



AZ-801

# Configuring Windows Server Hybrid Advanced Services



# AZ-801 Course Outline

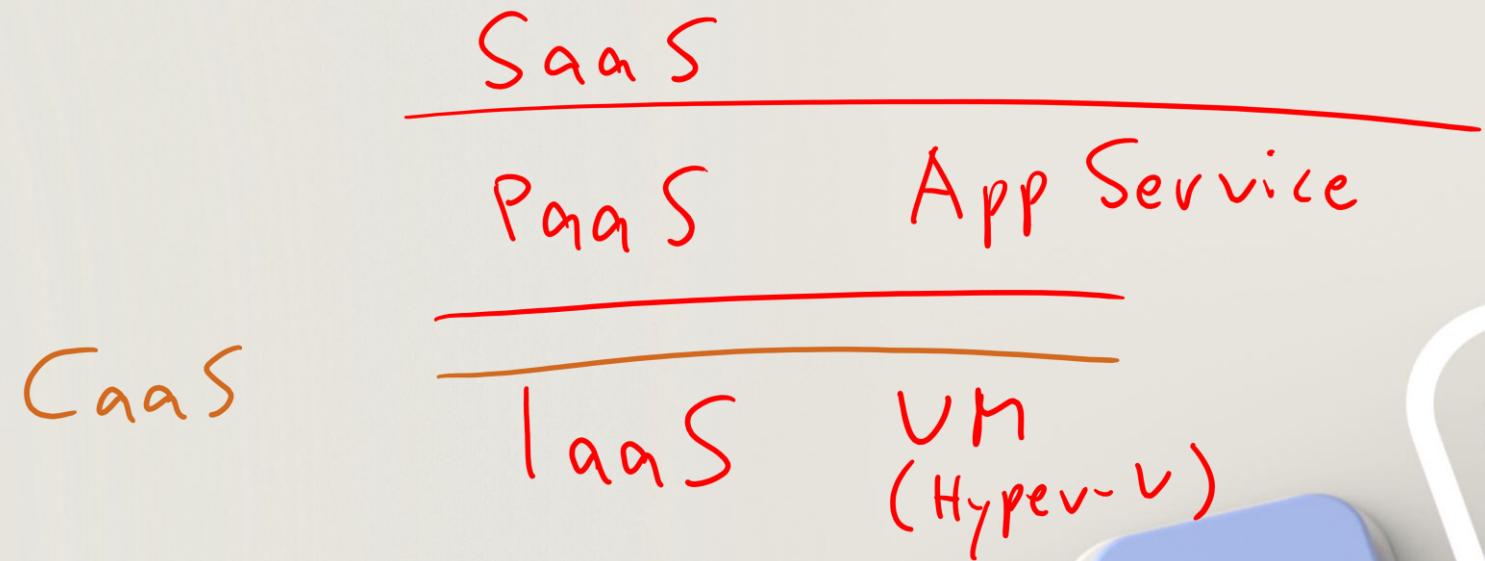
- 1 Windows Server Security on Prem
- 2 Windows Server Security Cloud
- 3 Failover Cluster
- 4 Disaster Recovery on Prem
- 5 Disaster Recovery Cloud
- 6 Windows Server Upgrade and Migrate
- 7 Migrate Windows Server to Cloud
- 8 Windows Server Monitoring
- 9 Monitoring in the Cloud

LP 1

# Secure Windows Server on-premises and Hybrid Infrastructures

*(Implementing Security Solutions in Hybrid Scenarios)*

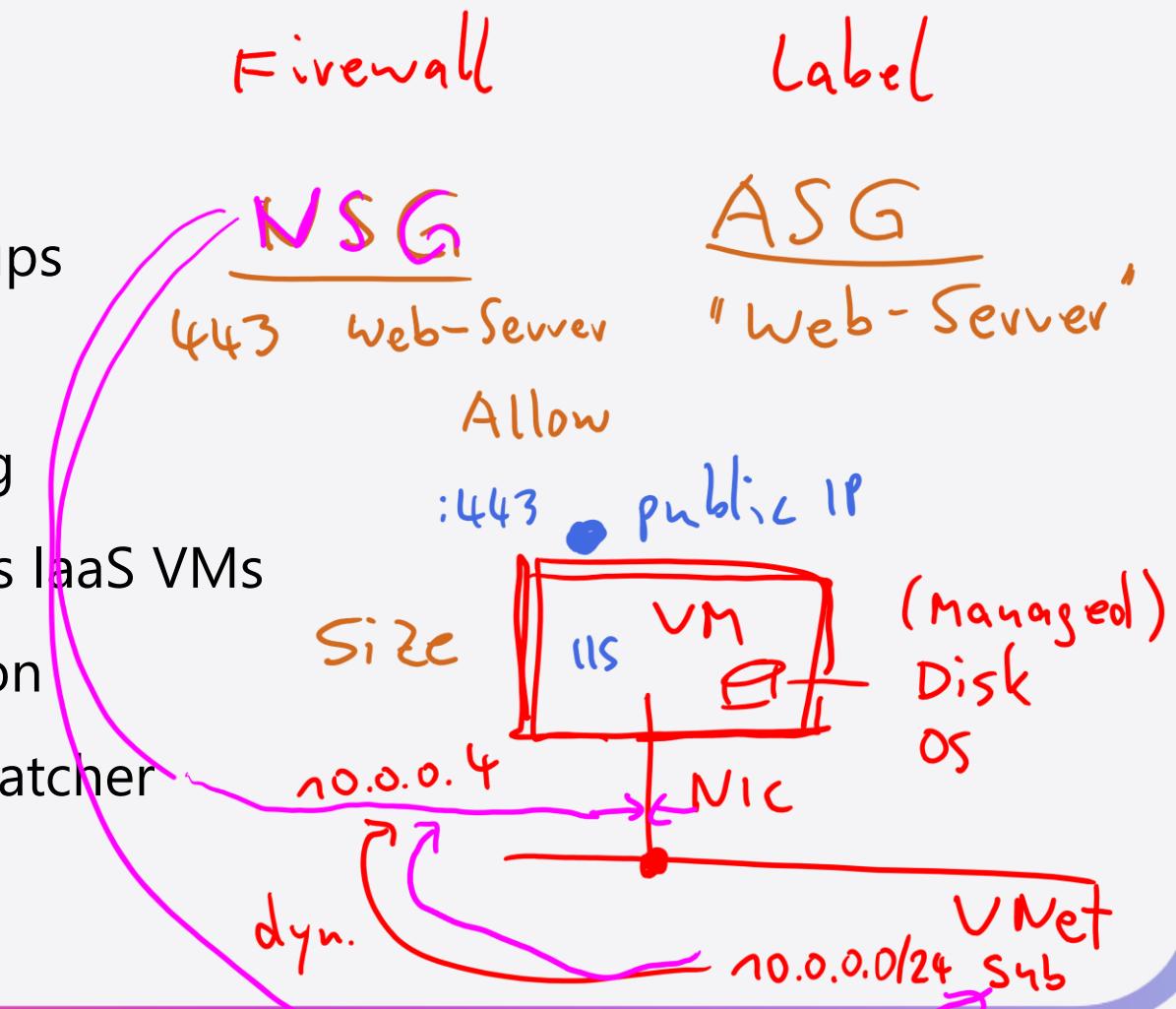
- Implement Windows Server IaaS VM network security |
- Audit the security of Windows Server IaaS Virtual Machines
- Manage Azure updates
- Create and implement application allowlists with adaptive application control
- Configure BitLocker disk encryption for Windows IaaS Virtual Machines
- Implement change tracking and file integrity monitoring for Windows IaaS VMs
- 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 adaptive network hardening
- Implement Azure Firewall and Windows IaaS VMs
- Choose the appropriate filtering solution
- Capture network traffic with network watcher
- Learning recap

