebar includes links for General (Overview, Getting started, Recommendations, Attack path analysis, Security alerts, Inventory, Cloud Security Explorer, Workbooks, Community, Diagnose and solve problems), Cloud Security (Security posture, Regulatory compliance, Workload protections, Data security, Firewall Manager, DevOps security), and a search bar. The main content area displays a list of findings under the 'DP. Data Protection' section, each with a 'Control details' link and MS/C icons. A red box highlights the first four items: DP-1, DP-2, DP-3, and DP-4. Below this, there are two tables: 'Automated assessments - Azure' and 'Automated assessments - AWS'. The Azure table lists findings for Virtual machines, Windows virtual machines, Azure SQL Managed Instance, Azure SQL Database, and Azure Database for PostgreSQL. The AWS table lists a finding for Amazon Elasticsearch Service domains. Each row includes columns for Resource type, Failed resources, and Resource compliance status (indicated by a progress bar).

Resource type	Failed resources	Resource compliance status
Virtual machines	1 of 1	<div style="width: 20%;"></div>
Virtual machines	1 of 1	<div style="width: 20%;"></div>
Azure resources	0 of 0	<div style="width: 100%;"></div>
Azure resources	0 of 0	<div style="width: 100%;"></div>
Azure resources	0 of 0	<div style="width: 100%;"></div>
Resource type	Failed resources	Resource compliance status
AWS resources	0 of 0	<div style="width: 100%;"></div>

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.

The screenshot shows two main views from the Microsoft Defender for Cloud interface:

- Regulatory compliance dashboard:** This view lists various compliance standards: Azure Security Benchmark V3, ISO 27001, PCI DSS 3.2.1, SOC TSP, HIPAA HITRUST, NIST SP 800 53 R4 (highlighted with a yellow circle 1), UKO and UK NHS, and Azure CIS 1.1.0. A survey question "Is the regulatory compliance experience clear to you?" has "Yes" selected (highlighted with a yellow circle 2). Below the standards, a section for "NIST SP 800 53 R4" is expanded, showing controls under "AC. Access Control".
 - Control 3:** AC-1, Access Control Policy and Procedures [Control details](#)
 - Control 4:** AC-2(1), Automated System Account Management [Control details](#)
 - Control 5:** AC-2(2), Removal of Temporary / Emergency Accounts [Control details](#)
 - Control 6:** AC-2(3), Disable Inactive Accounts [Control details](#)
 - Control 7:** AC-2(4), Automated Audit Actions [Control details](#)
 - Control 8:** AC-2(5), Inactivity Logout [Control details](#)
 - Control 9:** AC-2(6), Dynamic Privilege Management [Control details](#)
 - Control 10:** AC-2(7), Role-based Schemes [Control details](#)
- AC.2.7 Role-based Schemes table:** This table lists actions categorized by type (Technical or Operational) and action name.

Action Type	Action Name	Your Actions
Technical	Audit usage of custom RBAC rules	Automated (6)
Technical	Service Fabric clusters should only use Azure Active Directory for client authentication	Automated
Technical	SQL servers should have an Azure Active Directory administrator provisioned	Automated
Operational	Audit privileged functions	Manual (7)
Operational	Monitor account activity	Manual
Operational	Monitor privileged role assignment	Manual
Operational	Restrict access to privileged accounts	Manual
Operational	Revoke privileged roles as appropriate	Manual
Operational	Use privileged identity management	Manual

Example - Investigate issues

Azure Security Benchmark V3

ISO 27001

PCI DSS 3.2.1

SOC TSP

HIPAA HITRUST

NIST SP 800 53 R4

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. The regulations listed above are the ones that are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

NIST SP 800 53 R4 is applied to the subscription AG_Compliance_Compliance_TEST

Expand all compliance controls

^ **✖ AC. Access Control**

▼ **✓ AC-1. Access Control Policy and Procedures** [Control details](#)

^ **✖ AC-2. Account Management**

▼ **✖ AC-2.*. Additional assessments for AC-2 - Account Management**

▼ **✓ AC-2(1). Automated System Account Management** [Control details](#)

Example - Investigate issues (cont'd)

Dashboard > Microsoft Defender for Cloud > NIST SP 800 53 R4

AC.2.7 Role-based Schemes

Overview **Your Actions** Microsoft Actions

Your Actions	Action Name	Action Type	
Automated	Audit usage of custom RBAC rules	Technical	▼
Automated	Service Fabric clusters should only use Azure Active Directory for client authentication	Technical	<input checked="" type="checkbox"/> ▼
Automated	SQL servers should have an Azure Active Directory administrator provisioned	Technical	▼

Example - Remediate an automated assessment

Disk encryption should be applied on virtual machines ×

Severity

High

Freshness interval



24 Hours

▼ Description

▼ Remediation steps

^ Affected resources

Unhealthy resources (107)

Healthy resources (0)

Not applicable resources (18)

Search virtual machines



Name

↑↓ Subscription



vmtest

ASC DEMO ...



VMTEST

ASC DEMO ...



VM6

ASC DEMO ...

Example - Remediate an automated assessment (cont'd)

... > VM6 > Disk encryption should be applied on virtual machines > VM6 >



Ultra disk

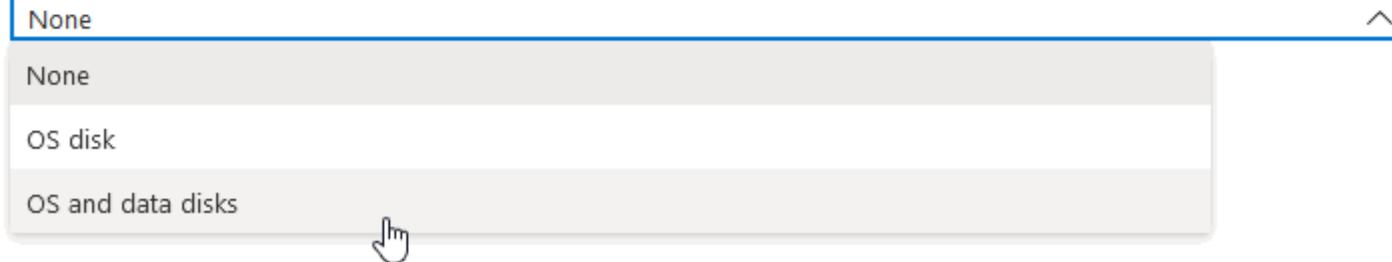
Enable Ultra disk compatibility ⓘ
 Yes
 No

Ultra disk is available only for Availability Zones in eastus2. [Learn more ↗](#)

Encryption settings

Azure Disk Encryption (ADE) provides volume encryption for the OS and data disks. [Learn more about Azure Disk Encryption](#).

