Microsoft

AZ-801

Configure Windows Server Hybrid Advanced Services

Agenda AZ-801

1 Security – Windows Server
2 Security – Hybrid

3 Failover Cluster

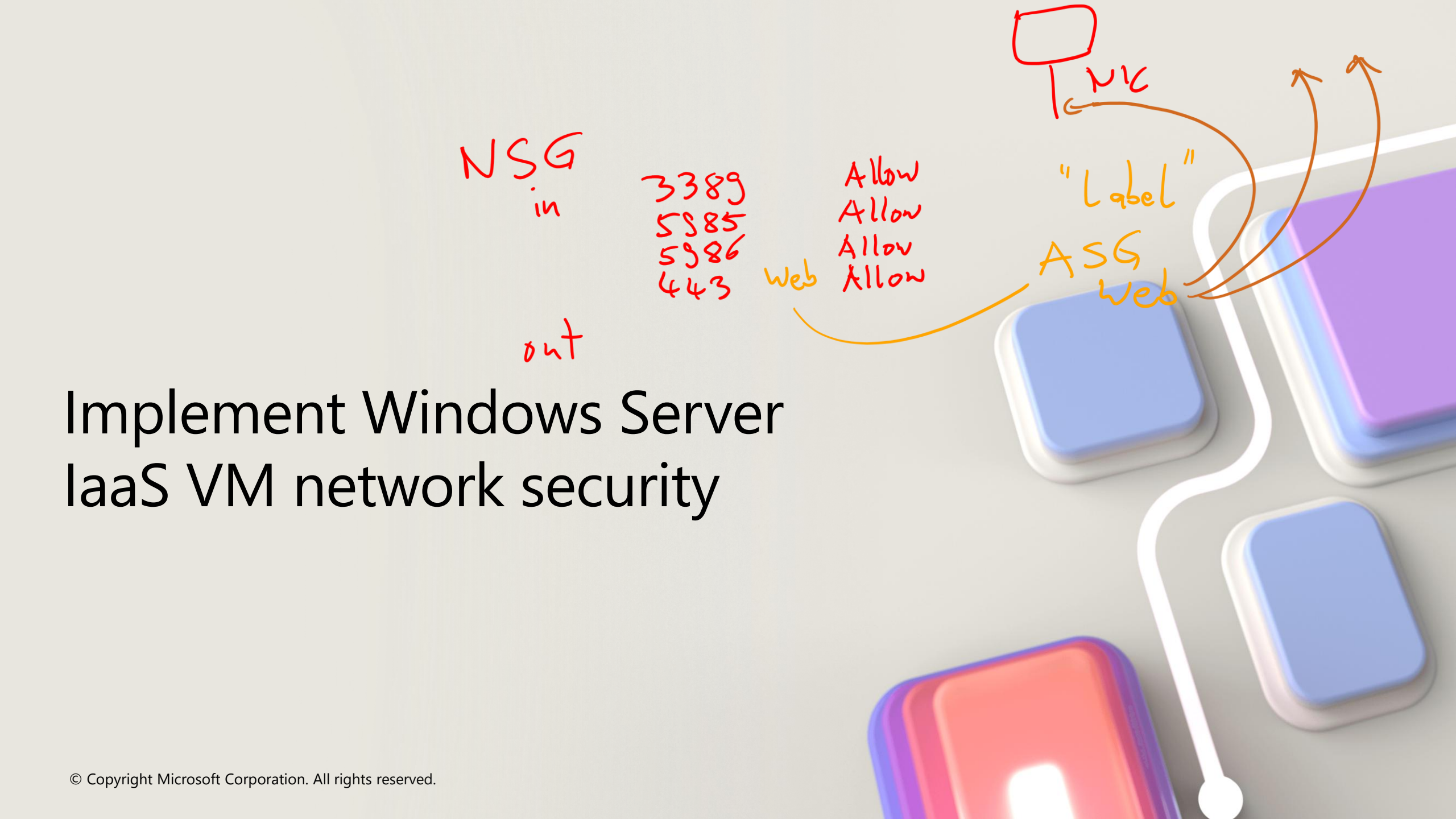
4 Disaster Recovery – Windows Server
5 Disaster Recovery – Hybrid

6 Upgrade and Migrate – Windows Server
7 Migrate Windows Server to the Cloud

8 Monitoring – Windows Server
9 Monitoring – Hybrid

Secure Windows Server on-premises and Hybrid Infrastructures *(Implementing Security Solutions in Hybrid Scenarios)*

- Implement Windows Server IaaS VM network security
- Audit the security of Windows Server IaaS Virtual Machines
- Manage Azure updates
- Configure BitLocker disk encryption for Windows IaaS Virtual Machines
- Lab 02: Implementing Security Solutions in Hybrid Scenarios



Implement Windows Server IaaS VM network security

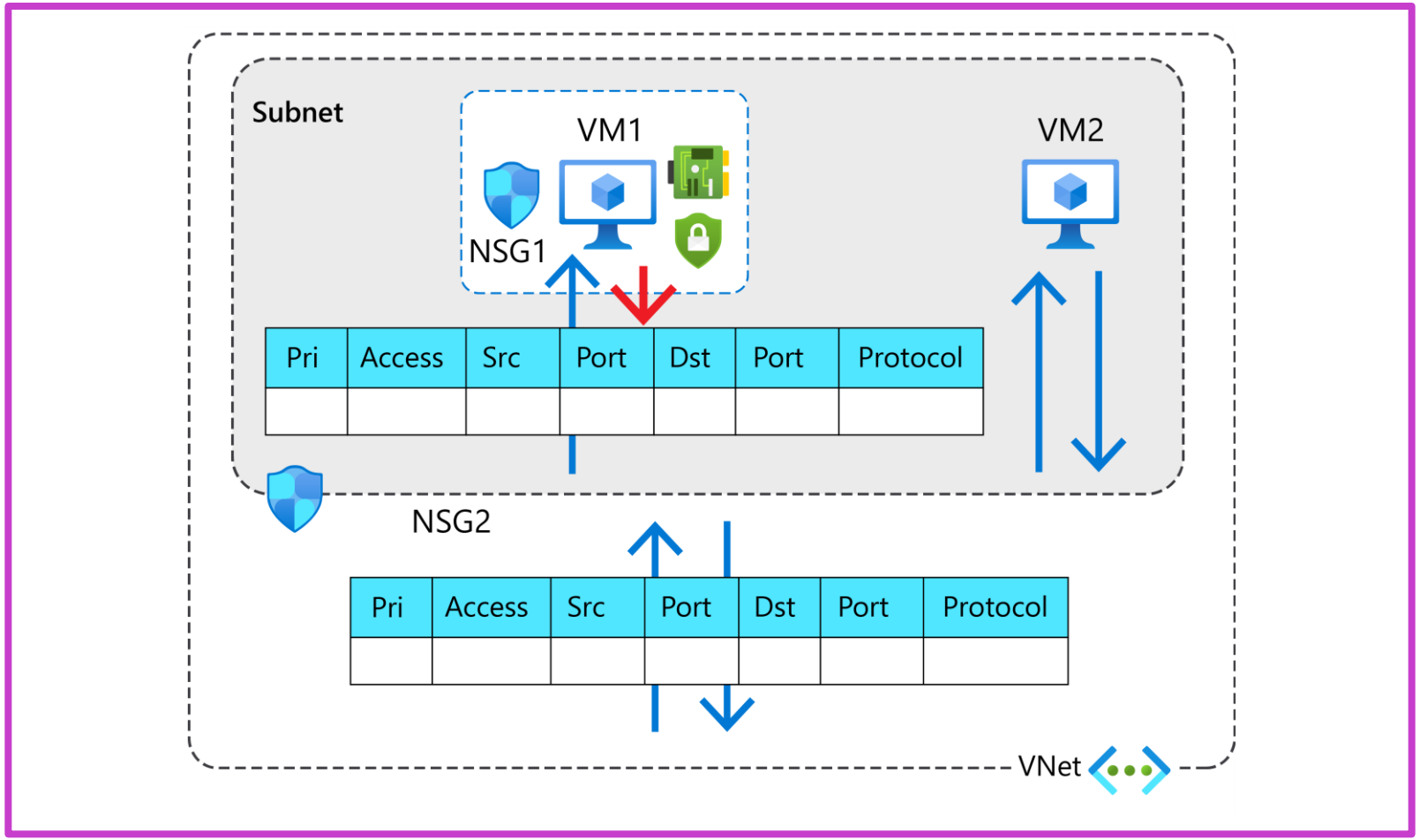
Learning Objectives – Implement Windows Server IaaS VM network security

- Implement network security groups
- Security rules for network security groups
- Application security groups
- Implement Azure Firewall and Windows IaaS VMs
- Choose the appropriate filtering solution
- Capture network traffic with network watcher
- Learning recap

Implement Network Security Groups

Network security groups (NSGs) filters inbound and outbound network traffic

- Configuring the security rules for a NSG allows you to control network traffic by allowing or denying specific traffic types.
- NSGs can apply both to the ***subnet*** (NSG2) and ***network interface*** (NSG1).
- A single NSG can be associated with multiple Subnets or Network interface cards (NICs).



Security Rules for Network Security Groups

First match!

Property	Meaning
Name	A unique name within the network security group.
Priority	A number between 100 and 4096. **Lower numbers have a higher priority and are processed first.**
Source or destination	Any, or an individual IP address, classless inter-domain routing (CIDR) block, service tag, or application security group.
Protocol	Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), or Any.
Direction	Whether the rule applies to inbound, or outbound traffic.
Port range	An individual port or range of ports. You can also use a wildcard (*).
Action	Allow or deny the traffic.
Description	Optional property for describing the purpose of the rule.

Network Watcher

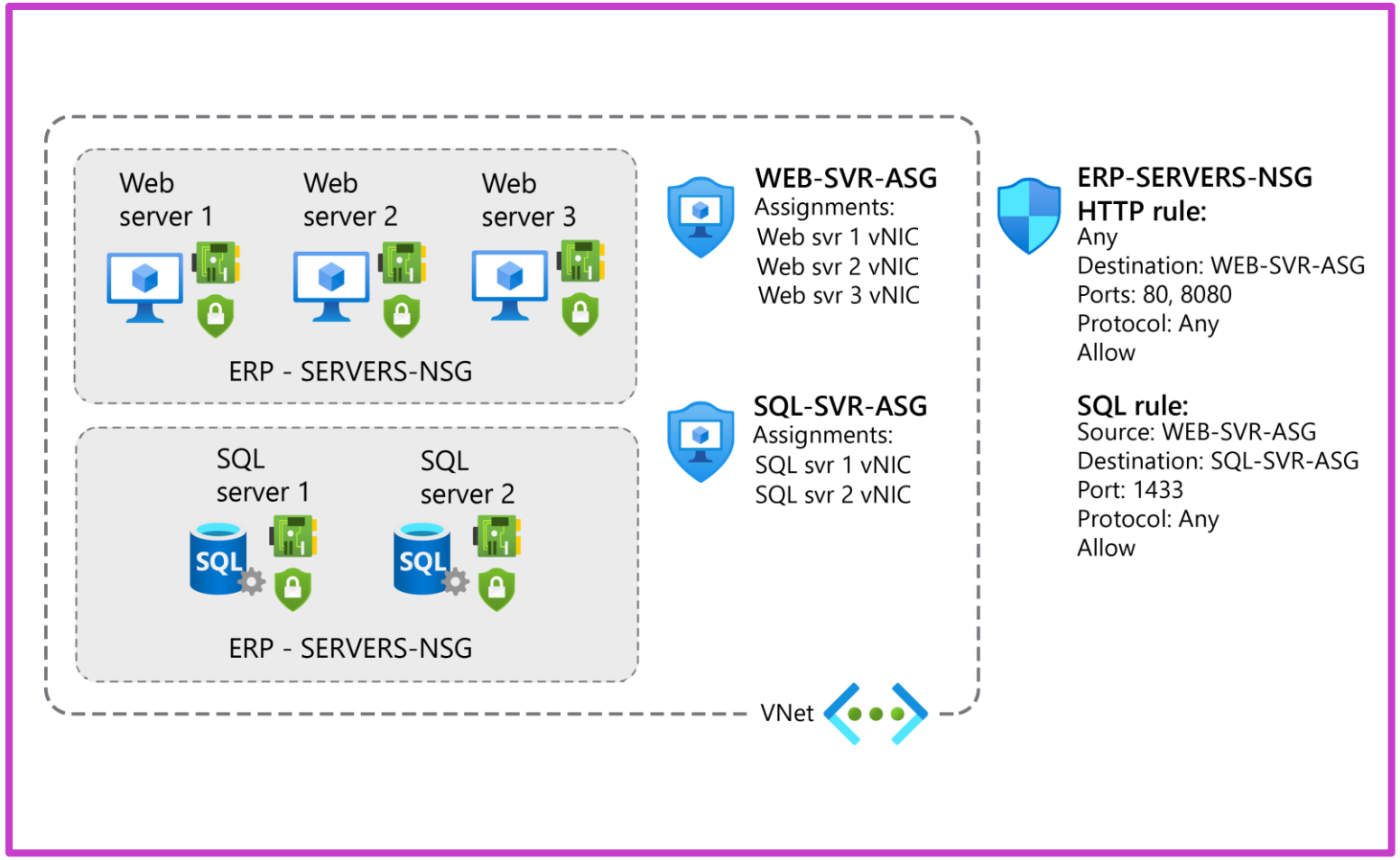
Application Security Groups

An application security group (ASG) allows you to logically group network interfaces together.