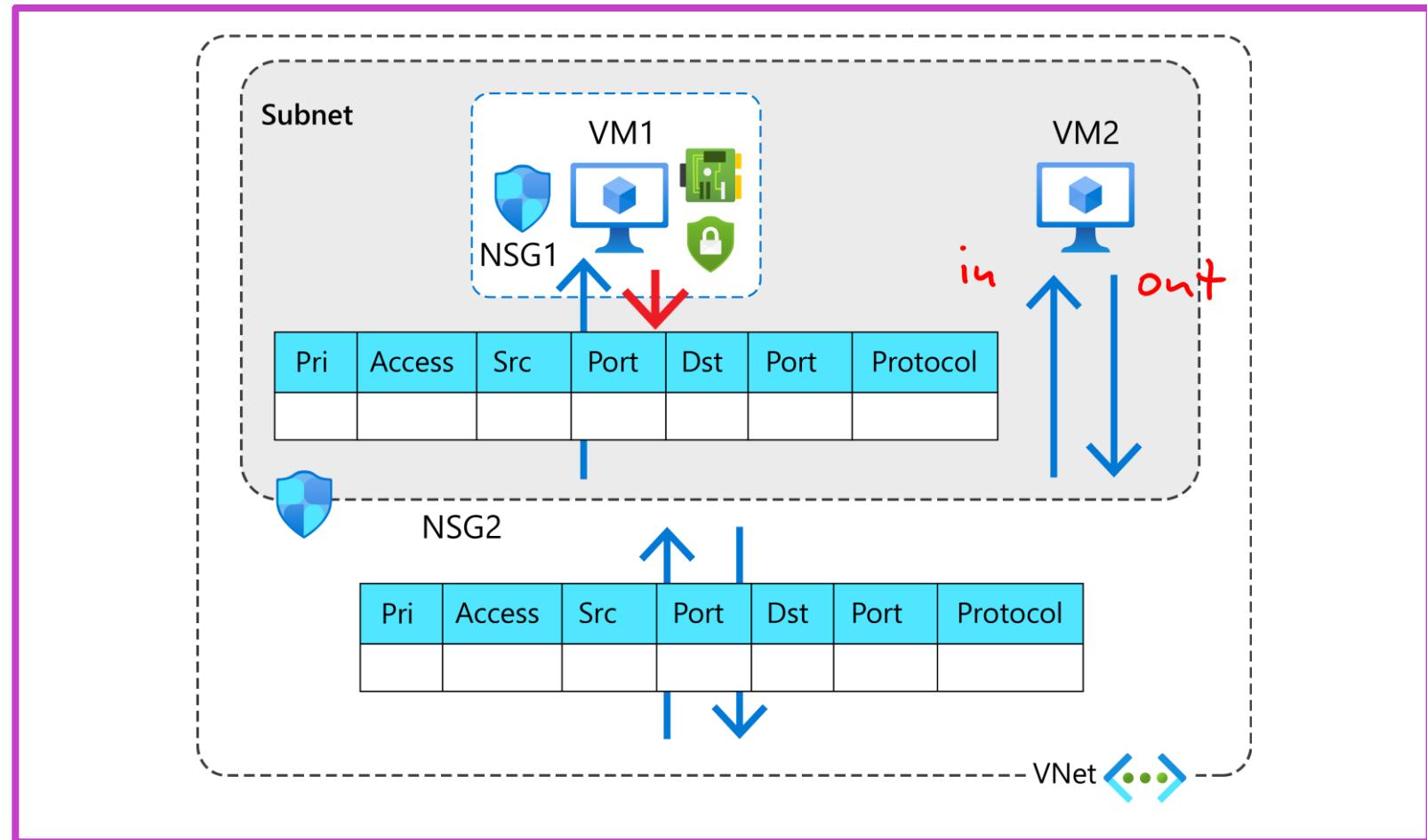


# Implement Network Security Groups

Stateful

Network security groups (NSG) 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.
- NSG is applied to the **subnet** (NSG2) and **network interface** (NSG1).
- You can reduce administrative effort by applying the same NSG to many resources



# Security Rules for Network Security Groups

Property	Meaning
Name	A unique name within the network security group.
Priority	A number between 100 and 4096. <b>Lower numbers have a higher priority and are processed first.</b>
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.