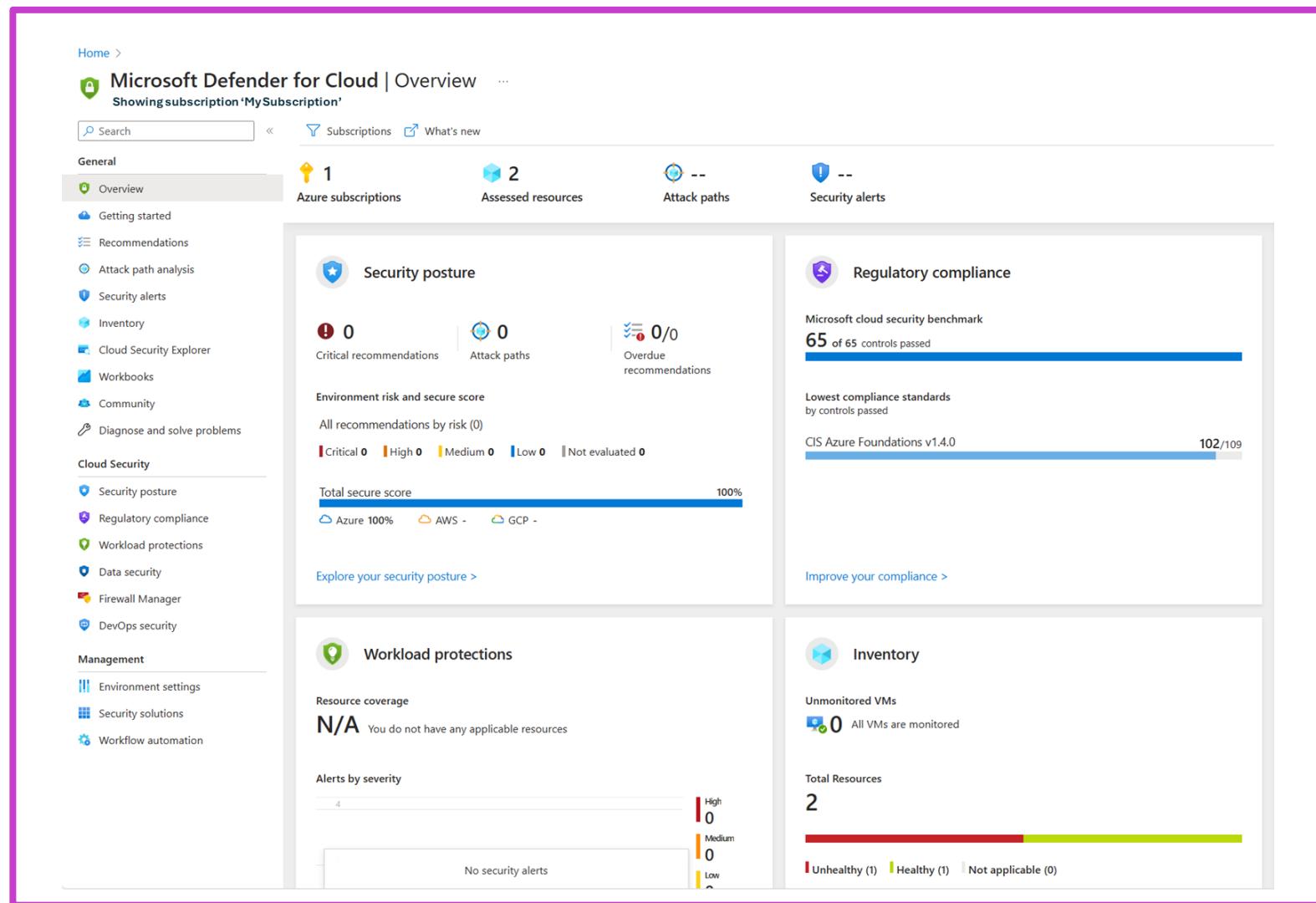
Disks to encrypt ⓘ



~~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.



The screenshot shows the Microsoft Defender for Cloud Settings interface under 'Defender plans'. A yellow callout box contains the text: "Note: **TO REVIEW ONLY** select Change plan > to display the details of the recommended Microsoft Defender for Servers Plan 2, then click the X in the top-right corner of the plan selection details to close the template." A red box highlights the 'Save' button at the top right of the main page. A red arrow points from the 'Change plan' button to a detailed 'Plan selection' modal window.

Plan selection

Defender for servers is offered in two plans.
Plan 1 provides a limited set of defenses with a focus on Defender for Endpoint's protections.
Plan 2 includes the full set of our enhanced security features for servers.
[Learn more](#)

Microsoft Defender for Servers Plan 2 \$15/Server/Month

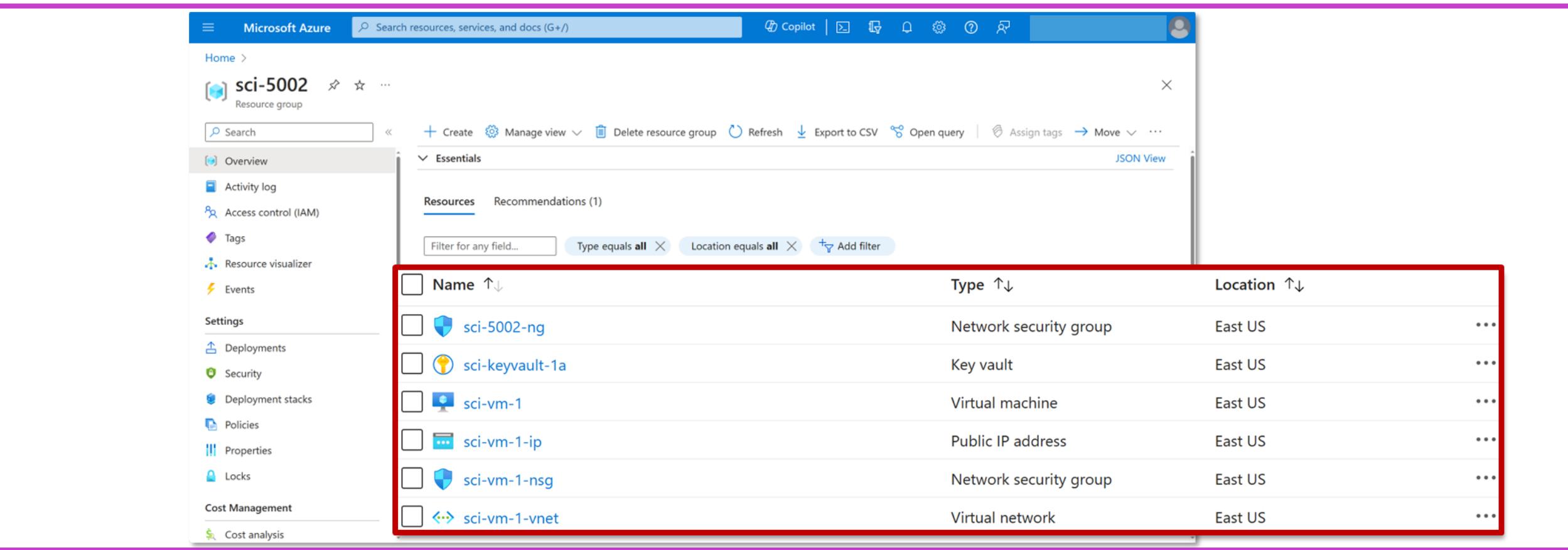
Plan details

- ✓ Microsoft Defender for Endpoint
- ✓ Microsoft Defender vulnerability management
- ✓ Automatic agent onboarding, alert and data integration
- ✓ Generates detailed, context-based, security alerts easily integrated with any SIEM
- ✓ Provides guidelines to help investigate and mitigate identified threats
- ✓ Agentless VM vulnerability scanning [Learn more](#).
- ✓ Agentless VM secrets scanning [Learn more](#).
- ✓ Agentless malware detection (preview)
- ✓ Control plane security alerts
- ✓ Resolve missing software updates gaps with Azure Update Manager (Free for Plan 2 Arc machines)
- ✓ Regulatory compliance and industry best practices
- ✓ Just-in-time VM access for management ports
- ✓ Network layer threat detection
- ✓ File integrity monitoring
- ✓ Baselines assessment
- ✓ Log Analytics 500MB free data ingestion

[Launch this Exercise in GitHub](#)

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

Azure Resource Group



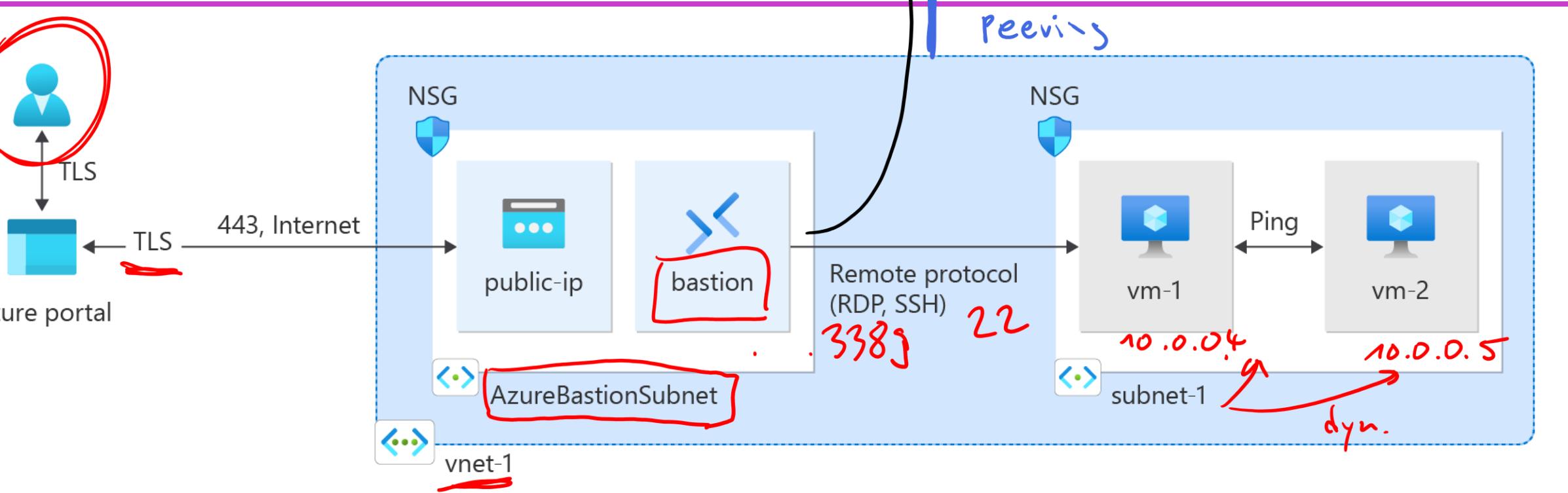
The screenshot shows the Microsoft Azure portal interface for a resource group named "sci-5002". The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings (Deployments, Security, Deployment stacks, Policies, Properties, Locks), and Cost Management (Cost analysis). The main content area displays the "Essentials" section with a table of resources. The table has columns for Name, Type, and Location. The resources listed are:

Name	Type	Location
sci-5002-nginx	Network security group	East US
sci-keyvault-1a	Key vault	East US
sci-vm-1	Virtual machine	East US
sci-vm-1-ip	Public IP address	East US
sci-vm-1-nsg	Network security group	East US
sci-vm-1-vnet	Virtual network	East US

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

Home > Microsoft.NetworkSecurityGroup-20240109211903 | Overview >

sci 5002-ng Network security group

Search Move Delete Refresh Give feedback

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Resource group (move) : sci-5002 Location : East US Subscription (move) : Associated with : 0 subnets, 0 network interfaces

Custom security rules : 0 inbound, 0 outbound

JSON View

Inbound Security Rules

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

Outbound Security Rules

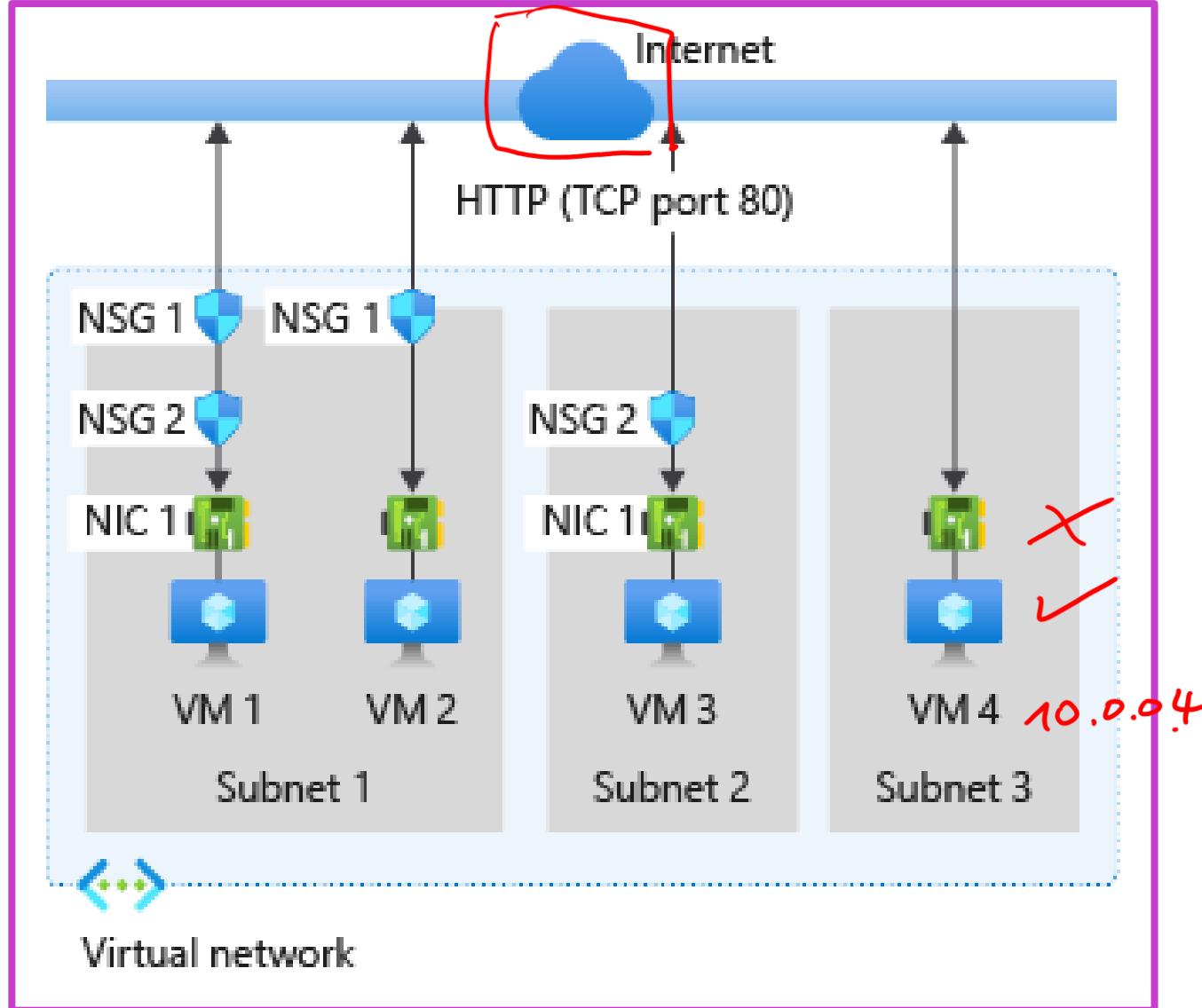
Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Service Tag ASG web Server

© Copyright Microsoft Corporation. All rights reserved.

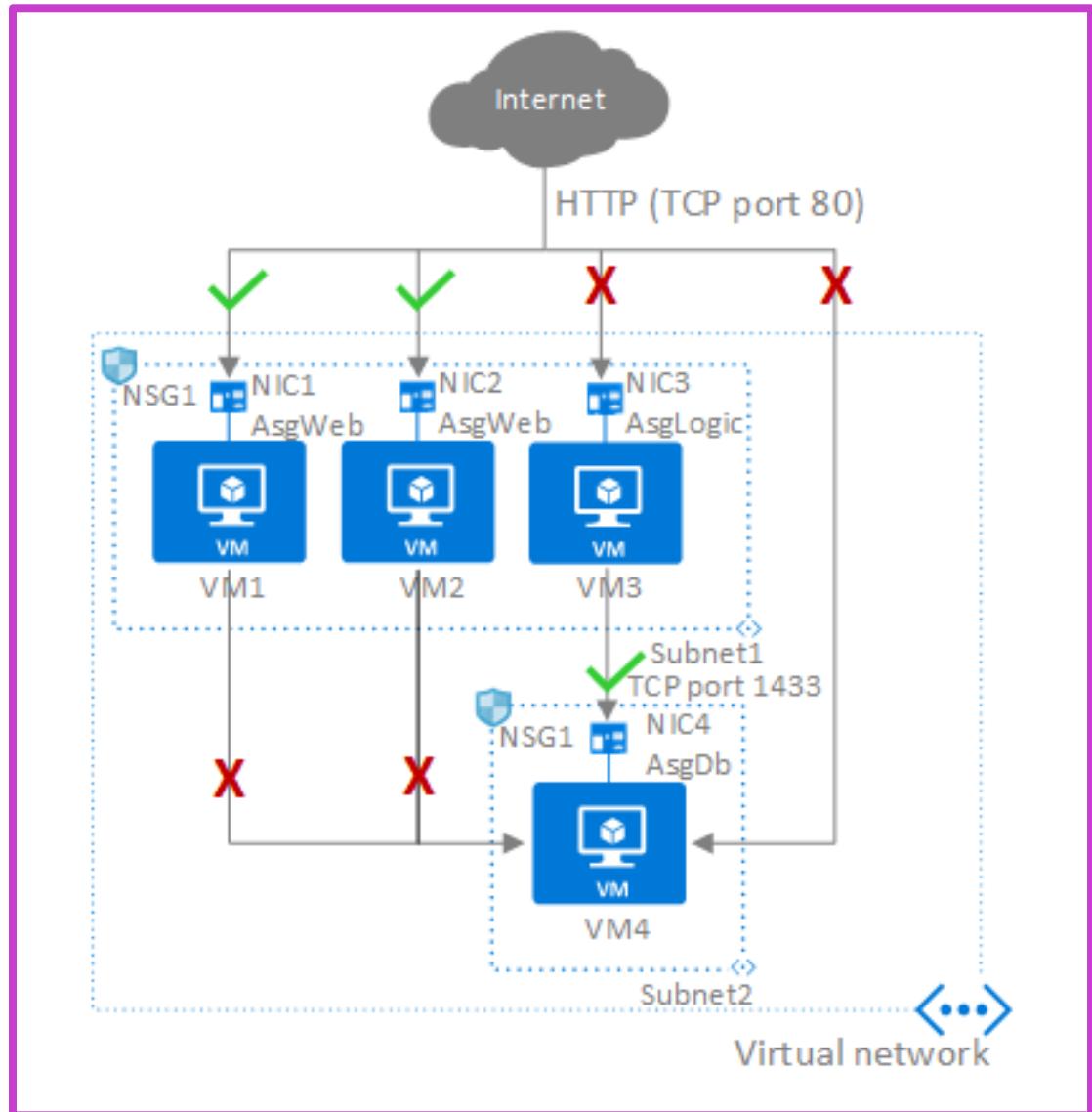
How network security groups filter network traffic (cont'd)

- 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.