You can then use that ASG as a source or destination rule within an NSG.

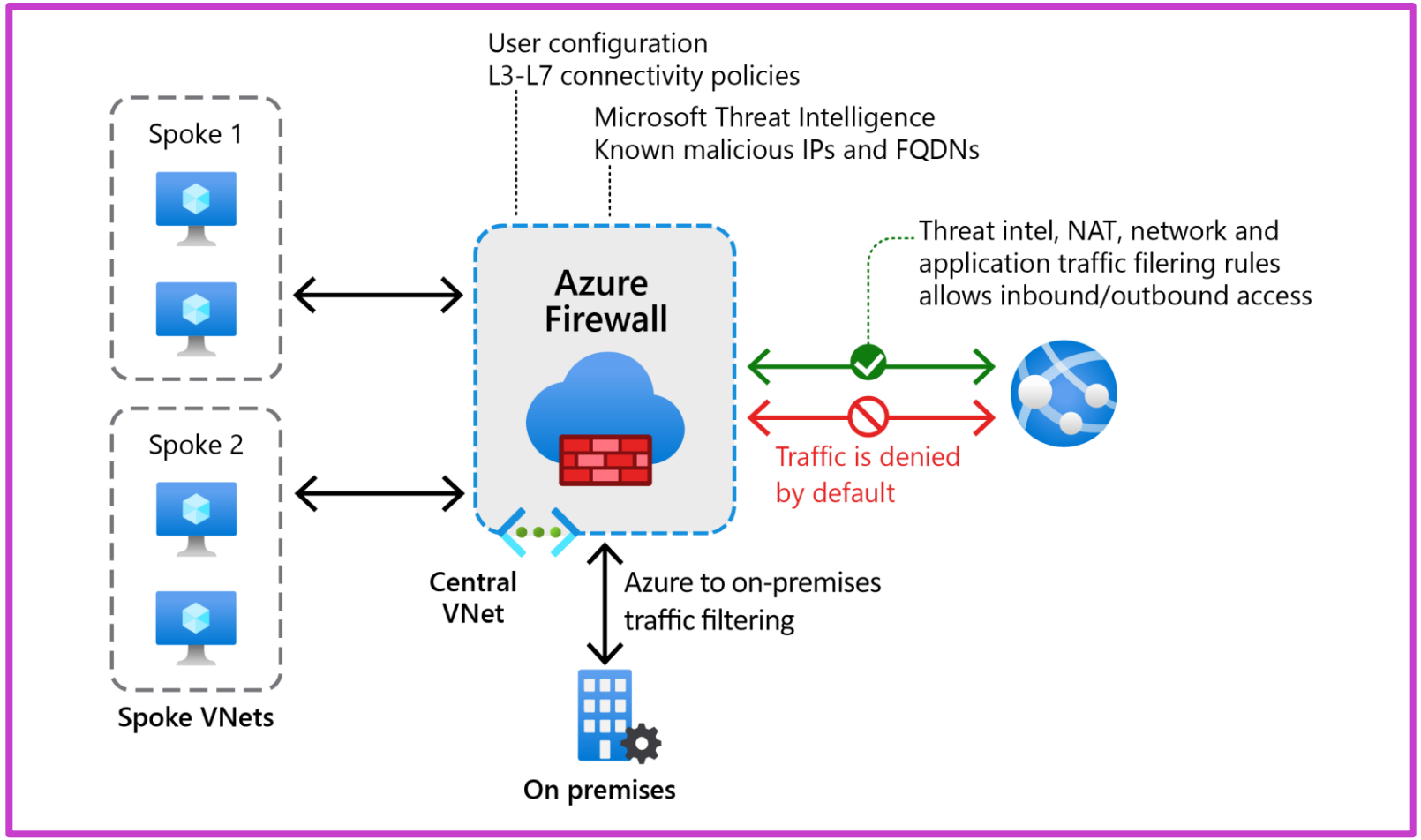
Without ASGs, you'd need to create a *separate rule for each* VM.

For example, Contoso has a number of front-end servers in a VNet. IT staff decide to implement NSGs and ASGs to secure the network resources.



Implement Azure Firewall and Windows IaaS VMs

- Azure Firewall is a cloud-based network security service.
- Azure Firewall is a stateful firewall as a service.
- Azure Firewall allows managing and controlling outbound network access is critical part of organization is network security plan.
- Use network address translation rules to manage inbound network access with Azure Firewall.



Implement Windows firewall with Windows Server IaaS VMs

What is Windows Defender Firewall with Advanced Security?

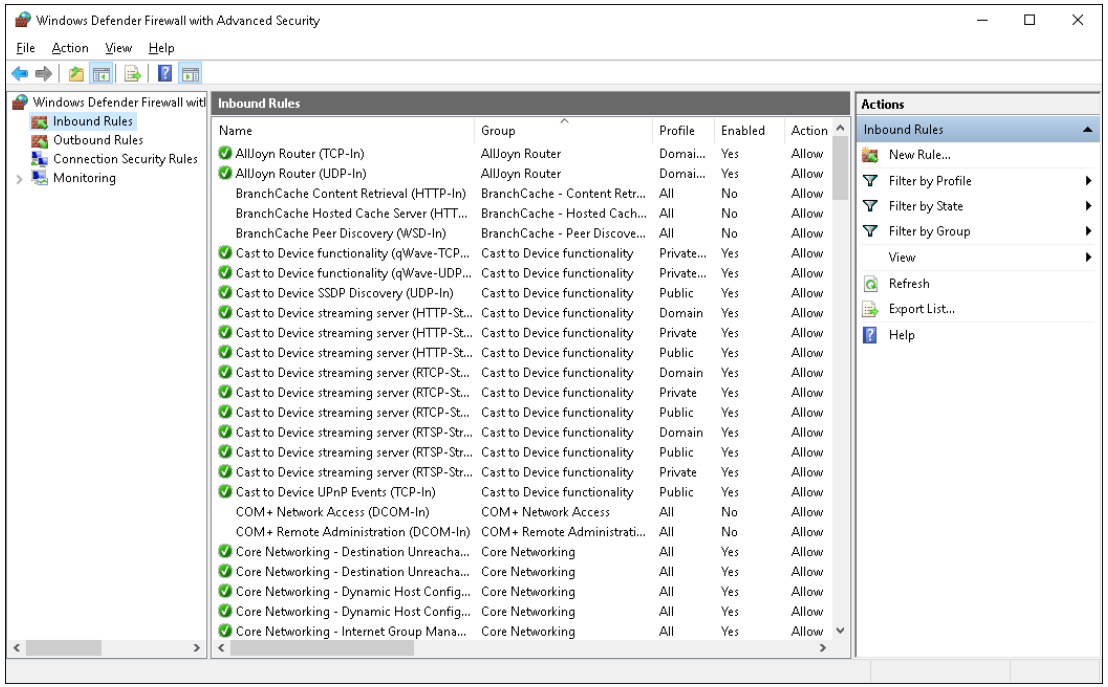
- **Windows Defender Firewall** with Advanced Security is a host-based firewall for enhancing the security of Windows Server.
- **Windows Defender Firewall** with Advanced Security is more than just a simple firewall, because it includes features such as firewall profiles and connection security rules.

Configuring Windows Defender Firewall rules

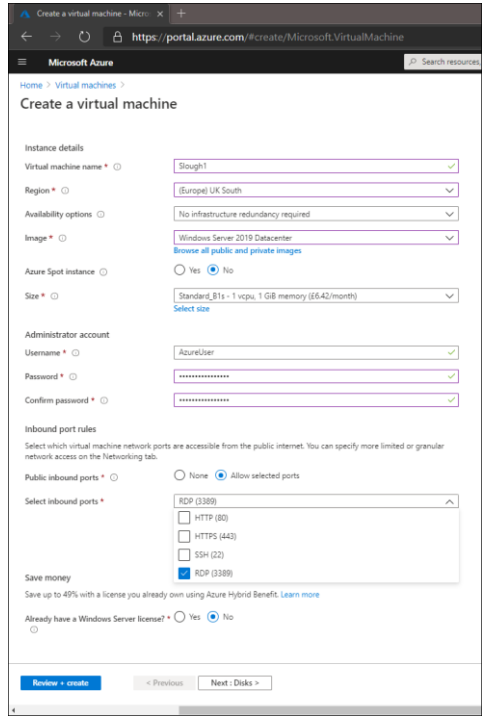
- Rules comprise a collection of criteria that define which traffic you will allow, block, or secure with the firewall.
- Inbound、Outbound、Connection security
- Inbound and outbound rule types
- Program rules, Port rules, Predefined rules, Custom rules

Implement Windows firewall with Windows Server IaaS VMs

Administering Windows Defender Firewall



Creating firewall rules when creating a VM in Azure



Choose the Appropriate Filtering Solution

You can use the following filtering options:

- NAT rules
- Network rules
- Applications rules

Direction	Rule types	Description
Outbound connectivity	Network rules and applications rules	If you configure both network rules and application rules, network rules are applied in priority order before application rules.
Inbound connectivity	Network address translation (NAT) rules	You can enable inbound internet connectivity by configuring Destination Network Address Translation (DNAT). NAT rules are applied in priority before the network rules.

Demonstration – Deploy and Configure Azure firewall

Set up a network and deploy Azure Firewall

Create a default route

Configure an application rules and network rules

Test the firewall settings

Capture Network Traffic with Network Watcher

What is Azure Network Watcher:

- Regional service that lets you monitor and diagnose network scenario level conditions in, to, and from Azure

Monitoring	Use Azure Network Watcher to monitor communications between VMs and endpoints
Diagnosing	Network Watcher provides several useful diagnostics capabilities.
Reviewing metrics	There are limits to the number of network resources that can be created. After these limits are reached, no more resources can be created.
Managing logs	NSGs deny or allow network traffic to a network interface in a VM. The VNet flow log capability enables you to capture information about traffic.
Create an Azure Network Watcher instance	When you create or update a VNet in your Azure subscription, Network Watcher is automatically enabled.