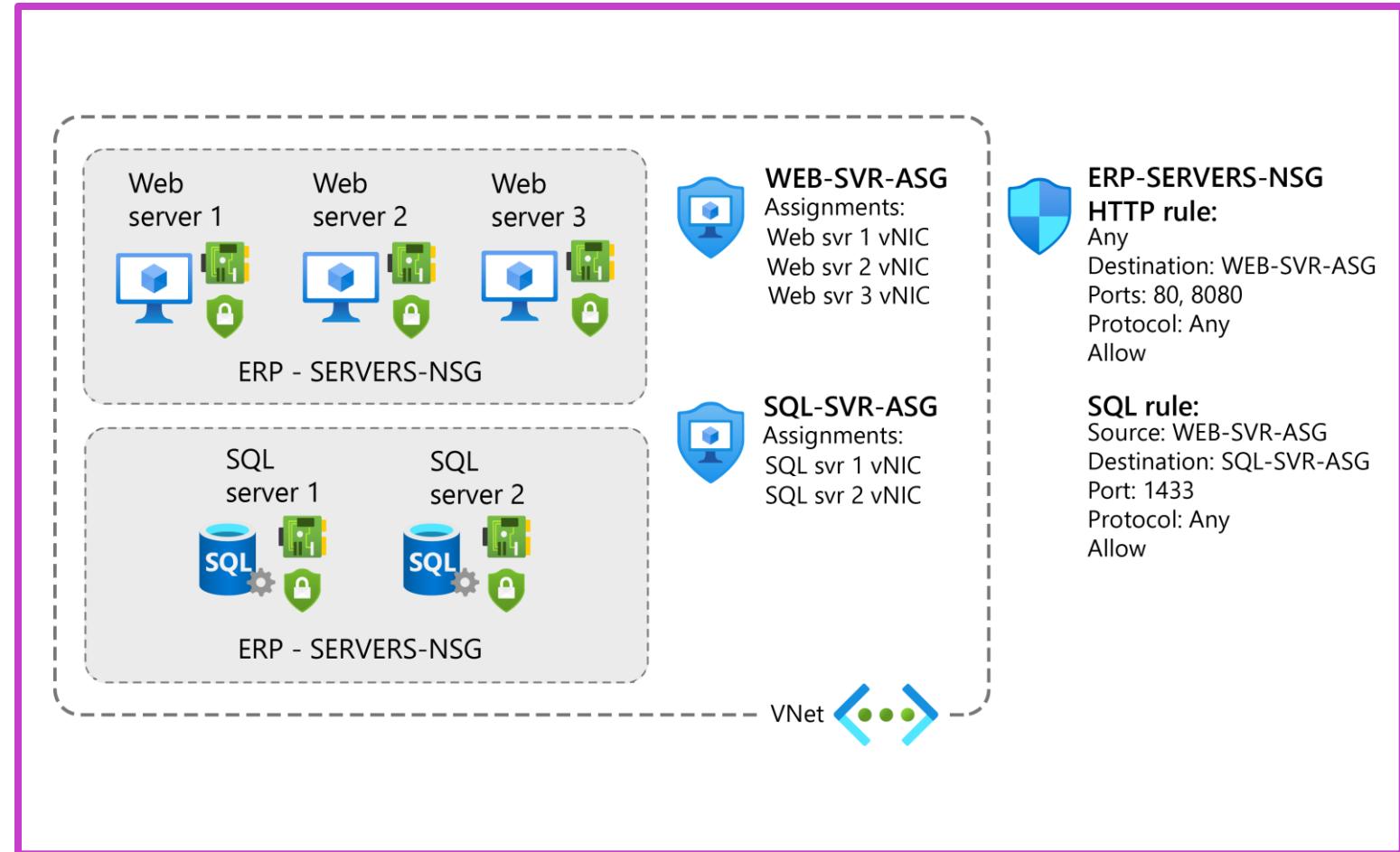
# Application Security Groups

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

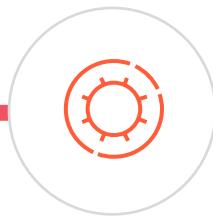
**ASG enables you to group network interfaces together. You can then use that ASG as a source or destination rule within an NSG.**

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

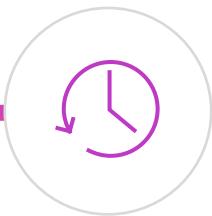
For example, Contoso has a number of front-end servers in a VNet. IT staff decide to implement NSGs and ASGs to secure the network resources.