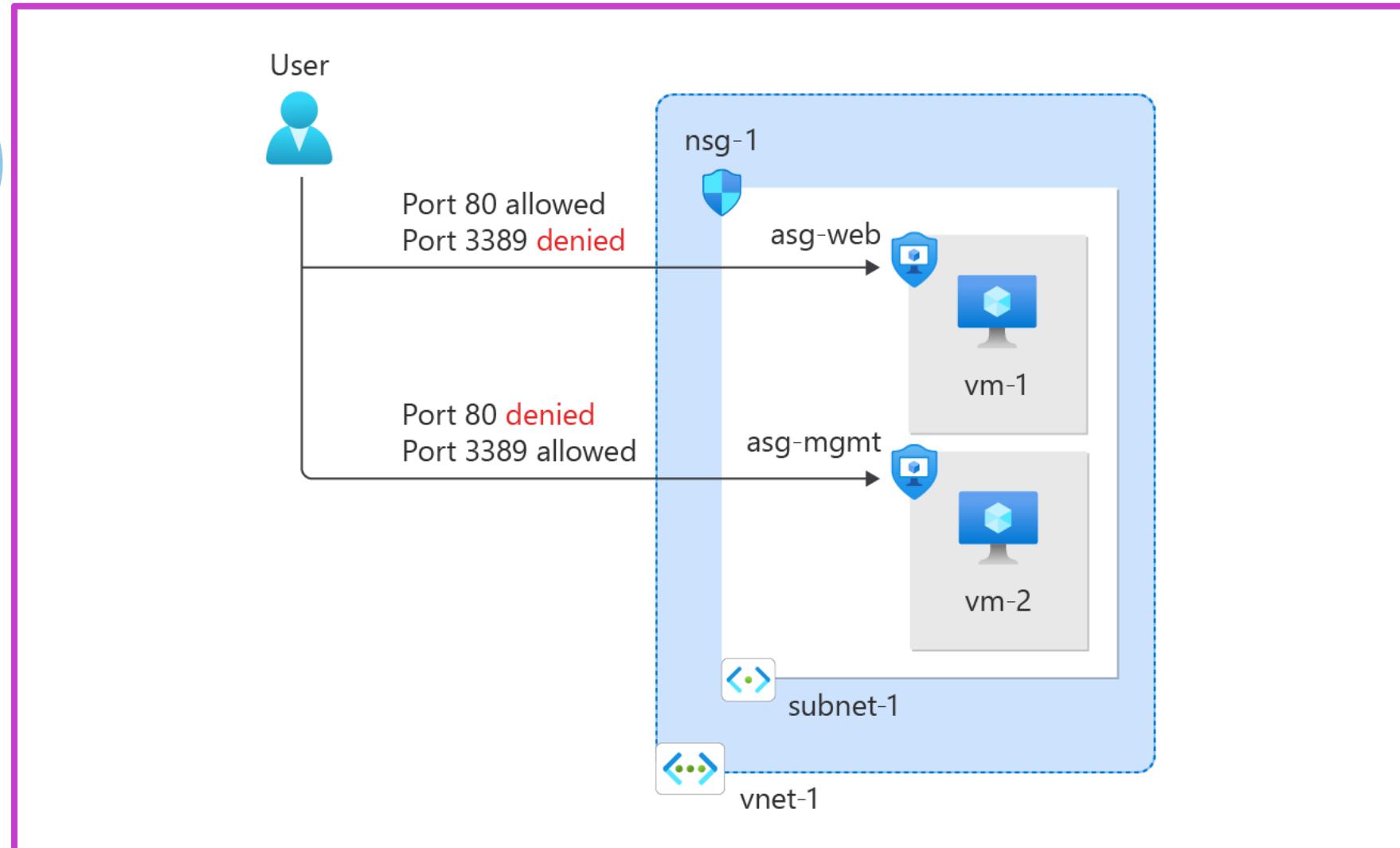


Exercise – Create a virtual network infrastructure



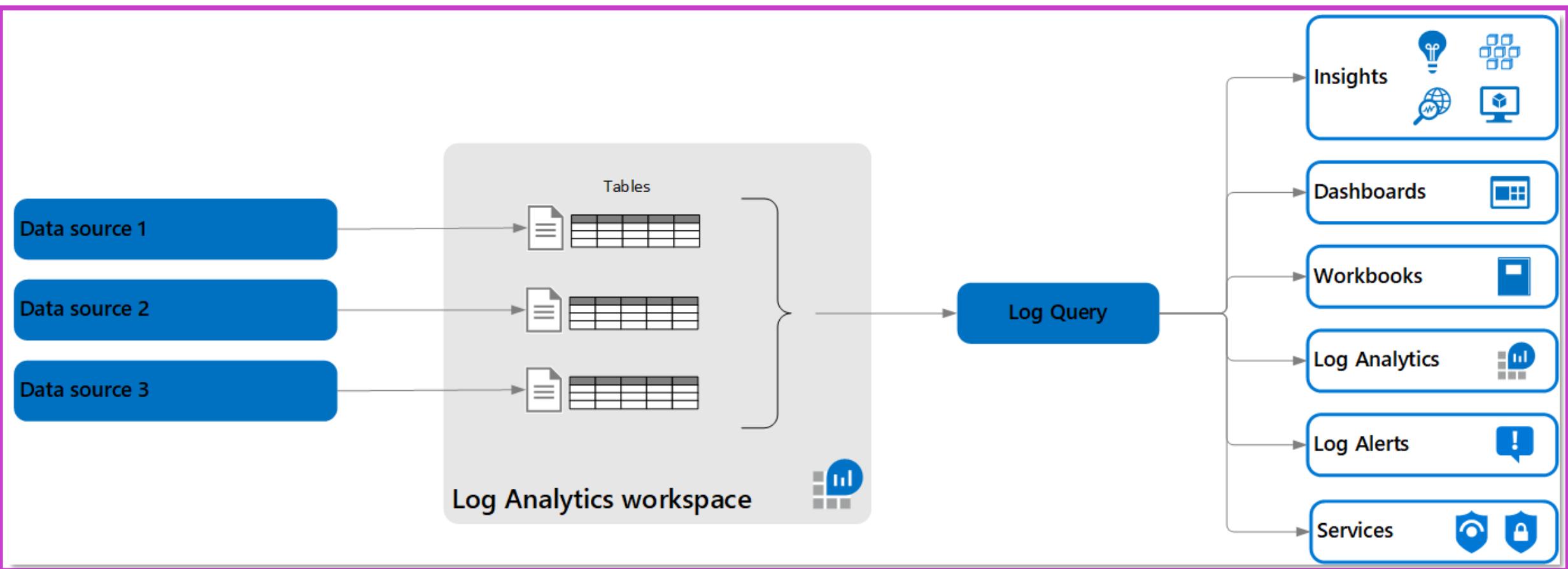
This exercise teaches students how to use a network security group to filter inbound and outbound network traffic to and from Azure resources in an Azure virtual network.