Demonstration – Log Network Traffic to and from a VM

Enable Network Watcher

Register Insights provider

Enable VNET flow log

Download and view flow log

Learning recap – Implement Windows Server IaaS VM network security

Knowledge Check

Microsoft Learn Modules (learn.microsoft.com/)

Implement Windows Server IaaS VM network security

Audit the security of Windows Server IaaS virtual machines

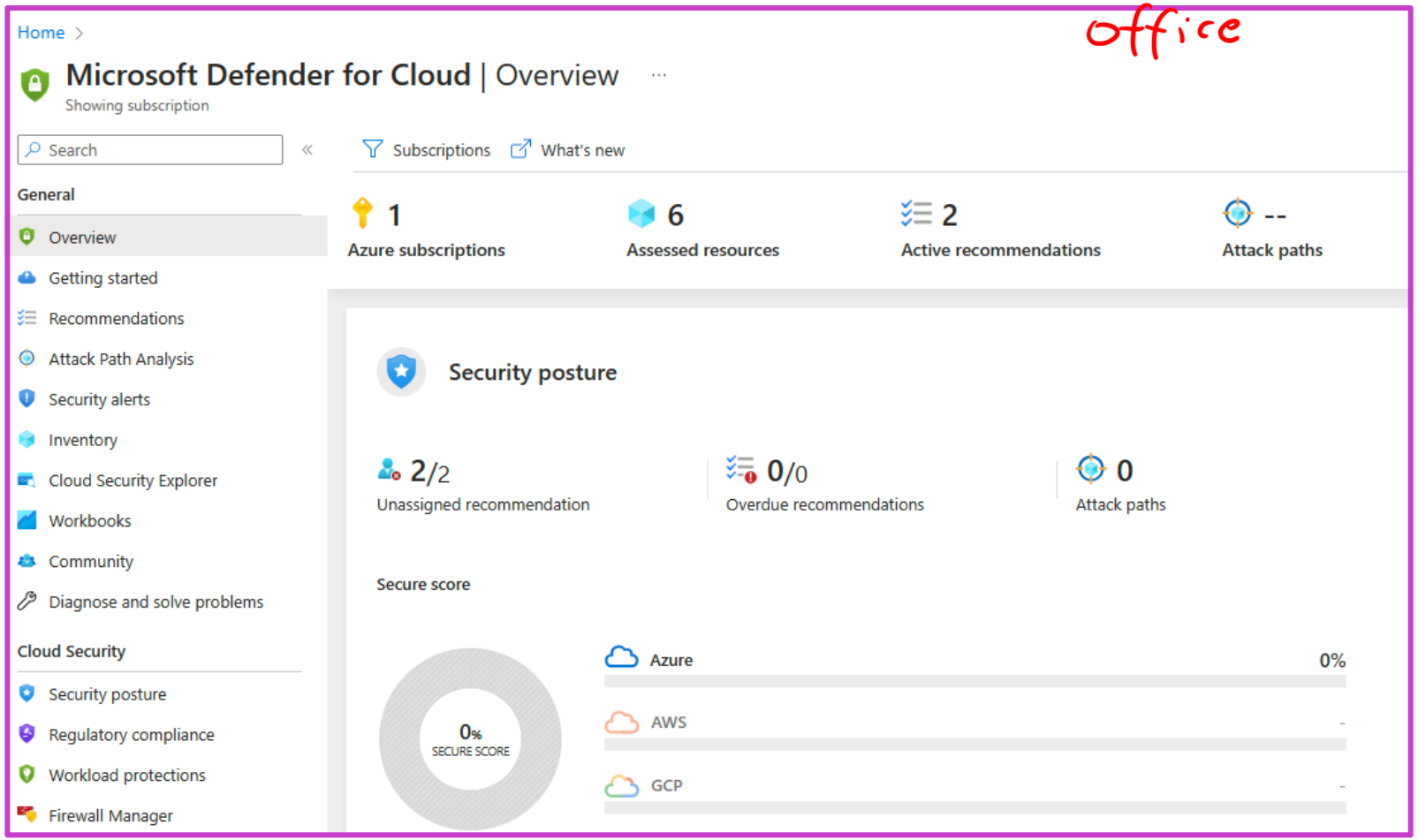
Learning Objectives – Audit Windows Server IaaS VMs

- Describe Microsoft Defender for Cloud
- Enable Microsoft Defender for Cloud in hybrid environments
- Audit your VM's regulatory compliance
- Implement and assess security policies
- Demonstration – Protect your resources with Microsoft Defender for Cloud
- What is Microsoft Sentinel?
- Implement SIEM and SOAR solutions in Microsoft Sentinel
- Learning recap

What is Microsoft Defender for Cloud?

With Microsoft Defender for Cloud capabilities, you can:

- Improve your security posture. In addition to security best practices, you can also track compliance against regulatory standards.
- Protect your environment.
- Protect your data. Defender for Cloud can also perform automatic data classification in your Azure SQL databases.

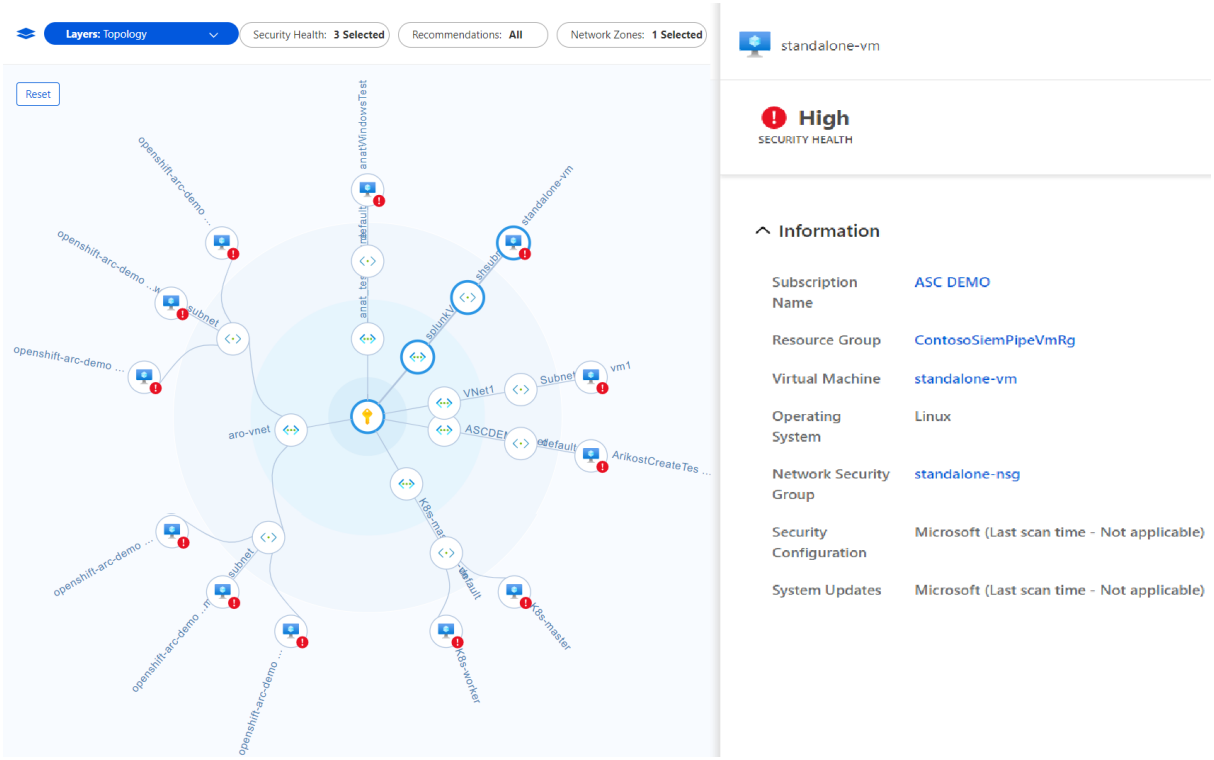


Defender for Cloud feature coverage for VMs

- Microsoft Intune Endpoint Protection assessment
- Missing operating system patches assessment, VM behavioral analytics and security alerts
- Security misconfigurations assessment 、
- Disk encryption assessment, File integrity monitoring, Fileless security alerts, Defender ATP
- Network security assessment, Network map, Network-based security alerts
- Native vulnerability assessment, Third-party vulnerability assessment
- Regulatory compliance dashboard and reports
- Adaptive network controls, Adaptive network hardening
- Just-in-time (JIT) VM access

3383 X

Network map: view of the topology map with security health



Enable Microsoft Defender for Cloud in Hybrid Environments

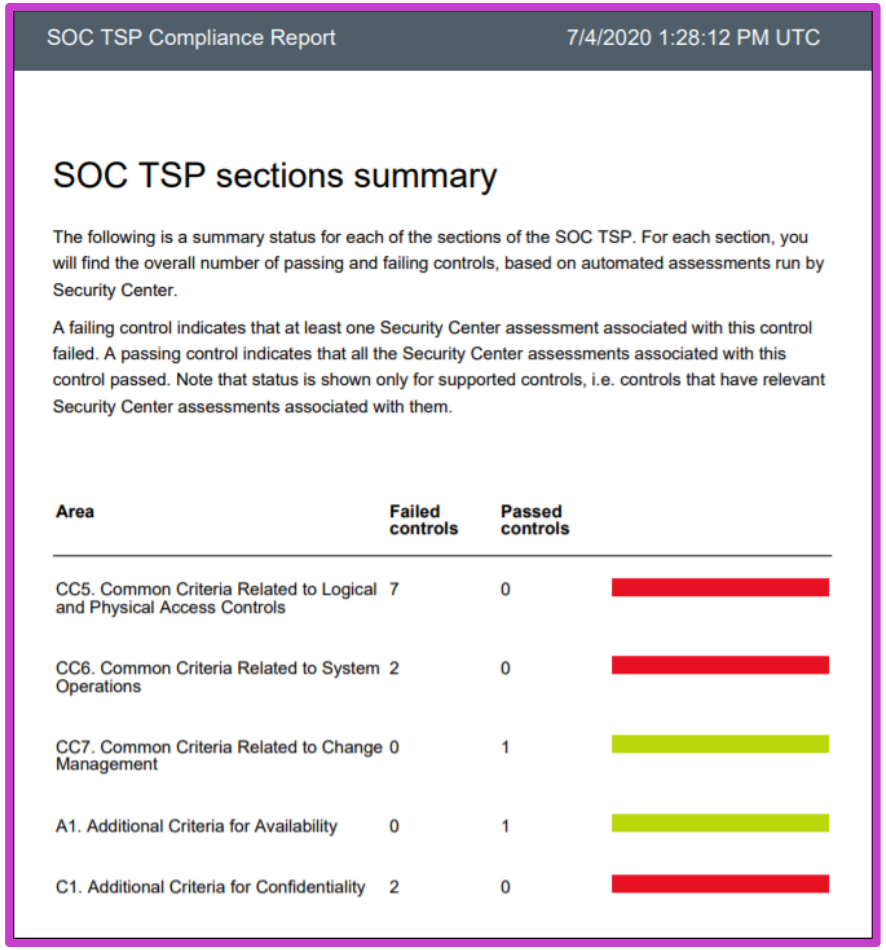
Enable the Defender for Cloud Standard pricing tier

Enable automatic provisioning

Onboard your on-premises servers and computers

Audit your VM's Regulatory Compliance

Compliance standard	Description
PCI DSS 4	The **Payment Card Industry** Data Security Standard (PCI DSS) addresses security issues for organizations that manage credit card payments and is intended to reduce card fraud.
ISO 27001:2022	Part of the **International Standards Organization** (ISO) 27000 family of standards, 27001 defines a system that can bring management to IT systems.
Azure CIS 2.0.0	The **Center for Internet Security** (CIS) is an organization involved in developing best practice for securing It system.
SOC TSP	The **Service Organization Controls** (SOC) framework is a standard for controls that focuses on safeguarding the confidentiality and privacy of information stored and processed in the cloud.



SOC TSP Compliance Report 7/4/2020 1:28:12 PM UTC

SOC TSP sections summary

The following is a summary status for each of the sections of the SOC TSP. For each section, you will find the overall number of passing and failing controls, based on automated assessments run by Security Center.

A failing control indicates that at least one Security Center assessment associated with this control failed. A passing control indicates that all the Security Center assessments associated with this control passed. Note that status is shown only for supported controls, i.e. controls that have relevant Security Center assessments associated with them.

Area	Failed controls	Passed controls
CC5. Common Criteria Related to Logical and Physical Access Controls	7	0
CC6. Common Criteria Related to System Operations	2	0
CC7. Common Criteria Related to Change Management	0	1
A1. Additional Criteria for Availability	0	1
C1. Additional Criteria for Confidentiality	2	0

Implement and Assess Security Policies

Remediate security recommendations

- It's important to do more than just review how your organization compares with security and compliance standards.
- You should also seek to tighten your security to try and meet those standards.
- To access and apply security recommendations, in the Azure portal, in Defender for Cloud, select the Overall Secure Score tile.

Run a vulnerability assessment against your Windows Server IaaS VM

- You can use Defender for Cloud to perform a vulnerability assessment on your VMs.
- First, however, you must install a vulnerability assessment solution on the required resources.