# Implement Adaptive Network Hardening



How it works



Reviewing Adaptive  
Network Hardening  
alerts and rules

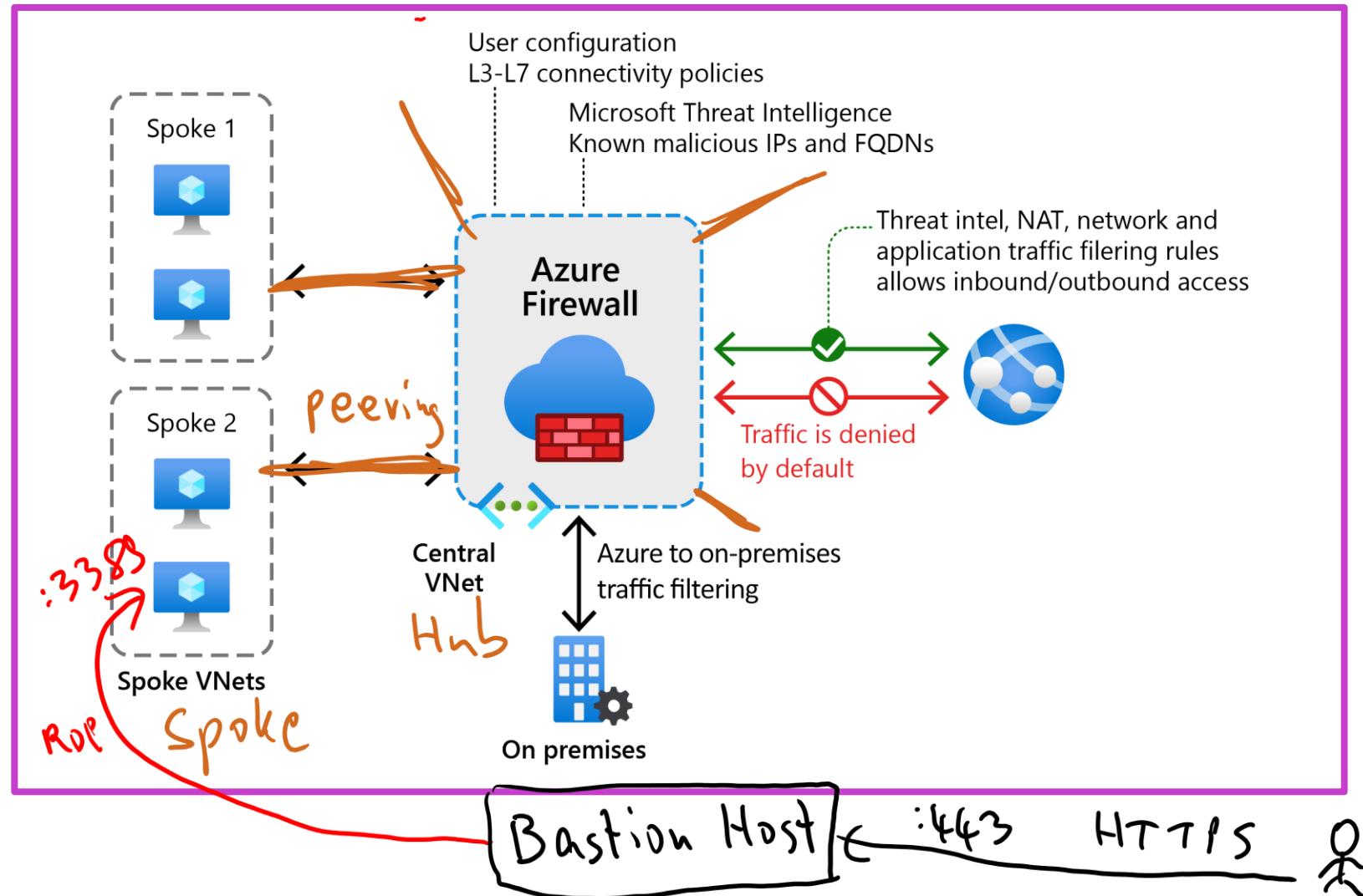


Applying Adaptive  
Network Hardening  
recommendations

SKU

# 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?

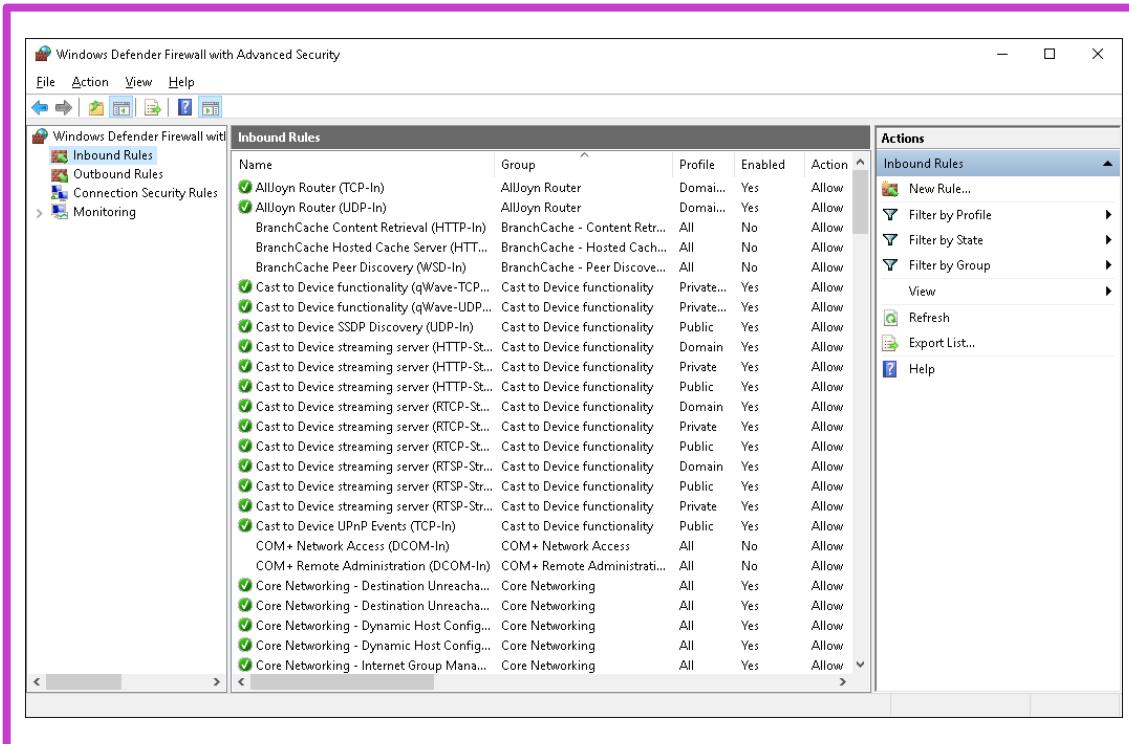
- **Windows Defender Firewall** with Advanced Security is a host-based firewall for enhancing the security of Windows Server.
- **Windows Defender Firewall** with Advanced Security is more than just a simple firewall, because it includes features such as firewall profiles and connection security rules.

## Configuring Windows Defender Firewall rules

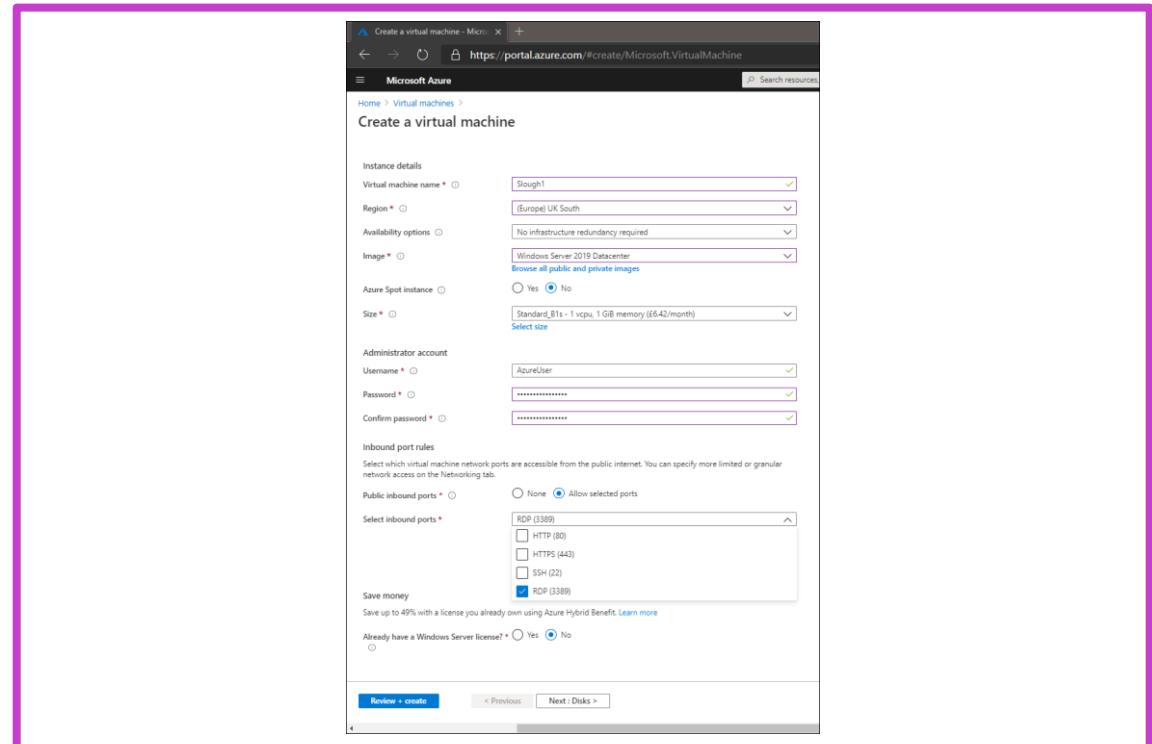
- Rules comprise a collection of criteria that define which traffic you will allow, block, or secure with the firewall.
- Inbound, Outbound, Connection security
- Inbound and outbound rule types
- Program rules, Port rules, Predefined rules, Custom rules

# Implement Windows firewall with Windows Server IaaS VMs

## Administering Windows Defender Firewall



## Creating firewall rules when creating a VM in Azure



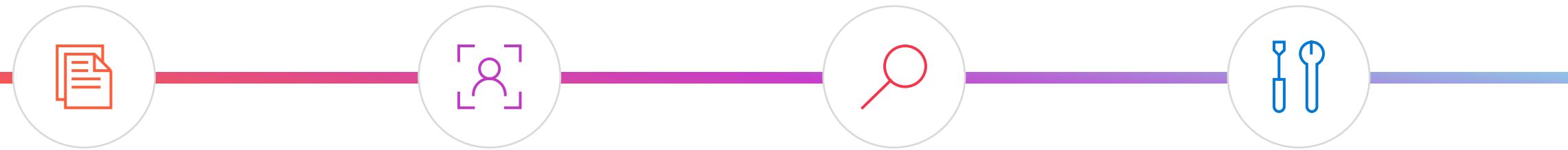
# Choose the Appropriate Filtering Solution

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:

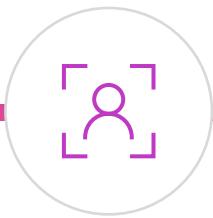
- Regional service that lets you monitor and diagnose network scenario level conditions in, to, and from Azure

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 NSG 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.