[Launch this Exercise in GitHub](#)



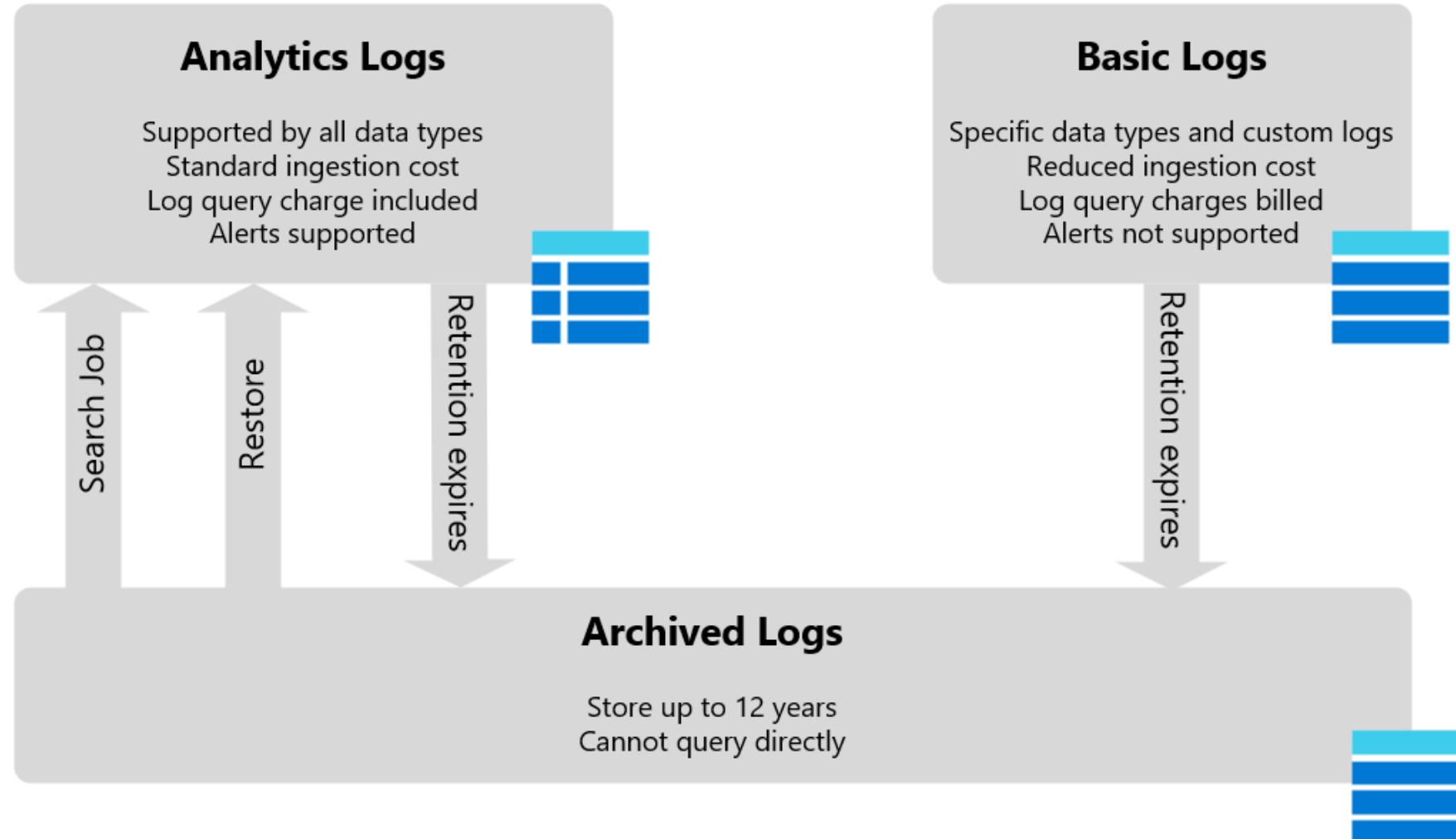
4/8 Create a Log Analytics workspace for Microsoft Defender for Cloud

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.



Home > **sciwrkspc1a** Log Analytics workspace

Search Delete

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Logs

Settings

Tables Agents Usage and estimated costs Data export

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

1 Connect a data source

Select one or more data sources to connect to the workspace

Azure virtual machines (VMs)
Windows and Linux Agents management
Storage account log
System Center Operations Manager

2 Configure monitoring solutions

Add monitoring solutions that provide insights for applications and services in your environment

[View solutions](#)

3 Monitor workspace health

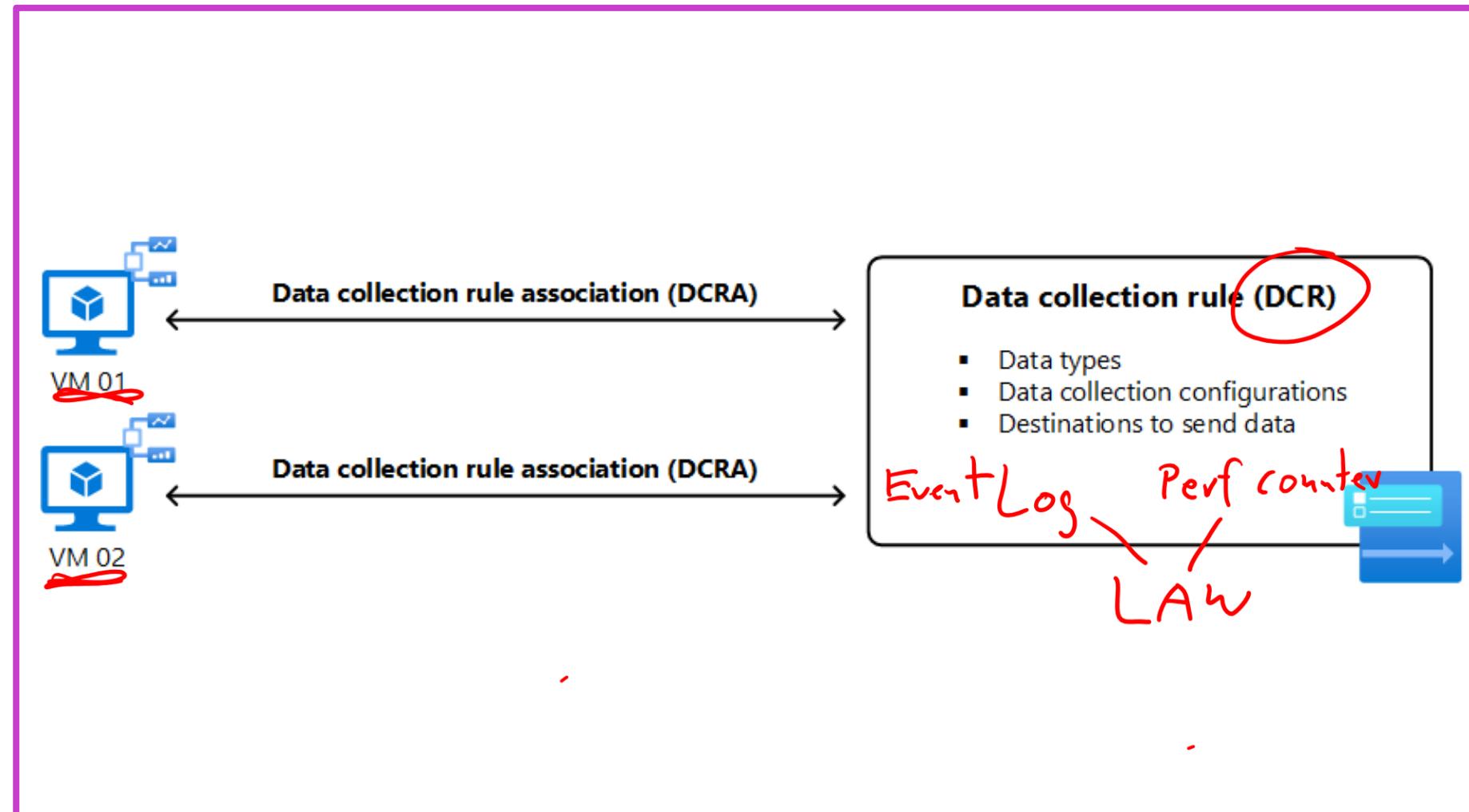
© Copyright Microsoft Corporation. All rights reserved.

[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

The screenshot shows two windows from the Azure portal. On the left is the 'dcr-1 | Data sources' blade, which lists various monitoring options like Overview, Activity log, and Data sources. The 'Data sources' item is selected. On the right is the 'Add data source' dialog, which is set to the 'Destination' tab. It shows a table with one row for 'Azure Monitor Logs'. The 'Destination type' is 'Subscription', 'Subscription' is 'My Subscription', and 'Destination Details' is 'az-rg-1-wrkspc (az-rg-1)'. There are buttons at the bottom for 'Add data source', '< Previous', and 'Cancel'.

- 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.