Demonstration – Protect your resources with Defender for Cloud

Access to Defender for Cloud

Explore Policy and Compliance

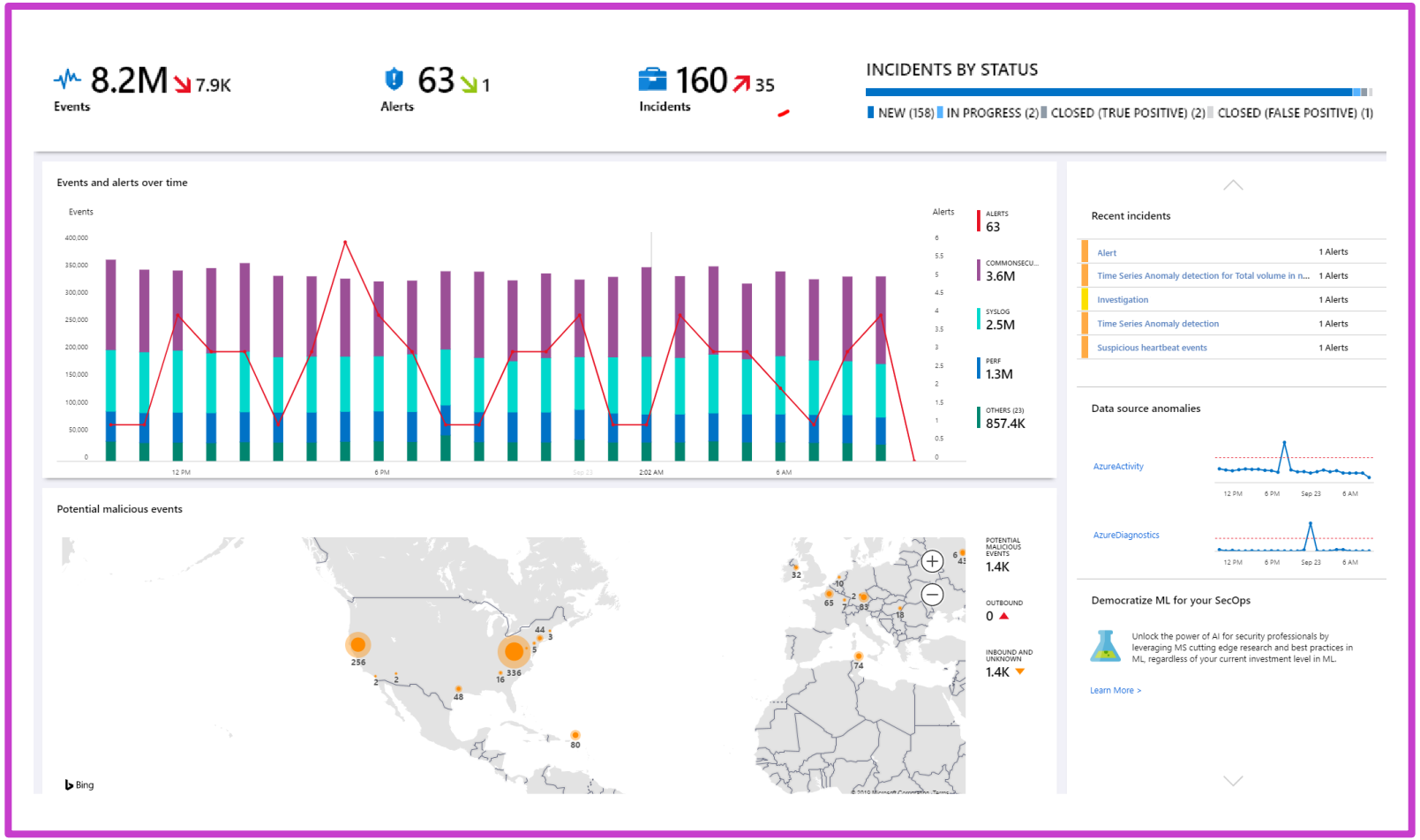
Select Windows Server VM

Install Endpoint protection and enable JIT

What is Microsoft Sentinel?

Sentinel meets the needs of both SIEM and SOAR solutions through:

- Collecting data across cloud-based and on-premises users, devices, apps, and infrastructure.
- Using AI to identify suspicious activity.
- Detecting threats with fewer false positives.
- Responding to incidents quickly and automatically.



Implement SIEM and SOAR solutions in Microsoft Sentinel

What is SIEM?

SIEM solutions store and analyze log data that comes from external sources.

To implement SIEM functionality in Sentinel:

- Enable Microsoft Sentinel.
- Create a data connection.
- Create a custom rule that generates an alert.

What is SOAR?

SOAR solutions enable you to manage or orchestrate analysis of data that you have collected about security threats.

Use the following best practices to implement SOAR in Sentinel:

- When you create analytics rules that raise alerts, also configure them to create incidents.
- Use the incidents to manage the investigation and response process.
- Group related alerts into an incident.

Learning recap – Audit the security of Windows Server IaaS Virtual Machines

Knowledge Check

Microsoft Learn Modules (learn.microsoft.com/)

Audit the security of Windows Server IaaS Virtual Machines

Manage Azure VM updates

Learning Objectives – Manage Azure updates

- Overview of Azure Update Manager
- How Azure Update Manager works
- Configure Azure Update Manager settings
- Manage pending updates
- Review update history and Azure Update Manager policies
- Reporting with Azure Update Manager
- Demonstration – Implementing updates
- Learning recap

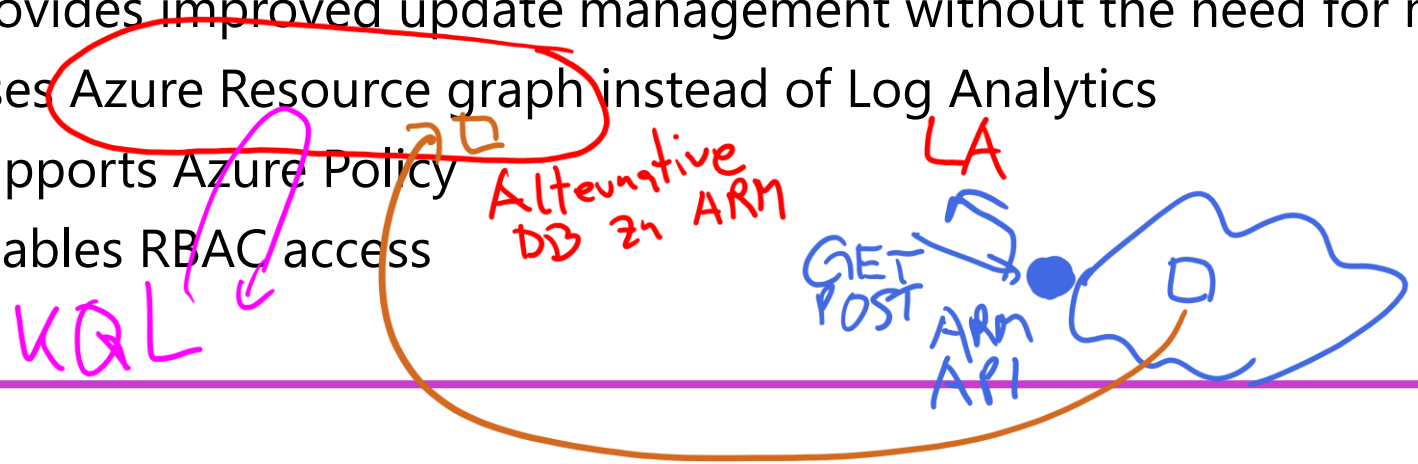
Azure Update Manager

Azure Update Manager manages updates for Azure Arc enabled servers (including on-premises and virtual machines deployed in other clouds).

You can use Azure Update Manager in conjunction with WSUS or instead of WSUS to manage updates on your servers, both Azure VMs and on-premises servers

What is Azure Update Manager?

- Provides improved update management without the need for machine on-boarding
- Uses Azure Resource graph instead of Log Analytics
- Supports Azure Policy
- Enables RBAC access



Describe the Process of Update Management

Update Management capabilities

Update Management includes the following capabilities related to on-premises servers:

- Check status of updates on your servers
- Configure dynamic groups of machines to target
- Search Azure Monitor logs

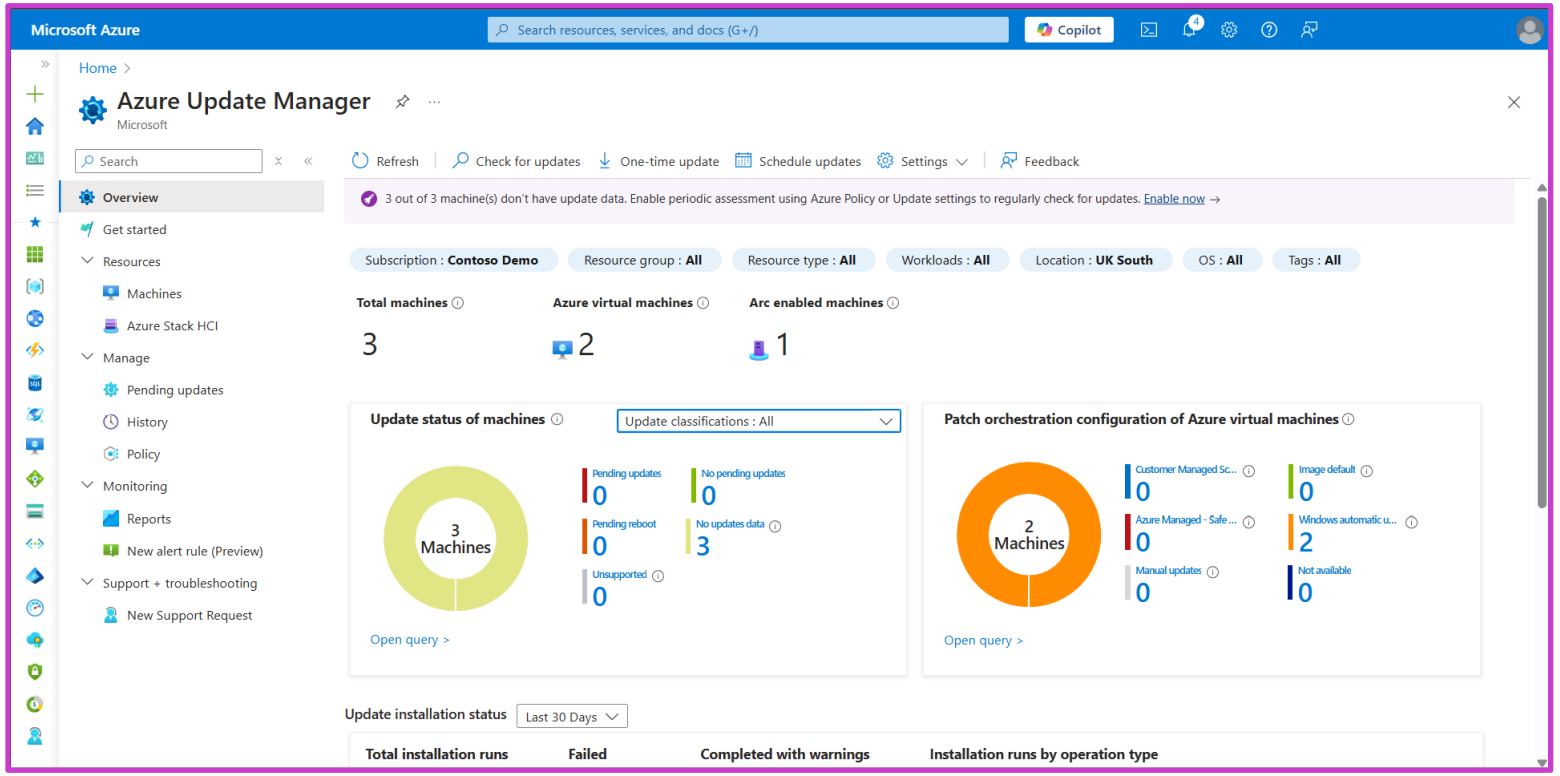
Onboarding your on-premises or cloud servers

- Onboard your on-premises virtual machines to Azure Arc
- On-board virtual machines in other clouds to Azure Arc
- The required Azure Update Manager VM extension is added when you perform an operation in Update Manager

Overview of Azure Update Manager

Update Manager:

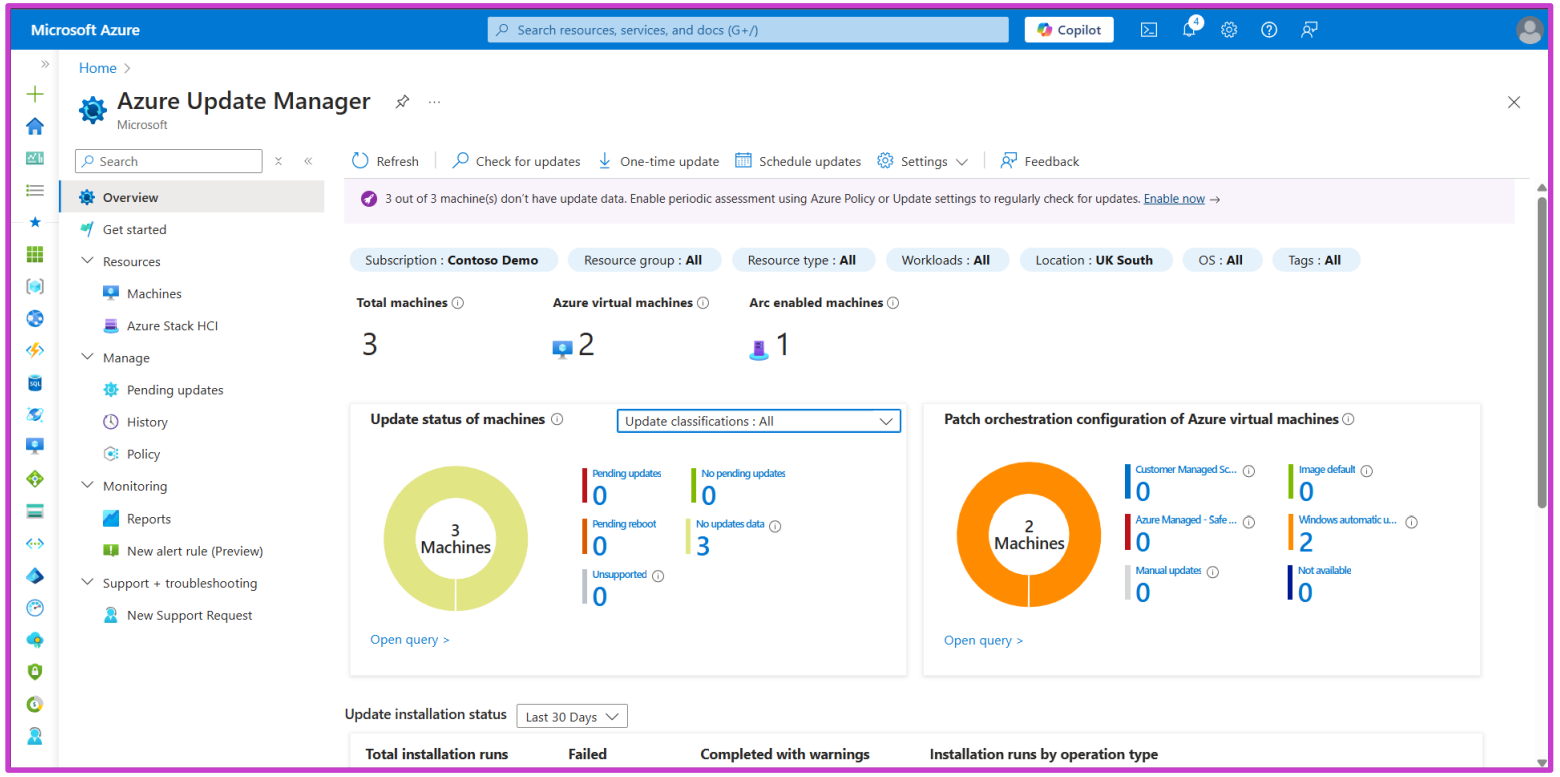
- Helps you manage and govern updates for all your machines
- Supports both Windows and Linux
- Enables you to manage updates for:
  - Azure VMs
  - VMs hosted in other cloud platforms (via Azure Arc)
  - On-premises devices (via Azure Arc)
- Supports update management for the following:
  - Hybrid machines
  - VMWare machines
  - SCVMM machines
  - Azure Local VMs



Features of Azure Update Manager

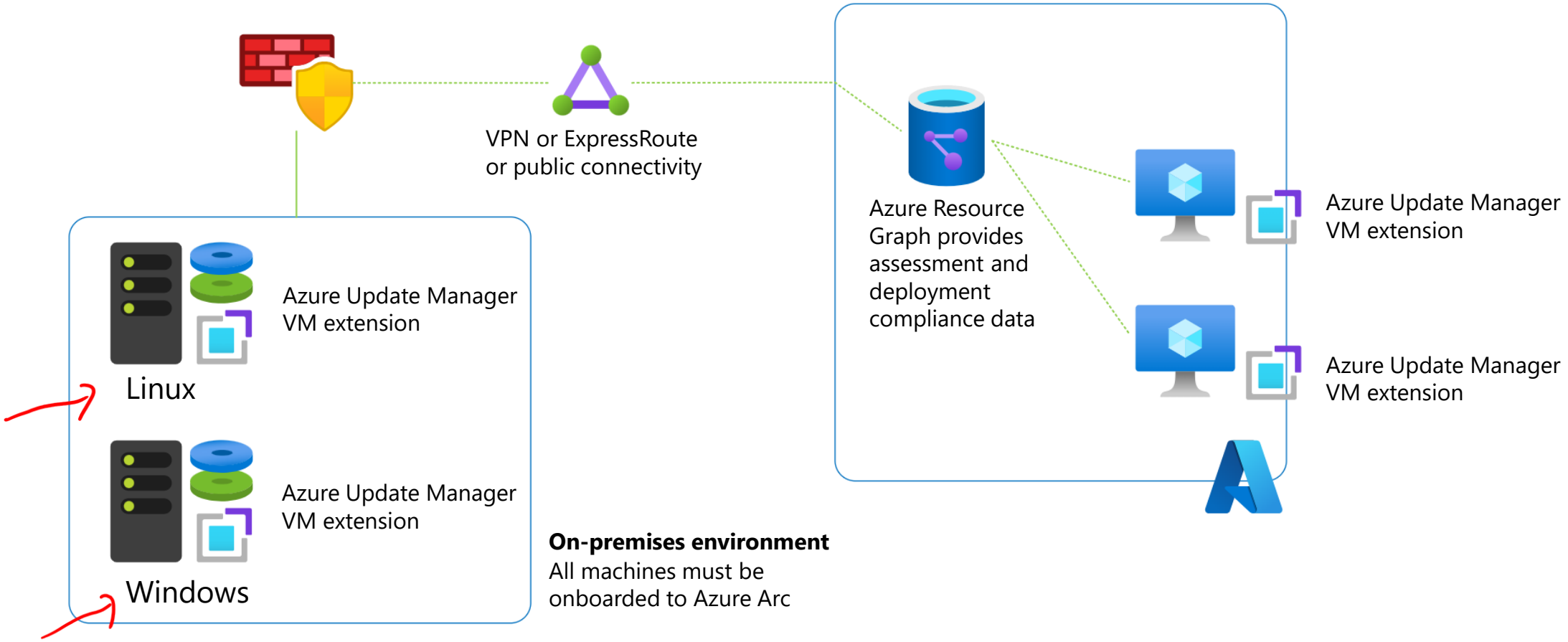
By using Update Manager, you can:

- Check for updates, both automatically and on-demand
- Deploy updates immediately or schedule the deployment
- Enable periodic update assessments
- Implement maintenance schedules for your machines
- Enable automatic VM guest patching and hot patching for Azure VMs
- Generate reports and configure alerts
- Manage machine compliance for all connected machines (Azure or Azure Arc-enabled)



How Azure Update Manager works

The following graphic depicts the key elements of the Update Manager architecture



Azure Update Manager RBAC roles and permissions

To manage an Azure VM (or an Azure Arc-enabled server) using Azure Update Manager, you must have the appropriate roles assigned. These are:

- **Azure VM**. You must hold the Azure Virtual Machine Contributor or Azure Owner role on the VM
- **Azure Arc-enabled server**. You must be assigned to the Azure Connected Machine Resource Administrator role.

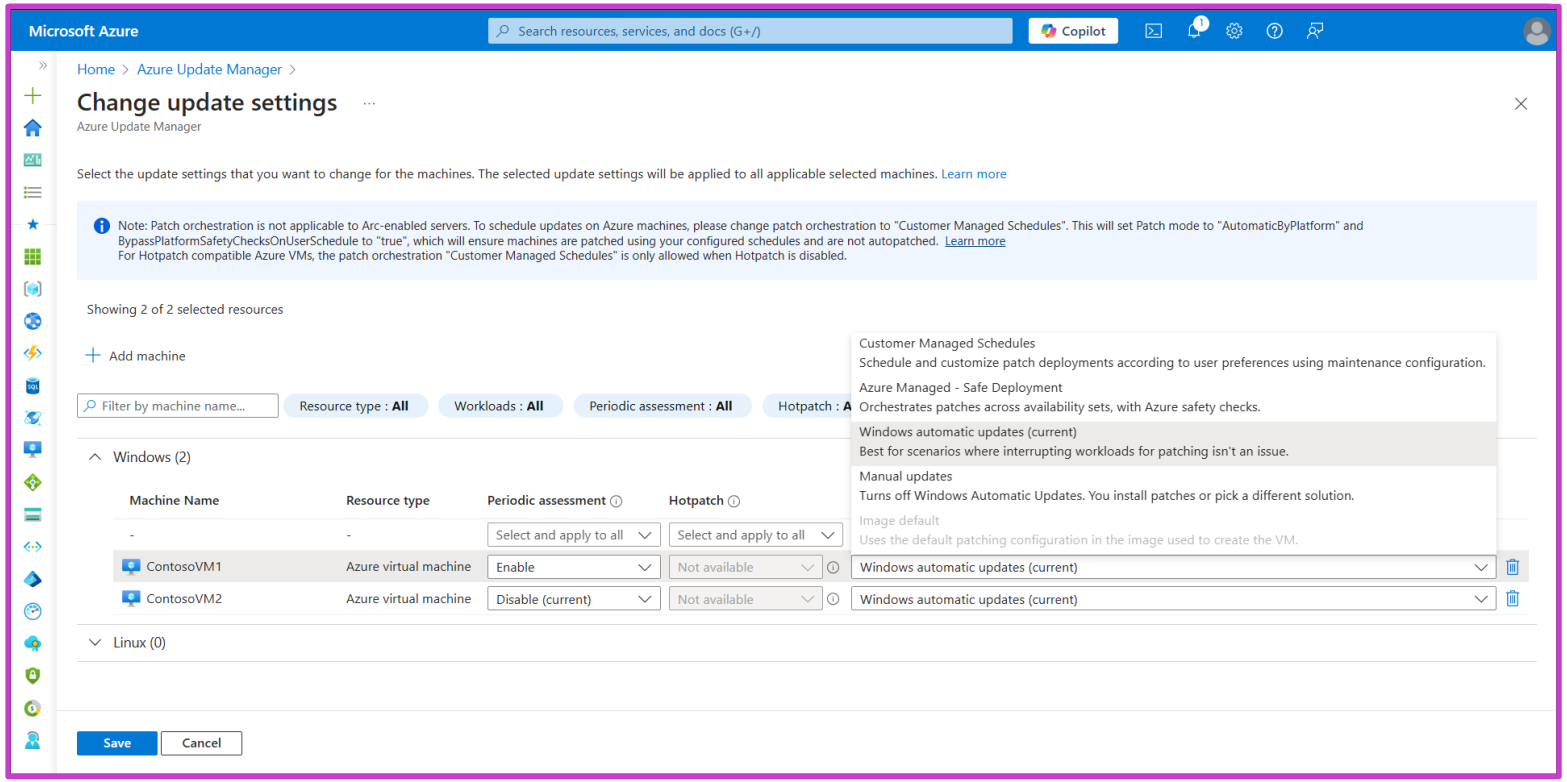
You need a range of specific permissions to perform the various management tasks in Update Manager:

- Read permissions for Update Manager to view Update Manager data
- Permissions to perform on-demand actions in Azure Update Manager
- Permissions to manage scheduled patching (Maintenance configuration)

Configure Azure Update Manager settings

Available options for update settings:

- **Periodic assessment**. When enabled, an update assessment occurs automatically every 24 hours.
- **Hotpatch**. Enables you to install security updates on Windows Server Azure Edition machines and supported Arc machines with fewer reboots.
- **Patch orchestration**. You choose between:
  - Customer managed schedules
  - Azure managed – safe deployment
  - Windows automatic updates
  - Manual updates



Selecting the appropriate patch orchestration option

Customer managed schedules

- Enables you to define the schedule in accord with your organization's maintenance schedules and user preferences

Azure managed – safe deployment

- Orchestrates patches across Azure availability sets to ensure safer deployments