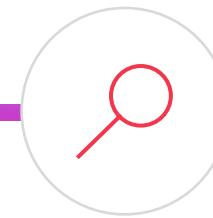
# Demonstration – Log Network Traffic to and from a VM



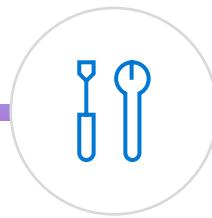
Enable Network  
Watcher



Register Insights  
provider



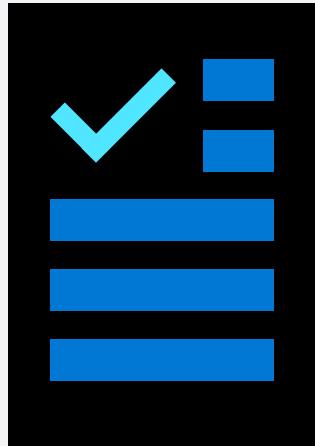
Enable NSG  
flow log



Download and  
view flow log

# Learning recap – Implement Windows Server IaaS VM network security

## Knowledge Check



**Microsoft Learn Modules ([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))**

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  
*Azure AWS | GCP | ...*
- What is Microsoft Sentinel?
- Implement SIEM and SOAR solutions in Microsoft Sentinel
- Learning recap

Defender Cloud  
12 Plans

Defender M365

- Defender EP
- Def. App
- Def. Identity
- Def. O365

ARC

# What is Microsoft Defender for Cloud?

With Microsoft Defender for Cloud capabilities, you can:

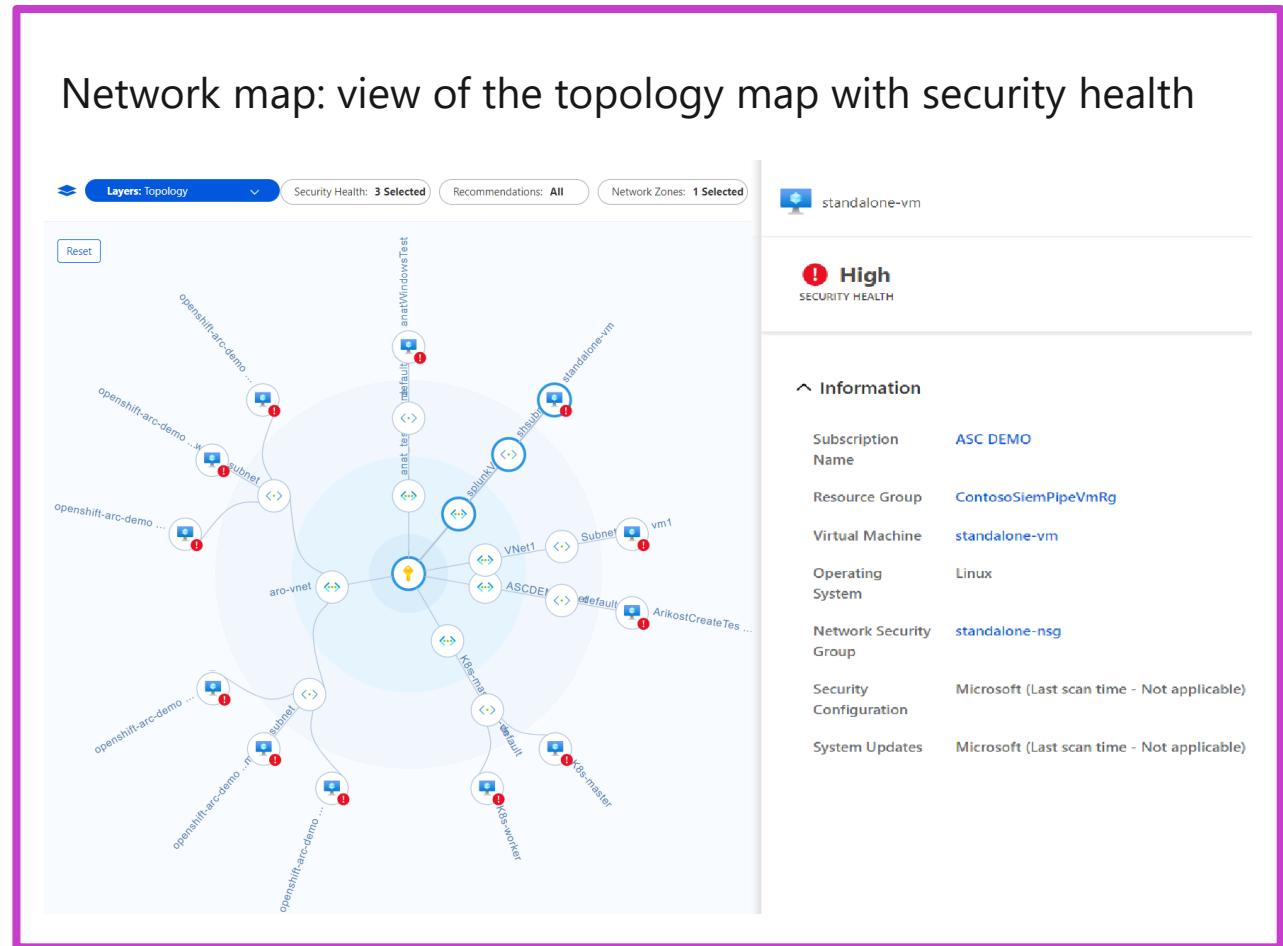
- Improve your security position. In addition to security best practices, you can also track compliance against regulatory standards.
- Protect your environment.
- Protect your data. Defender for Cloud can also perform automatic data classification in your Azure SQL databases.

The screenshot shows the Microsoft Defender for Cloud Overview page. At the top, there are three main metrics highlighted with red circles: 1 Azure subscriptions, 6 Assessed resources, and 2 Active recommendations. The left sidebar includes links for Overview, Getting started, Recommendations, Attack Path Analysis, Security alerts, Inventory, Cloud Security Explorer, Workbooks, Community, and Diagnose and solve problems. Under Cloud Security, there are links for Security posture, Regulatory compliance, Workload protections, and Firewall Manager. The main content area displays the Security posture section with 2/2 Unassigned recommendation and 0/0 Overdue recommendations. It also shows a Secure score of 0% for Azure, AWS, and GCP. The URL in the browser bar is [Microsoft Defender for Cloud | Overview](#).

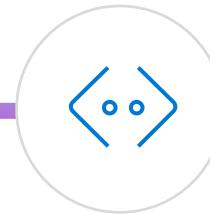
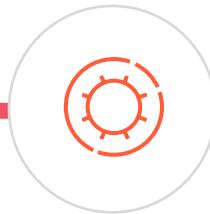
# Defender for Cloud feature coverage for VMs

- 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
- Adaptive application controls
- Regulatory compliance dashboard and reports
- Adaptive network controls, Adaptive network hardening
- Just-in-time (JIT) VM access