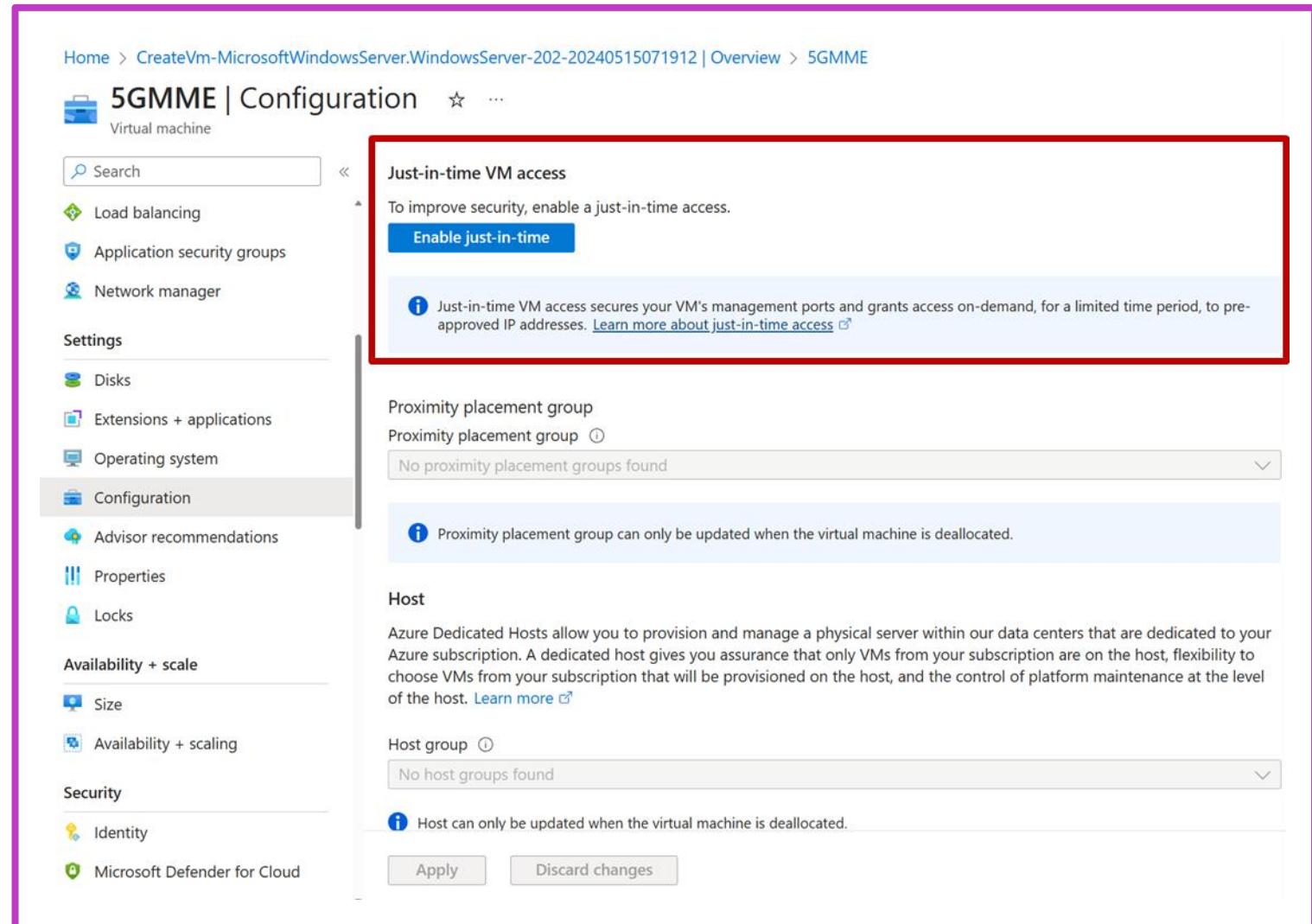
[Launch this Exercise in GitHub](#)

The screenshot shows the 'Create Data Collection Rule' wizard in the Azure portal. The current step is 'Collect and deliver'. A note at the bottom left says 'This data collection rule doesn't have any data sources or destinations selected.' A yellow callout box highlights the 'Event logs' section in the configuration pane, which lists Application, Security, and System logs with their respective log levels (Critical, Error, Warning, Information, Verbose) checked or unchecked. The configuration pane also includes sections for 'Data source type' (set to 'Windows Event Logs') and 'Basic' vs 'Custom' collection options. Navigation buttons at the bottom include 'Review + create', '< Previous', 'Next : Tags >', 'Add data source', 'Next : Destination >', and 'Cancel'.

6/8 Explore just-in-time VM access

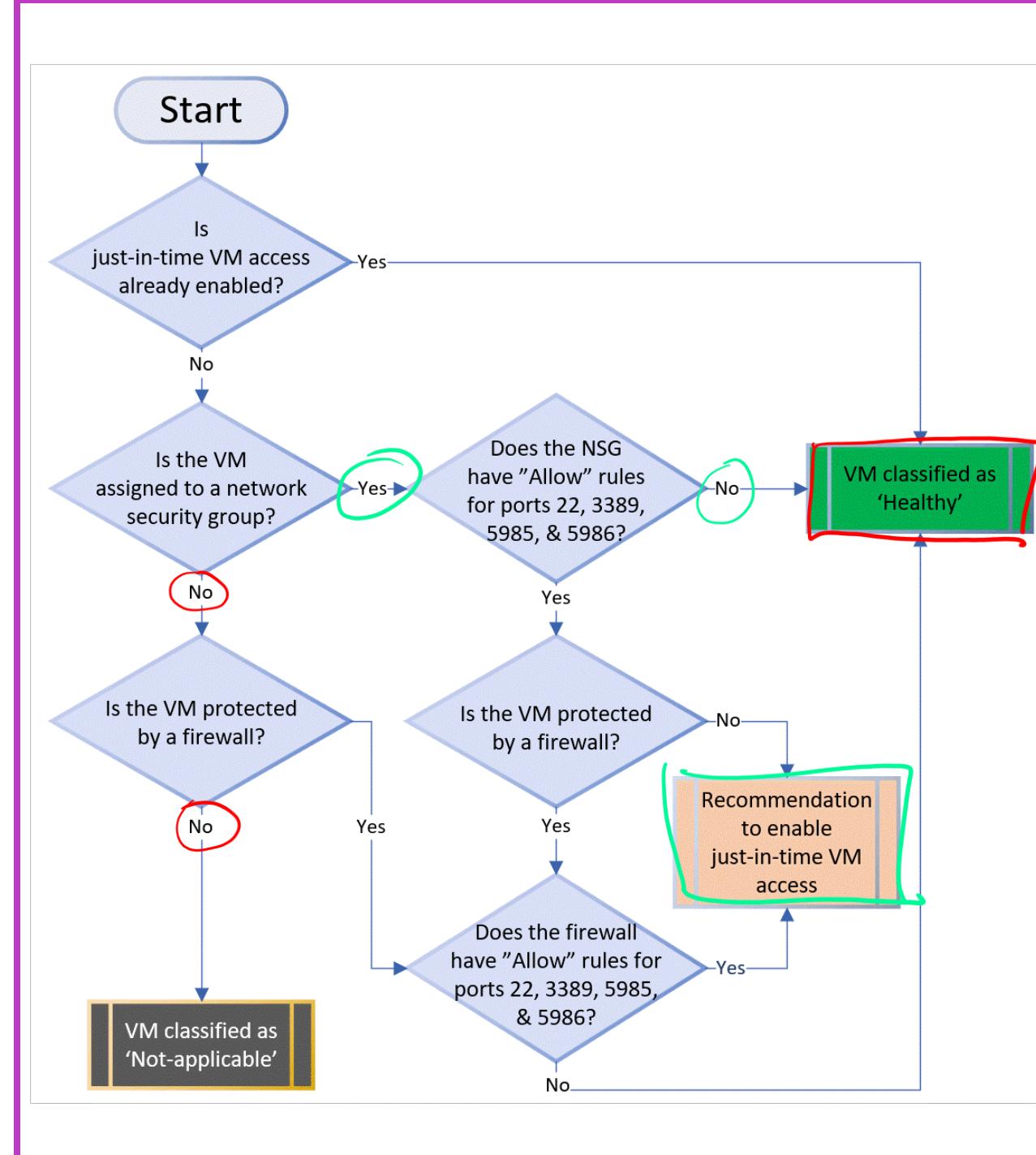
Understanding just-in-time VM access

- 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.