Windows automatic updates

- Provides patching to machines where interrupting workloads isn't a factor

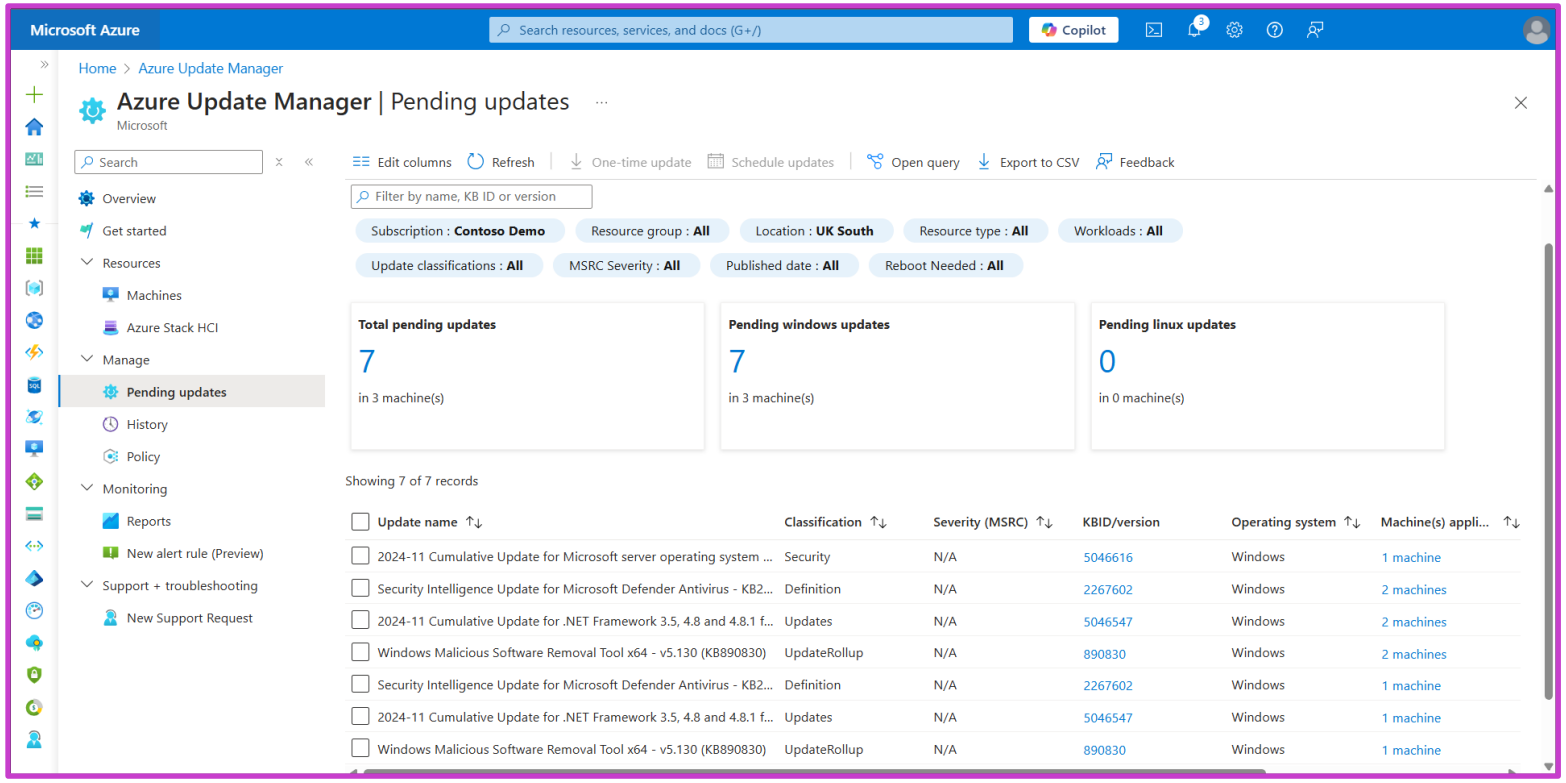
Manual updates

- Disables Windows Automatic Updates enabling you to manually schedule and apply patches

Manage pending updates

Pending updates

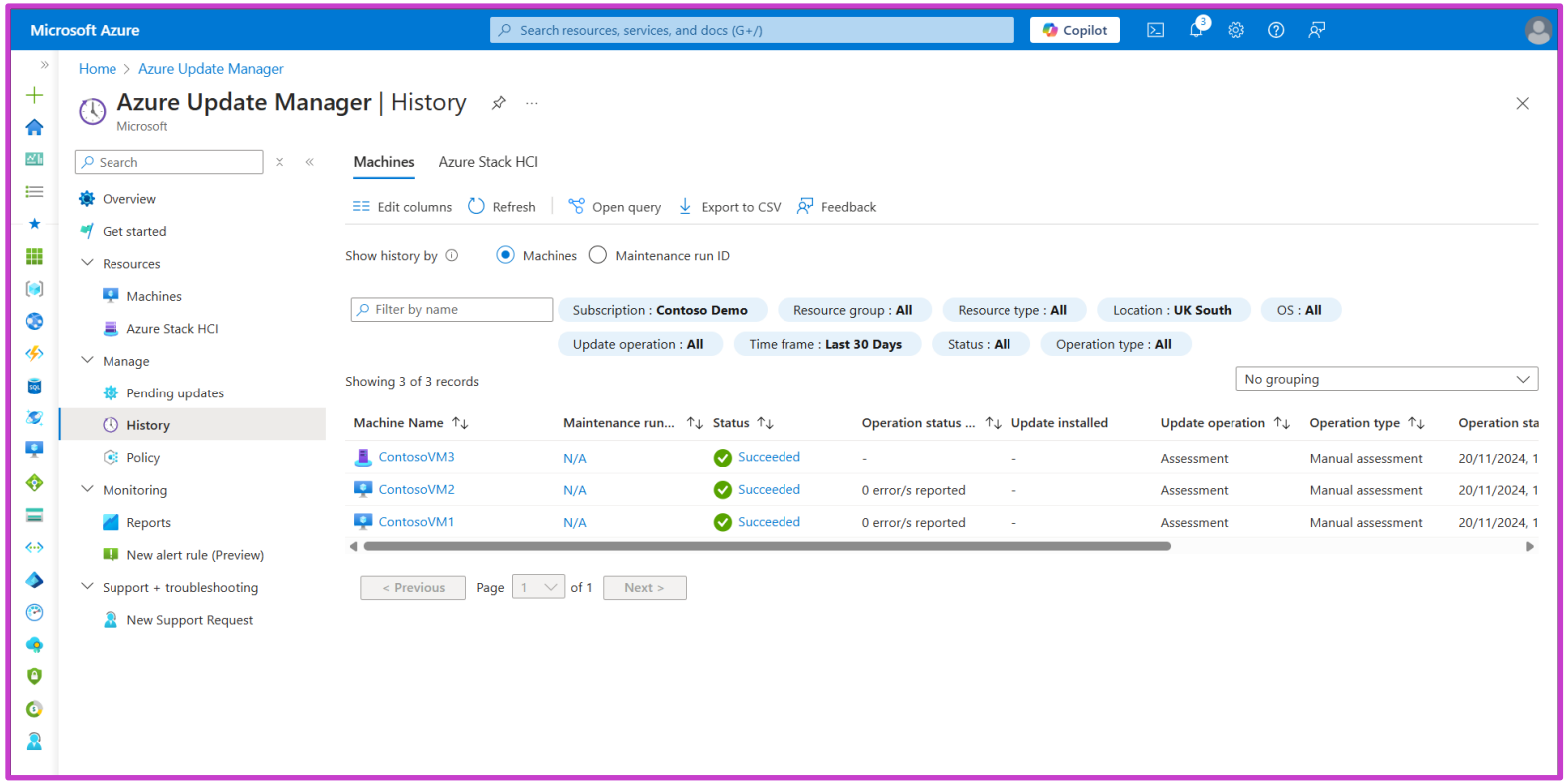
- You can use the Pending updates page to review the various pending updates and the machines to which they apply
- You can then choose to apply a one-time update or schedule the pending updates for the targeted machines



Review update history

History

- From the History page, you can review the current update status for your machines
- You can select specific machine(s) to review their update history

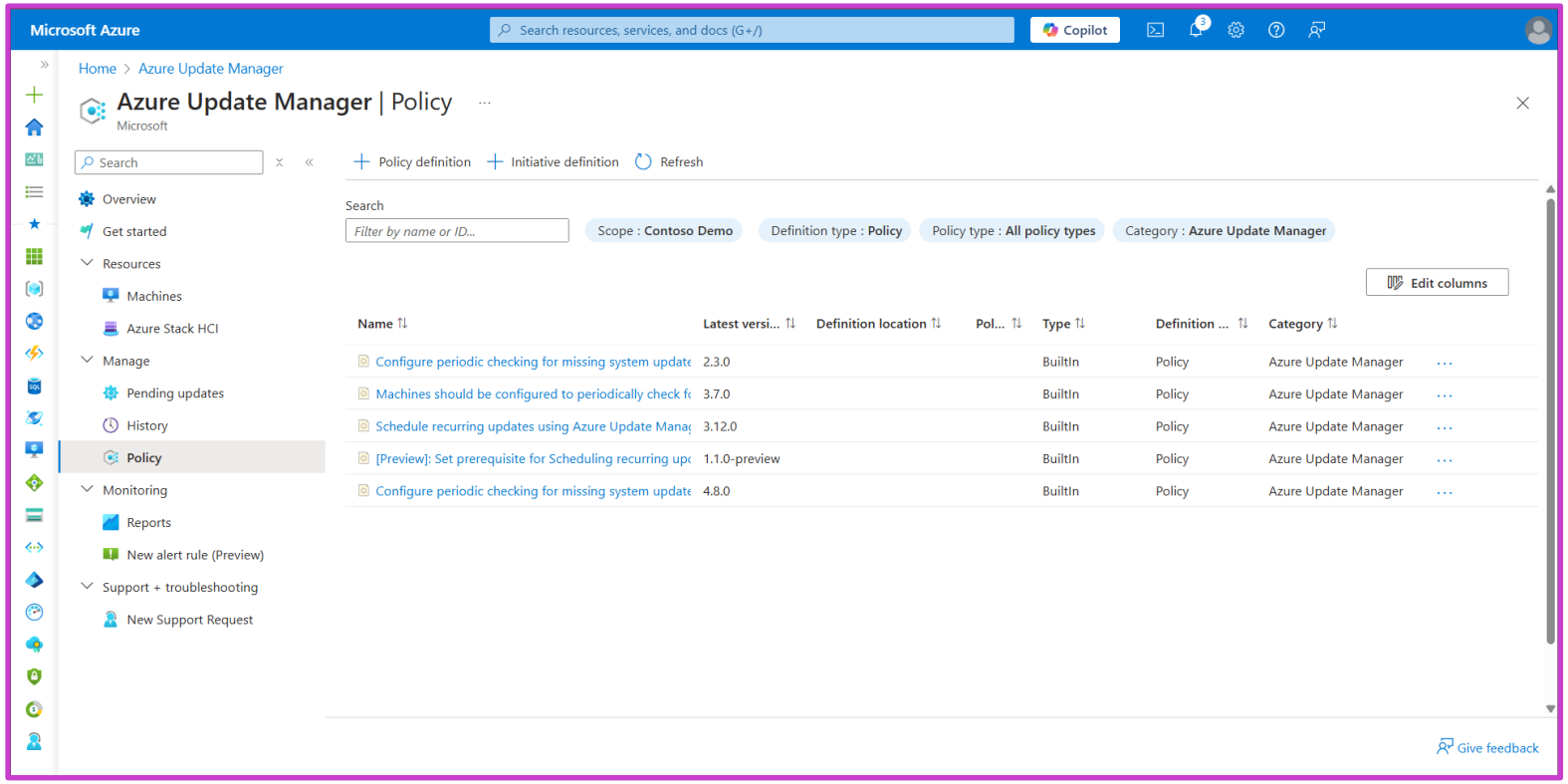


Review Azure Update Manager policies

Policy

There are five default built-in policies for Azure Update Manager:

- Configure periodic checking for missing system updates on azure Arc-enabled servers
- Machines should be configured to periodically check for missing system updates
- Schedule recurring updates using Azure Update Manager
- [Preview]: Set prerequisite for Scheduling recurring updates on Azure virtual machines
- Configure periodic checking for missing system updates on azure virtual machines