3389  
22



# Enable Microsoft Defender for Cloud in Hybrid Environments



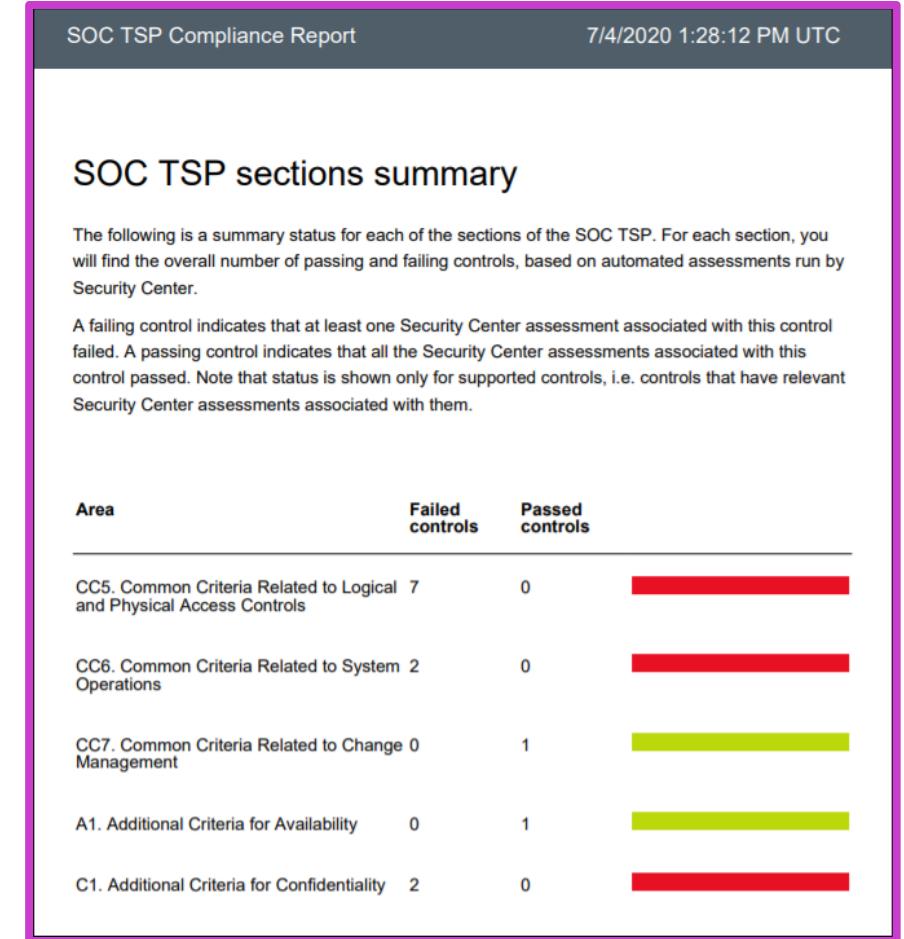
Enable the Defender for  
Cloud Standard pricing tier

Enable automatic  
provisioning

Onboard your on-premises  
servers and computers

# Audit your VM's Regulatory Compliance

Compliance standard	Description
PCI DSS 3.2.1	The <b>Payment Card Industry</b> Data Security Standard (PCI DSS) addresses security issues for organizations that manage credit card payments and is intended to reduce card fraud.
ISO 27001	Part of the <b>International Standards Organization</b> (ISO) 27000 family of standards, 27001 defines a system that can bring management to IT systems.
Azure CIS 1.1.0	The <b>Center for Internet Security</b> (CIS) is an organization involved in developing best practice for securing It system.
SOC TSP	The <b>Service Organization Controls</b> (SOC) framework is a standard for controls that focuses on safeguarding the confidentiality and privacy of information stored and processed in the cloud.



# Implement and Assess Security Policies

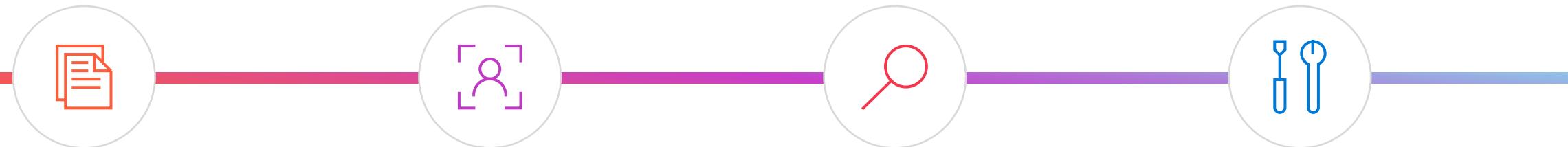
## Remediate security recommendations

- 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

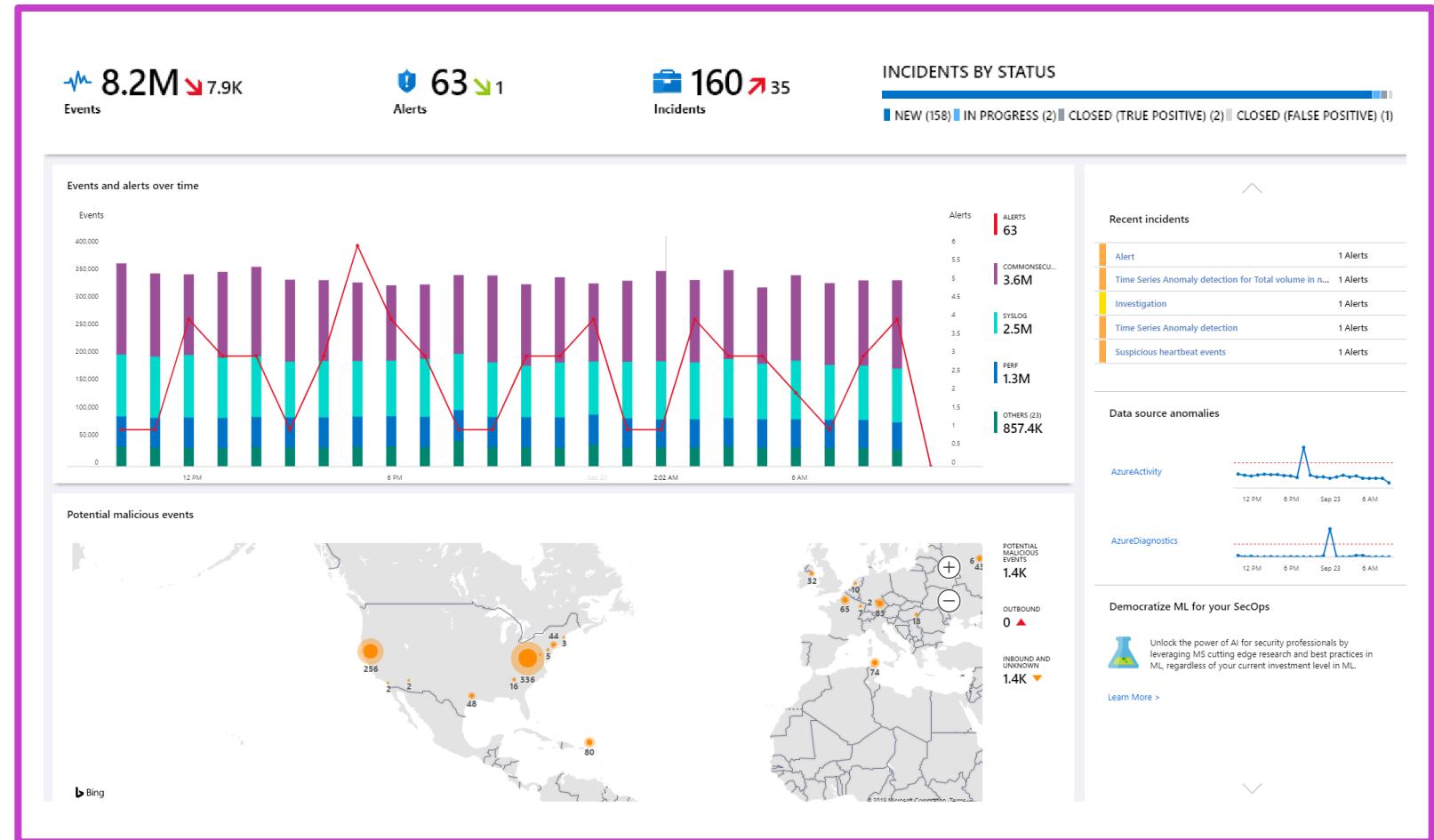
Install Endpoint  
protection and  
enable JIT