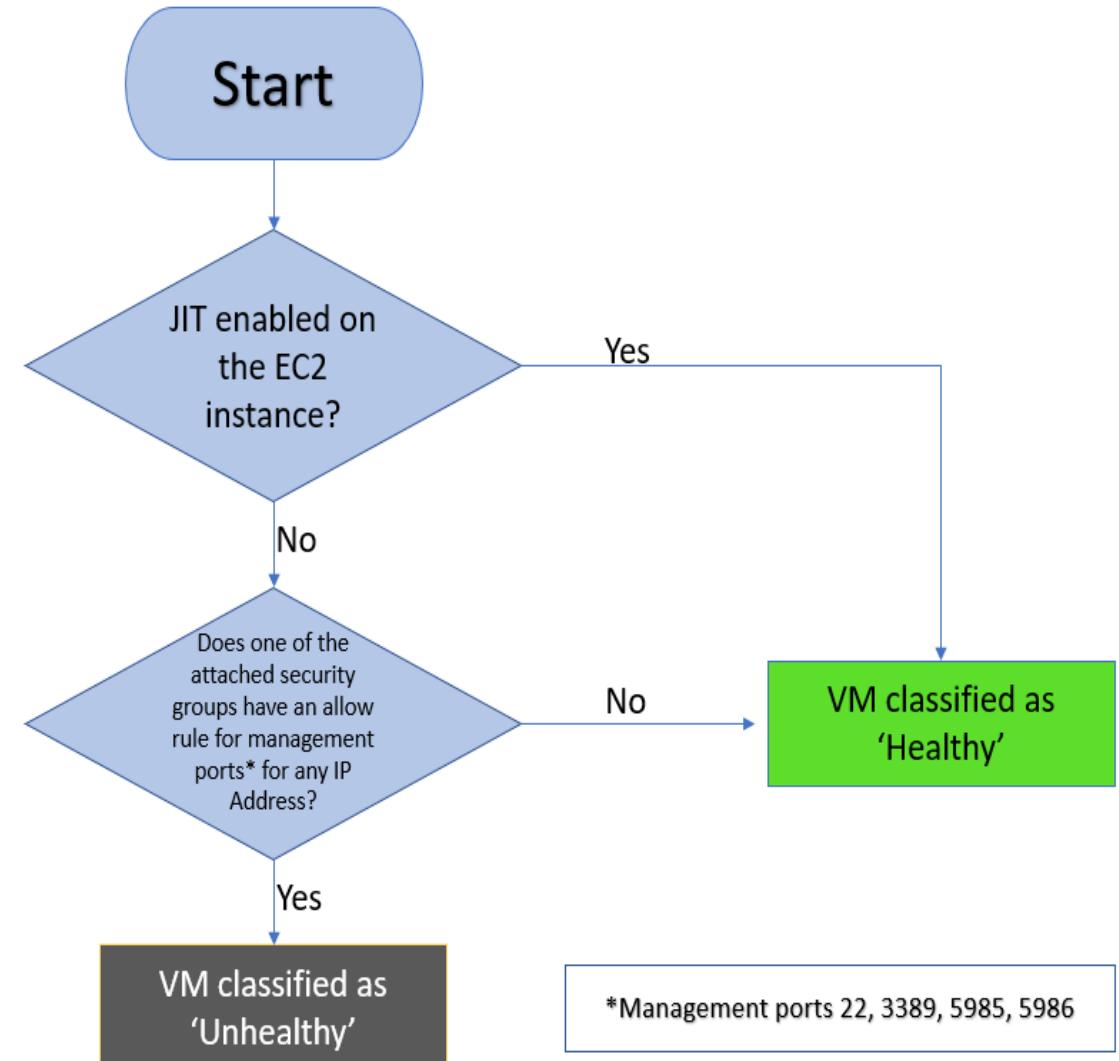
Just-in-time VM is enabled an Azure Virtual Machine

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.

Example: Affected resources

Dashboard > Microsoft Defender for Cloud | Recommendations >

Management ports of virtual machines should be protected with just-in-time network access control

Unhealthy resources (78) Healthy resources (112) Not applicable resources (66)

Name	Subscription
ContosoWeb2	Contoso IT - demo
ContosoWeb1	Contoso IT - demo
ContosoSQLSvr3	Contoso IT - demo
ContosoSQLSvr3	Contoso IT - demo
ContosoSQLSrv2	Contoso IT - demo

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.

The screenshot shows the 'Just-in-time VM access' page in the Microsoft Defender for Cloud interface. At the top, there's a message about subscriptions not having full protections enabled, with a link to upgrade. Below that, two links are shown: 'What is just-in-time VM access?' and 'How does it work?'. The main section is titled 'Virtual machines' and includes tabs for 'Configured' (which is selected), 'Not Configured', and 'Unsupported'. A note says 'VMs for which the just-in-time VM access control is already in place. Presented data is for the last week.' It shows 1 VM named 'romebuild' with 0 Requests, N/A for Last access, and a shield icon for Connection details. The 'Last user' column shows 'N/A'. A 'Request access' button is at the top right of the table area. A search bar is at the bottom left, and a three-dot menu is at the bottom right.

Virtual machine	Approved	Last access	Connection details	Last user
romebuild	0 Requests	N/A	shield icon	N/A

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](#)

sci-vm-1 | Configuration

Virtual machine

Just-in-time VM access

To improve security, enable a just-in-time access.

Enable just-in-time

Just-in-time VM access secures your VM's management ports and grants access on-demand, for a limited time period, to pre-approved IP addresses. [Learn more about just-in-time access](#)

Proximity placement group

No proximity placement groups found

Host

Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. [Learn more](#)

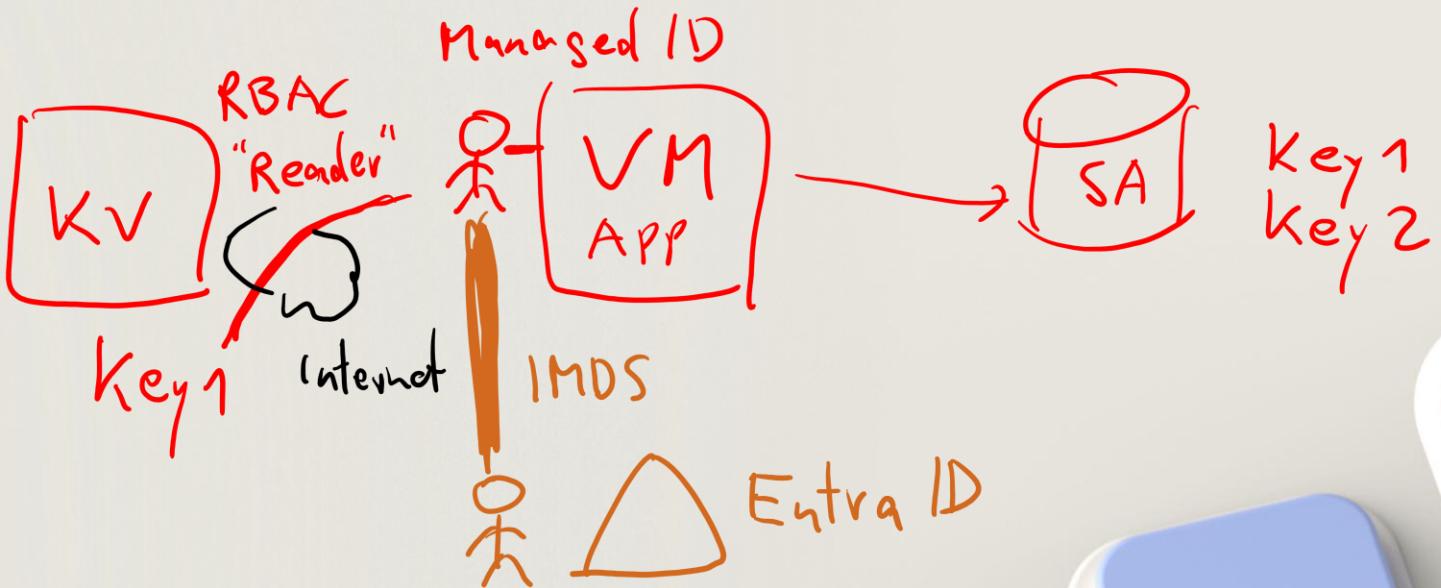
Host group

No host groups found

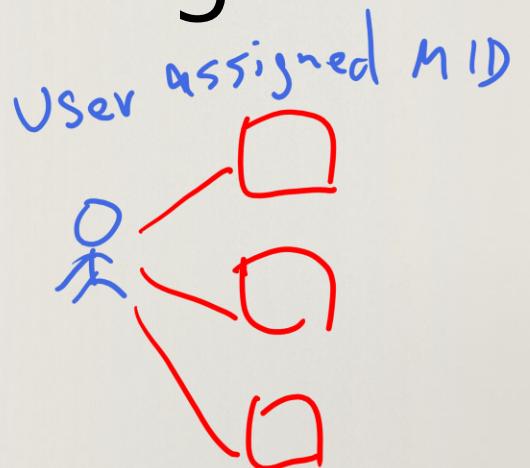
Security type

The different levels of security available for your virtual machines. Standard offers basic protection at no extra costs. Trusted launch virtual machines provide additional security features on Gen 2 virtual machines to protect against persistent and advanced attacks. Confidential virtual machines include additional confidentiality protections for isolated machines or encrypted data on Gen 2 virtual machines. [Learn more about security types](#)

Apply Discard changes



7/8 Configure Azure Key Vault networking settings



Azure Key Vault basic concepts

RSA 2048 Bit

$$\begin{array}{r} 3 \cdot 5 = 15 \\ 15 \quad = ? \end{array}$$

- 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](#)

Home >

Key vaults

Microsoft Non-Production

+ Create Manage deleted vaults Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

Showing 1 to 1 of 1 records.