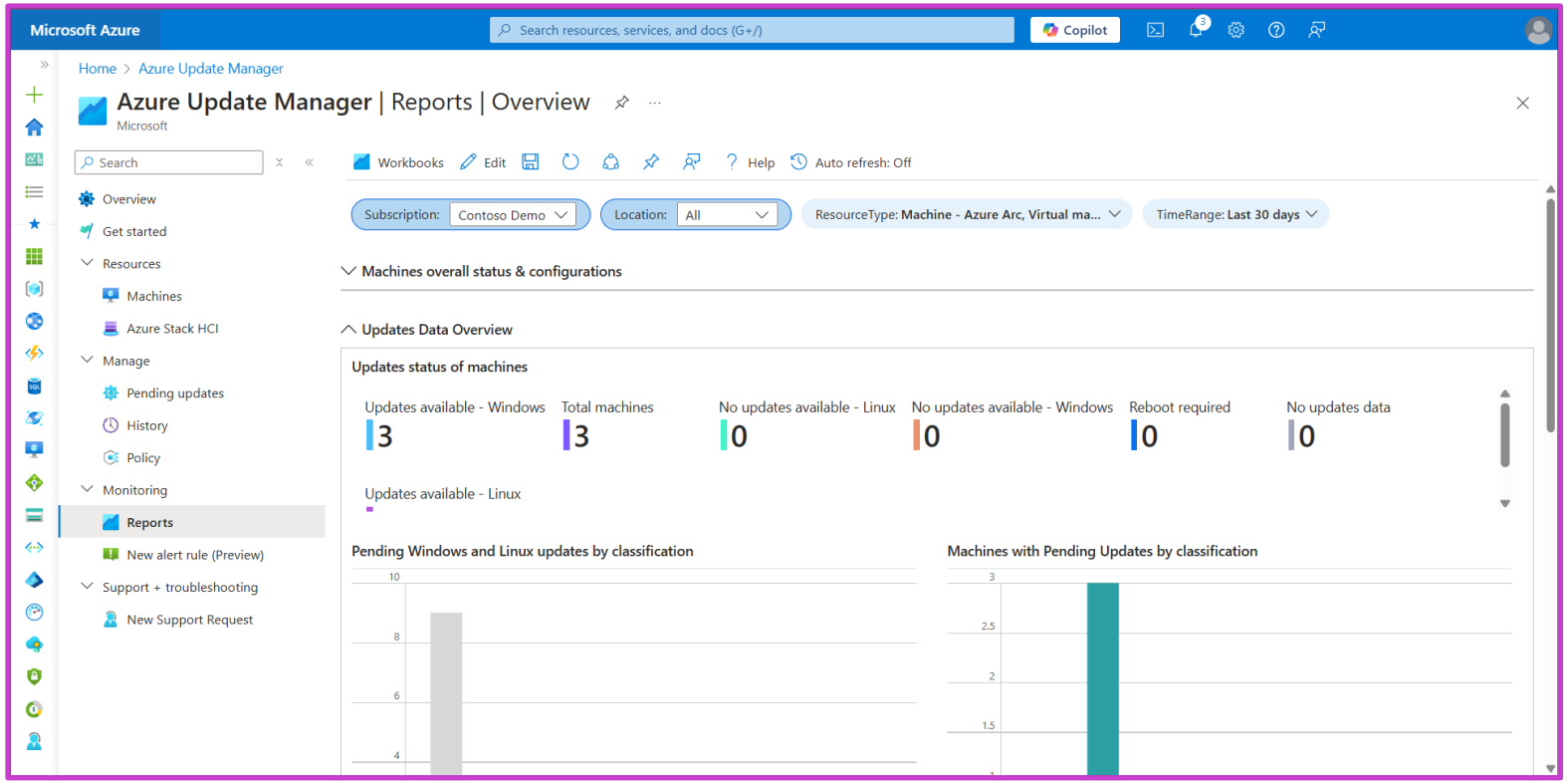


You can review and assign these policies with Azure Update Manager

Reporting with Azure Update Manager (1 of 2)

Reports Gallery

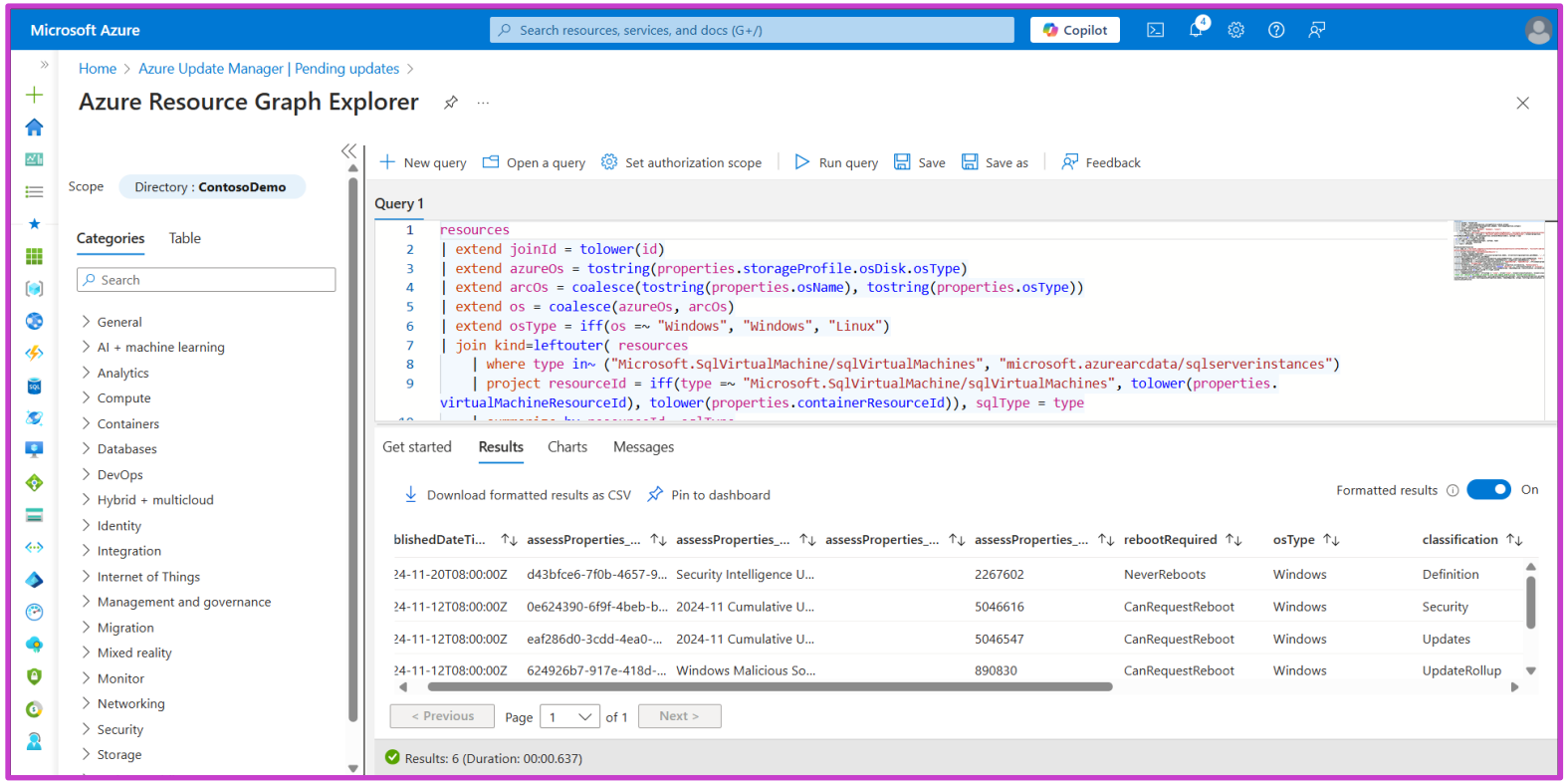
- The reports gallery provides you with a way of reviewing your organization's update environment and status
- You can use predefined templates or create your own templates to generate the desired report(s)



Reporting with Azure Update Manager (2 of 2)

Resource Graph Explorer

- You can also create queries using **Resource Graph Explorer** to understand more about your organization's updates
- To access Resource Graph Explorer, select the Open query link, for example on the Pending updates page



Demonstration – Implementing updates with Azure Update Manager

Review Azure Update Manager

Review machines and run a query

Check for pending updates

Perform a one-time update and then review update history

Learning recap – Manage Azure VM updates

Knowledge Check

Microsoft Learn Modules (learn.microsoft.com/)

Manage Azure VM updates

Configure BitLocker disk encryption for Windows IaaS virtual machines

Learning Objectives – BitLocker disk encryption for Windows IaaS VMs

- Describe Azure Disk Encryption and server-side encryption
- Configure Key Vault for Azure Disk Encryption
- Encrypt Azure IaaS Virtual Machine hard disks
- Back up your Azure Disk Encryption–protected VMs
- Restore your Azure Disk Encryption–protected VMs
- Decrypt a disk
- Learning recap

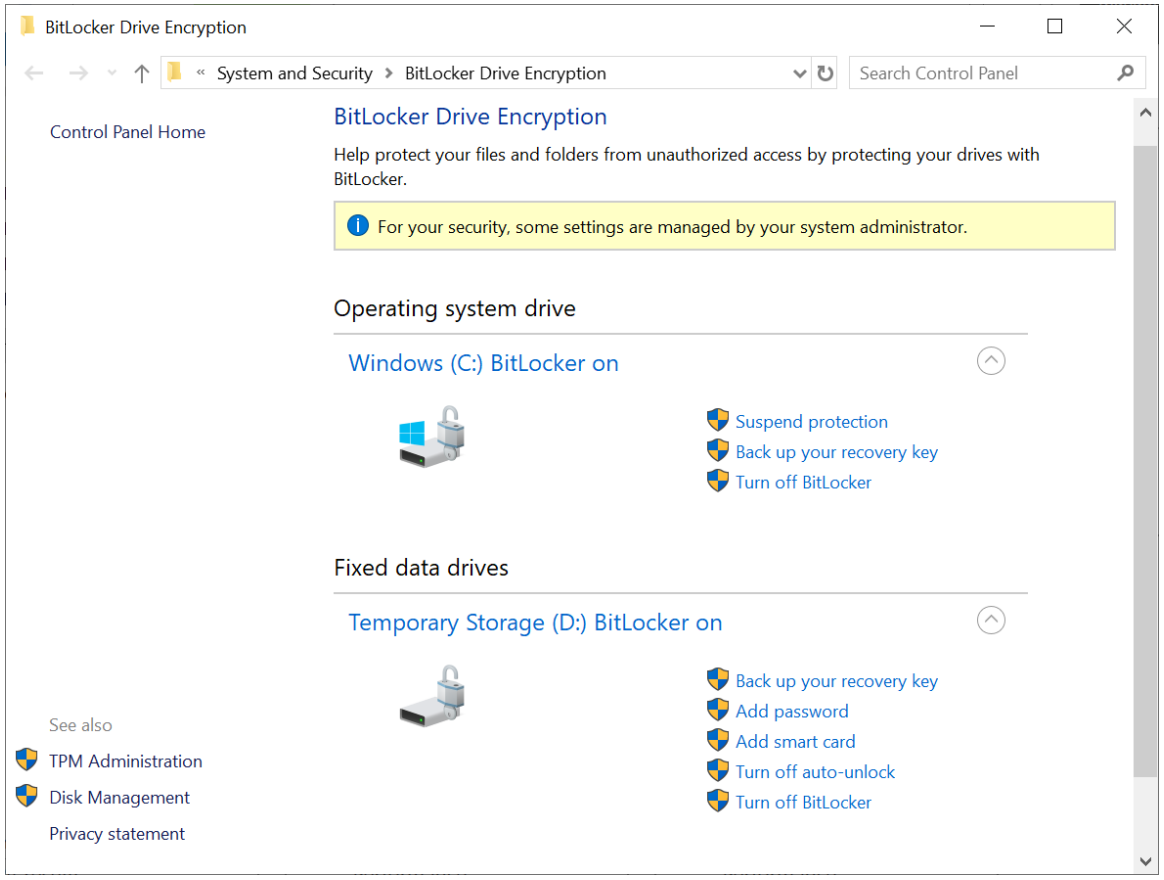
Describe Azure Disk Encryption and server-side encryption

Azure Disk Encryption:

- For Windows, Azure Disk Encryption uses BitLocker Drive Encryption.
- For Linux, Azure Disk Encryption uses DM-Crypt.

Server-side encryption of Azure-managed disks:

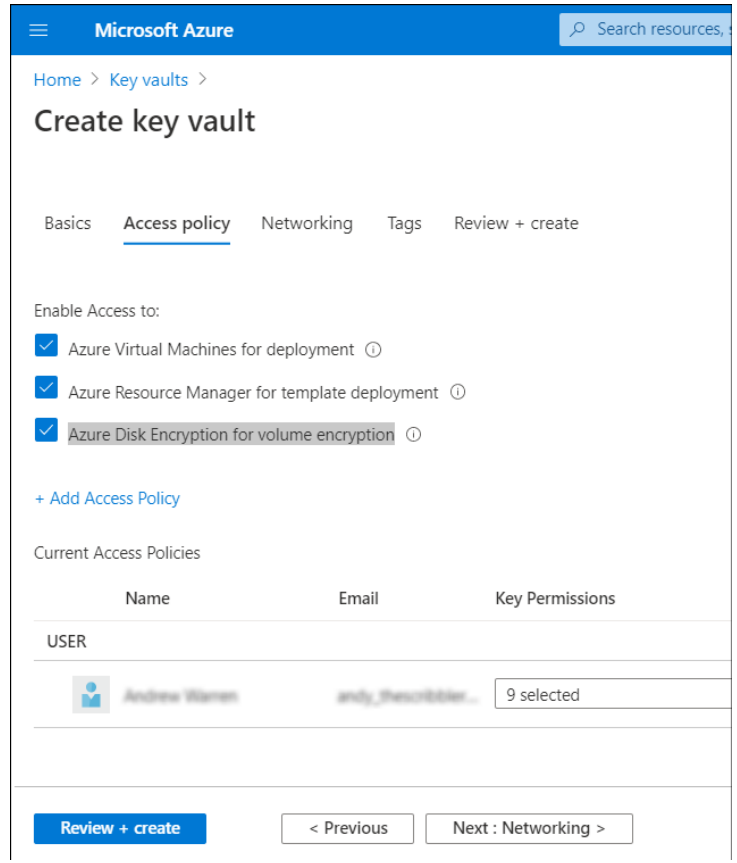
- Supports Generation 2 Azure VMs and all existing Azure VM sizes
- It is automatic



Configure Key Vault for Azure Disk Encryption

There are three steps required to configure a key vault:

1. **Create a resource group.** This is an optional step. You can create a resource group to host your key vault or use one which already exists.
2. **Create a key vault and allow KeyVault to be used for Disk Encryption.**
3. **Set the key vault advanced access policies**. Azure requires access to the encryption keys or secrets in your key vault. This enables Azure to make them available to the VM for starting and decrypting the volumes.