# Splunk

# 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.



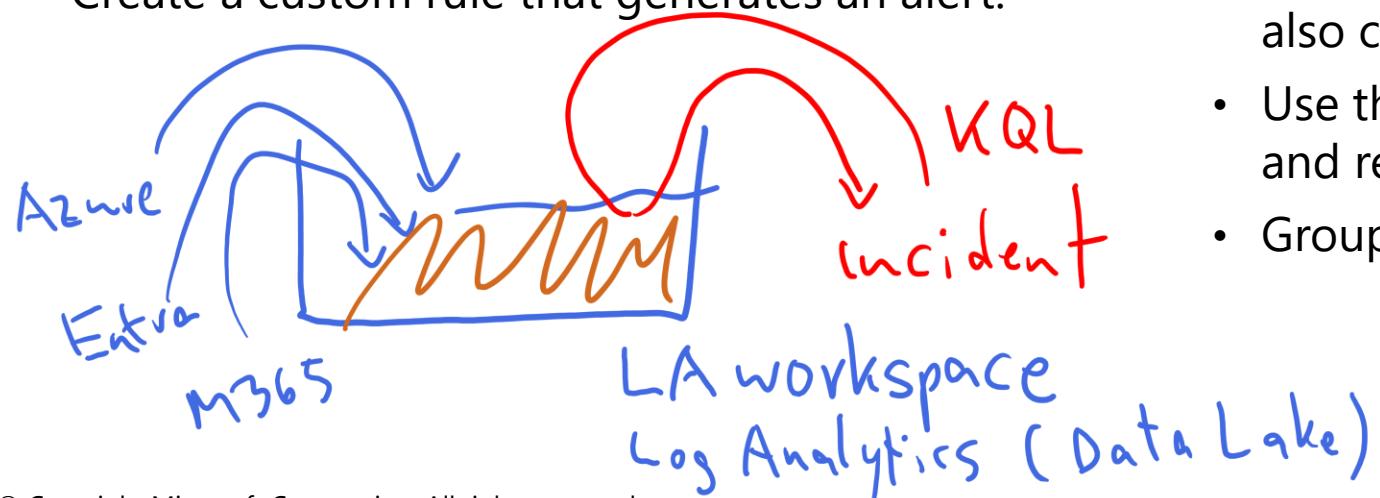
# Implement SIEM and SOAR solutions in Microsoft Sentinel

## 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.

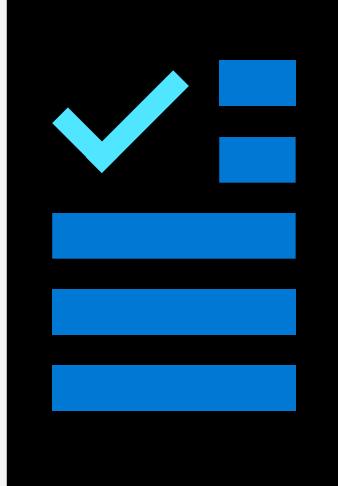
Use the following best practices to implement SOAR in Sentinel:

- 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.

KQL   Knob Query Lang

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

## Knowledge Check



**Microsoft Learn Modules ([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))**

Audit the security of Windows Server IaaS Virtual Machines

# Manage Azure VM updates

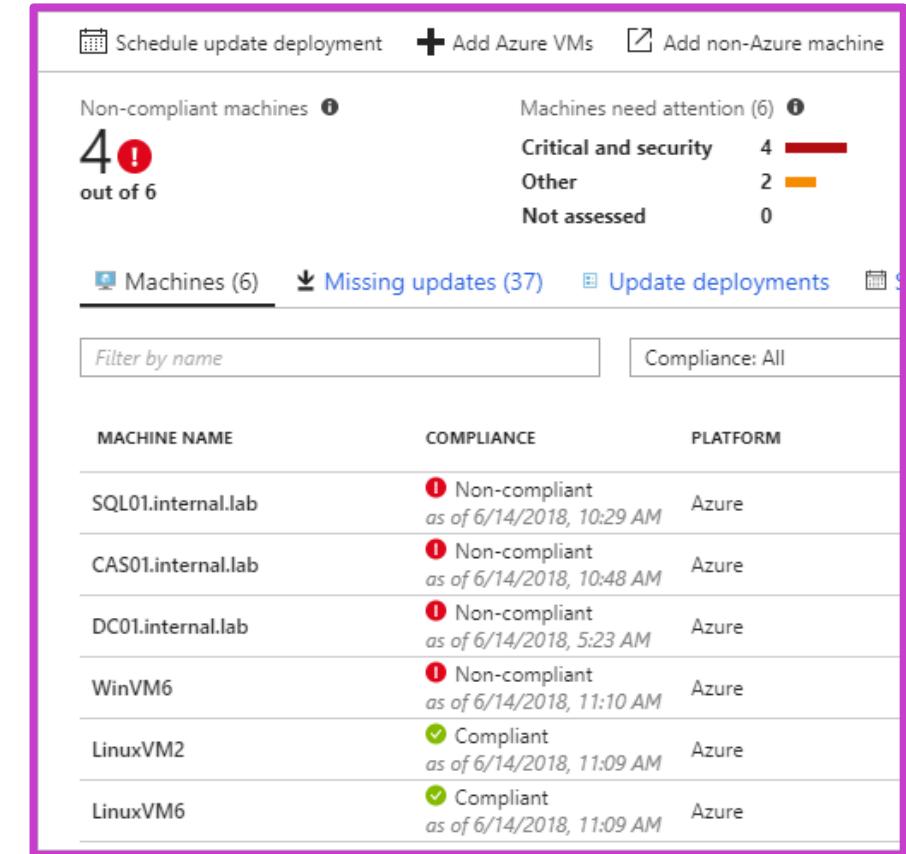
# Learning Objectives – Manage Azure updates

- Describe Azure updates
- Enable Update Management
- Deploy updates
- Review an update assessment
- Manage updates for your Azure VMs
- Learning recap

# Azure Automation and Update Management

Update Management features helps to update Azure VMs:

Feature	How it can help
Review the status of updates on your VMs	The service includes a cloud-based console where you can review the status of updates across your Azure organization and for a specific VM.
Configure dynamic groups of VMs to target	It also allows you to define a query based on a computer group. A computer group is a group of computers that are defined based on another query or imported from another source such as WSUS or Microsoft Endpoint Configuration Manager.
Search the Azure Monitor logs	Update Management collects records from the Azure Monitor Logs.