Name ↑↓	Type ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓	Tags
<input type="checkbox"/> sci-keyvault-1a	Key vault	sci-5002	East US	My Subscription	...

< Previous Page 1 of 1 Next >

Give feedback

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.

The screenshot shows the Azure portal interface for managing network settings for an Azure Key Vault. On the left, under 'Firewalls and virtual networks', there are sections for 'Allow access from:' and 'Private endpoint connections'. Under 'Allow access from:', three options are listed: 'Allow public access from all networks' (radio button), 'Allow public access from specific virtual networks and IP addresses' (radio button, selected), and 'Disable public access'. A note below states: 'Only networks you choose can access this key vault.' Under 'Virtual networks', it says 'Allow selected virtual networks to connect to your resource securely and directly using service endpoints'. Three buttons are available: '+ Add a virtual network', '+ Add existing virtual networks' (which is highlighted with a red box), and '+ Add new virtual network'. Below this is the 'Firewall' section, which allows adding IP ranges for internet or on-premises access. On the right, a modal window titled 'Add networks' is open, showing configuration for a specific virtual network. It includes fields for 'Subscription' (set to 'My Subscription'), 'Virtual networks' (set to 'sci-vm-1-vnet'), and 'Subnets' (set to 'default (Service endpoint required)'). A note in the modal says: 'The following networks don't have service endpoints enabled for 'Microsoft.KeyVault'. Enabling access will take up to 15 minutes to complete. After starting this operation, it is safe to leave and return later if you do not wish to wait.' At the bottom of the modal is a checkbox 'Do not configure 'Microsoft.KeyVault' service endpoint(s) at this time' and a blue 'Enable' button.

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](#)

Home > Key vaults > sci-keyvault-1a

sci-keyvault-1a | Properties

Key vault

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Access policies

Events

Objects

Keys

Secrets

Certificates

Save Discard changes Refresh

Subscription ID

Subscription Name

Directory ID

Directory Name

Soft-delete

Days to retain deleted vaults

Purge protection

My Subscription

Microsoft Non-Production

Soft delete has been enabled on this key vault

90

Disable purge protection (allow key vault and objects to be purged during retention period)

Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)

A screenshot of the Azure Key Vault Properties page for 'sci-keyvault-1a'. The left sidebar shows navigation links like Overview, Activity log, and Access control (IAM). The main area displays subscription details ('My Subscription' and 'Microsoft Non-Production'), directory information, and soft-delete settings. A note states 'Soft delete has been enabled on this key vault'. It shows a retention period of 90 days and two radio button options for purge protection: 'Disable purge protection (allow key vault and objects to be purged during retention period)' (selected) and 'Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)'.

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

Azure Private Endpoint

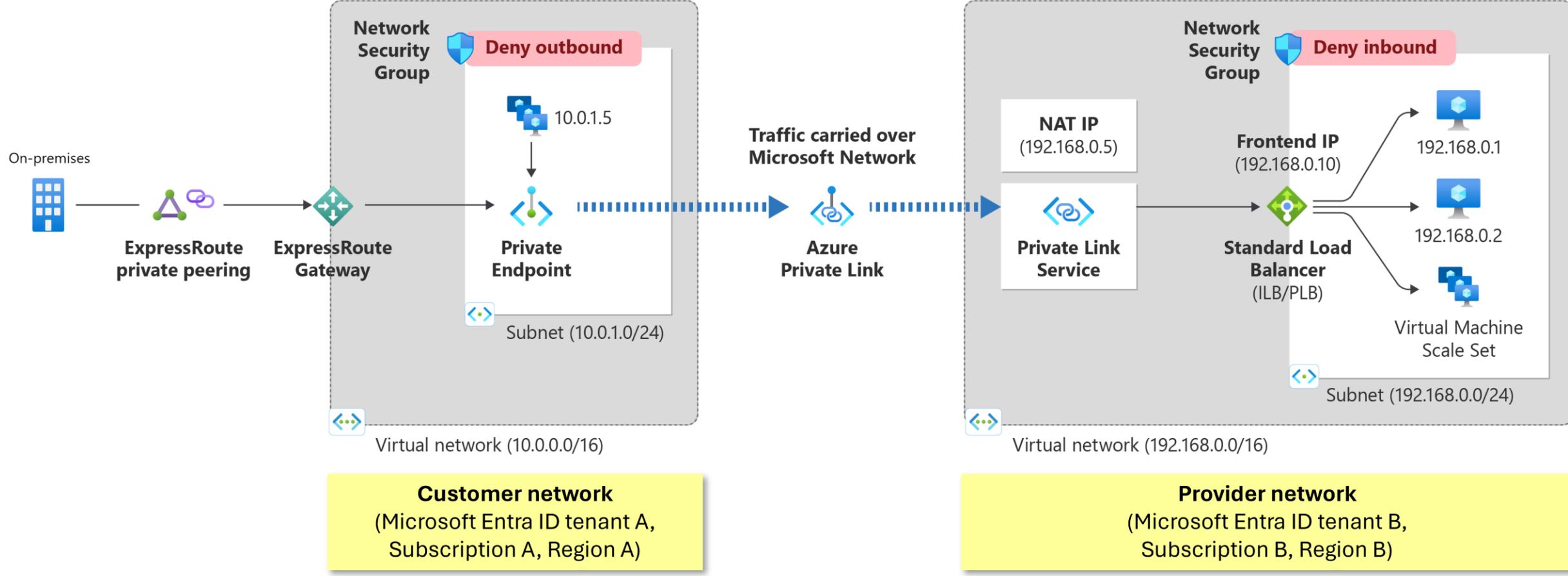
- **Private Endpoint Function:** Connects virtual networks to Azure services securely using Azure Private Link.
- **Deployment Considerations:** Supports one-way connections, maintains static IP, allows multiple endpoints across regions/subscriptions.
- **Network Security Features:** Secures traffic,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

The screenshot shows the Azure Private Link Center interface. The left sidebar has a navigation menu with 'Overview', 'Pending connections', 'Private endpoints' (which is selected and highlighted in grey), 'Private link services', 'Azure Arc private link scopes', and 'Azure Monitor private link scopes'. Below this is a 'Resources' section with 'Active connections' and 'Supported resources'. The main content area is titled 'Private Link Center | Private endpoints'. It includes a search bar, a toolbar with 'Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags' buttons, and filter options like 'Subscription equals all' and 'Add filter'. A message says 'Showing 1 to 1 of 1 records.' Below this is a table with one row. The columns are 'Name' (with a checkbox), 'Private IP' (10.0.0.5), 'Resource' (mysqlserver1az), 'Target sub-resource' (SqlServer), and 'Subnet' (myVNet1a/mysql). At the bottom are page navigation buttons ('<', 'Page 1 of 1', '>') and a 'Give feedback' link.

Name	Private IP	Resource	Target sub-resource	Subnet
myPrivateSQLEnd...	10.0.0.5	mysqlserver1az	SqlServer	myVNet1a/mysql

*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](#)

The screenshot shows the Azure portal interface for managing a MySQL server named 'mysqlserver1az'. The left sidebar lists various management options: Settings (Microsoft Entra ID, SQL databases, SQL elastic pools, DTU quota, Properties, Locks), Data management (Backups, Deleted databases, Failover groups, Import/Export history), and Security (Networking). The main content area is titled 'Networking' under the 'mysqlserver1az | Networking' section. It includes tabs for Public access, Private access, and Connectivity. The 'Public access' tab is selected, showing the 'Public network access' section which describes public endpoints and their security requirements. A configuration section allows selecting 'Disable' (selected) or 'Selected networks' for private endpoint connectivity. A note at the bottom states that only approved private endpoint connections will be accepted, retaining existing firewall rules or virtual network endpoints.

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