Encrypt Azure IaaS Virtual Machine Hard Disks

Azure Portal

1. On the Virtual machine blade, in the navigation pane, in the Settings section, select **Disks**.
2. On the Disks blade, select **Encryption**.
3. Select the **Select a key vault and key for encryption** link.
4. To create a key, in the Key section, select **Create new**.
5. Enter a Name for the key, specify the Key Type and RSA Key Size, and then select **Create**.
6. On the Select key from Azure Key Vault blade, select a version from the Version drop-down list (or create a new version), and then select `**Select**`.

Bash PowerShell

Use Azure CLI to encrypt a VM

```
az vm encryption enable \
  -g ContosoResourceGroup  \
  --name ContosoVM1  \
  --disk-encryption-keyvault ContosoADEKeyVault
```

PowerShell Only

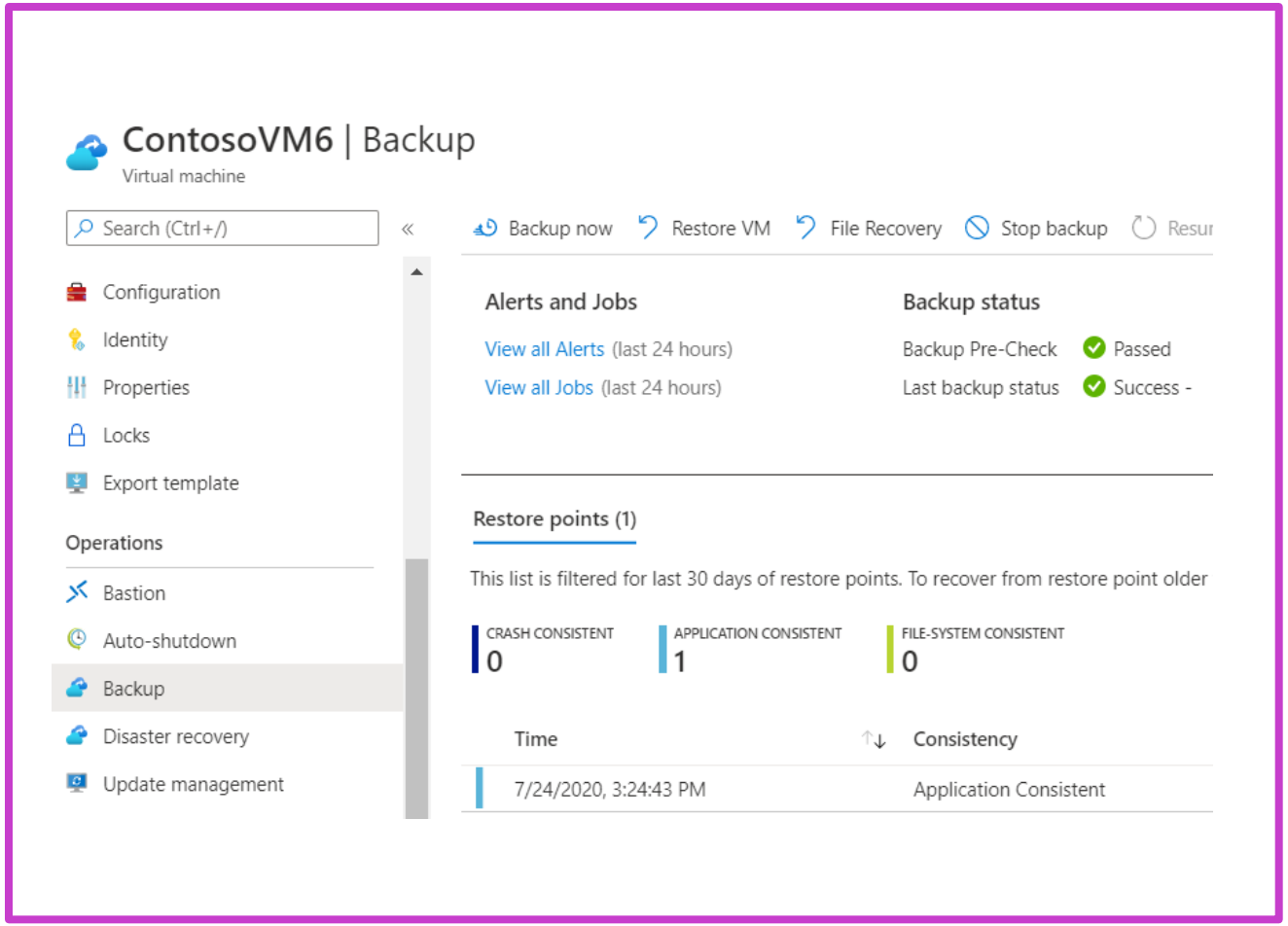
Use PowerShell to encrypt a VM

```
$KeyVault = Get-AzKeyVault `
  -VaultName ContosoADEKeyVault `
  -ResourceGroupName ContosoResourceGroup

Set-AzVMDiskEncryptionExtension
  -ResourceGroupName MyResourceGroup `
  -VMName ContosoVM1 `
  -DiskEncryptionKeyVaultUrl $KeyVault.VaultUri `
  -DiskEncryptionKeyVaultId $KeyVault.ResourceId
```

Back up your Azure Disk Encryption–protected VMs

- On the **Recovery Services Vault** blade, select **Backup**.
- On the **Backup Goal** blade, specify the location of your workload.
- On the **Backup** blade, in the Policy section, select a **backup policy**
- In the **Virtual Machines** section, select **Add**.
- In the **Select virtual machine** blade, select the encrypted VMs, and then select OK.
- On the **Backup** blade, select Enable **Backup**.
- On the **Backup Goal** blade, select **Backup**.
- You can force a manual backup of a protected VM by selecting that VM on the Virtual machines blade in the Azure portal.

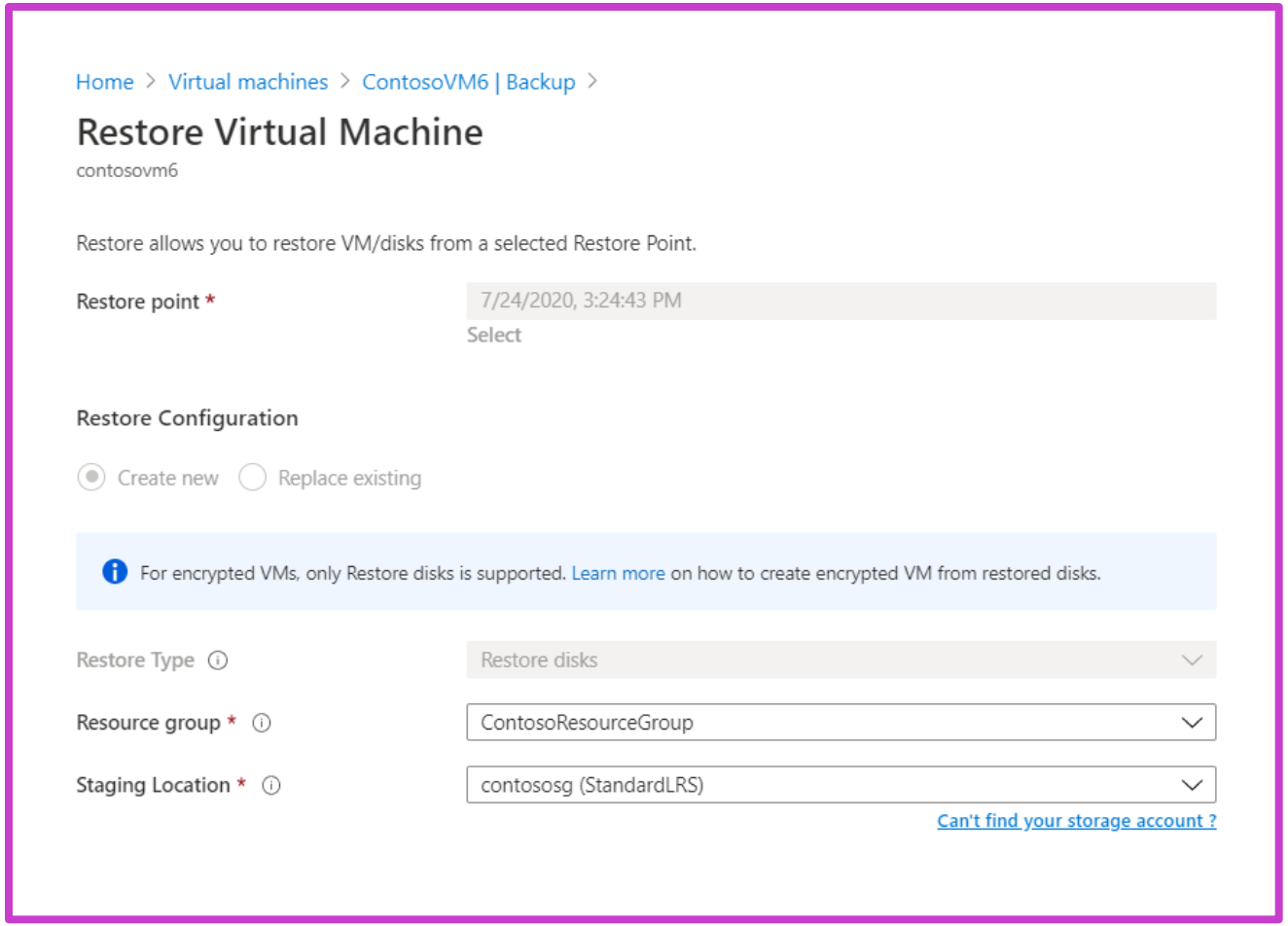


Restore your Azure Disk Encryption–protected VMs

Use the following procedure to restore the VM:

1. In the Azure portal, on the **Virtual machines** blade, select the VM you want to recover.
2. On the **Backup** blade, in the **Operations** section, select **Backup**, and then review the available Restore points.
3. In the **Restore points** section, select the appropriate restore point, and then select the ellipsis button.
4. Select **Restore VM**.
5. Select a **Staging** location, and then select **Restore**.

Note: File-level restore is not supported.



Decrypt a disk

You can decrypt a disk by using either the Azure CLI, PowerShell, or the Azure portal.

Use Azure CLI

```
az vmss encryption disable --resource-group ContosoResourceGroup \
   --name ContosoVM6
```

Use PowerShell

```
Disable-AzVMDiskEncryption -ResourceGroupName ContosoResourceGroup `
   -VMName ContosoVM6
```

Use the Azure portal

1. In the Azure portal, navigate to your **VMs**, and then select the appropriate VM.
2. On the **Virtual machine** blade, in the navigation pane, in the **Settings** section, select **Disks**.
3. On the Disks blade, select **Encryption**.
4. On the Encryption blade, from the Disks to encrypt list, select **None**, and then select **Save**.

Demonstration – Create and encrypt a Windows VM (Azure CLI)

Prepare Cloud Shell to run Azure CLI commands

Provision KeyVault with enabled Disk Encryption

Enable Encryption for disk of the VM from Azure CLI

Check Result

Learning recap – Configure BitLocker disk encryption for Windows IaaS Virtual Machines

Knowledge Check

Microsoft Learn Modules (learn.microsoft.com/)

Configure BitLocker disk encryption for Windows IaaS Virtual Machines

Lab 02: Implementing Security Solutions in Hybrid Scenarios

Lab 02 – Implementing Security Solutions in Hybrid Scenarios

Lab scenario

To identify Microsoft Azure security-related integration features with which you can further enhance your on-premises and cloud security environment, you have decided to onboard Windows servers in your proof-of-concept environment into Microsoft Defender for Cloud. You also want to integrate on-premises servers and Azure VMs running Windows Server with various Azure features, including Inventory, Change tracking, and Update management.

Objectives

- Create an Azure Log Analytics workspace.
- Configure Microsoft Defender for Cloud.
- Provision Azure VMs running Windows Server.
- Onboard on-premises Windows Server into Microsoft Defender for Cloud and Azure Update Manager.

End of presentation