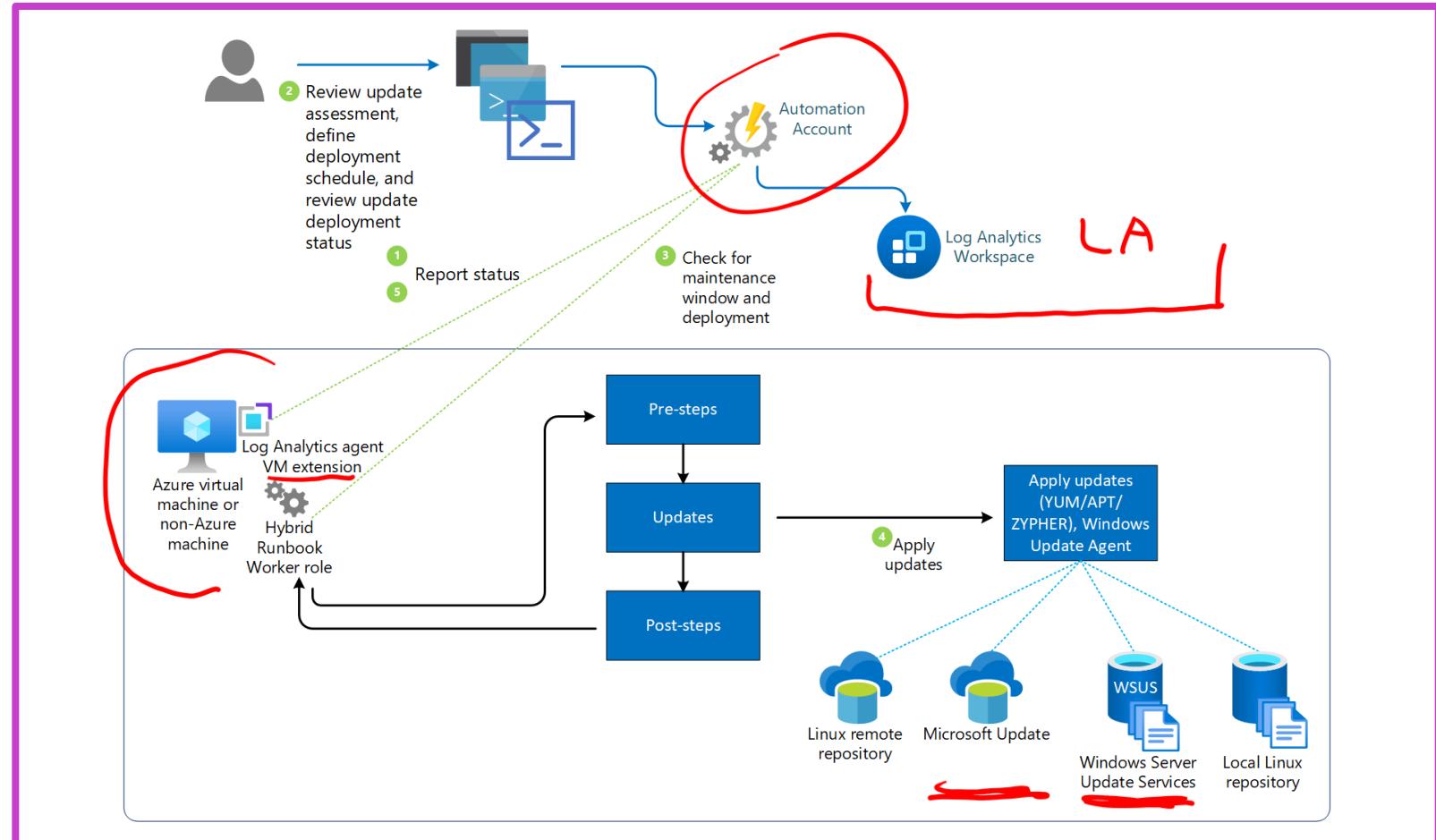


# Azure Update Management

bisher

## Steps for implementing Azure Update Management:

- Create an Azure Automation account
- Enable Update Management
- Onboard your azure/on-premises servers
- Select the machines to manage
- Schedule updates



# Interaction with Windows Update

Azure Automation Update Management relies on the Windows Update client to download and install Windows updates.

You can manage many of these settings by:

- Using Local Group Policy Editor
- Using Group Policy
- Using Windows PowerShell
- Editing the Registry directly

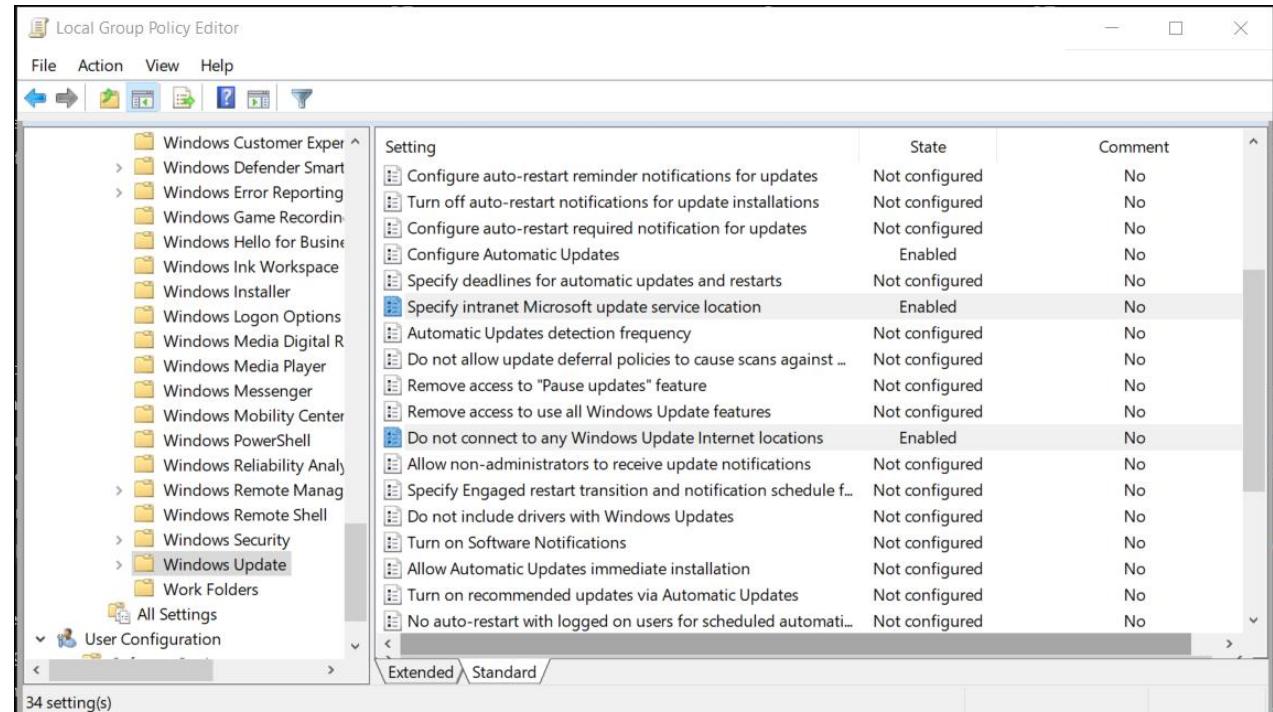
Update Management respects many of the settings specified to control the Windows Update client.

# Configure WSUS for Managing Updates

- WSUS improves the security of the by applying security updates to Microsoft products and third-party products.
- It provides the infrastructure to download, test, and approve security updates. Applying security updates quickly helps prevent security incidents.
- Update Management in Azure supports WSUS settings.

\* To restrict machines to the internal update service, set *Do not connect to any Windows Update Internet locations*.

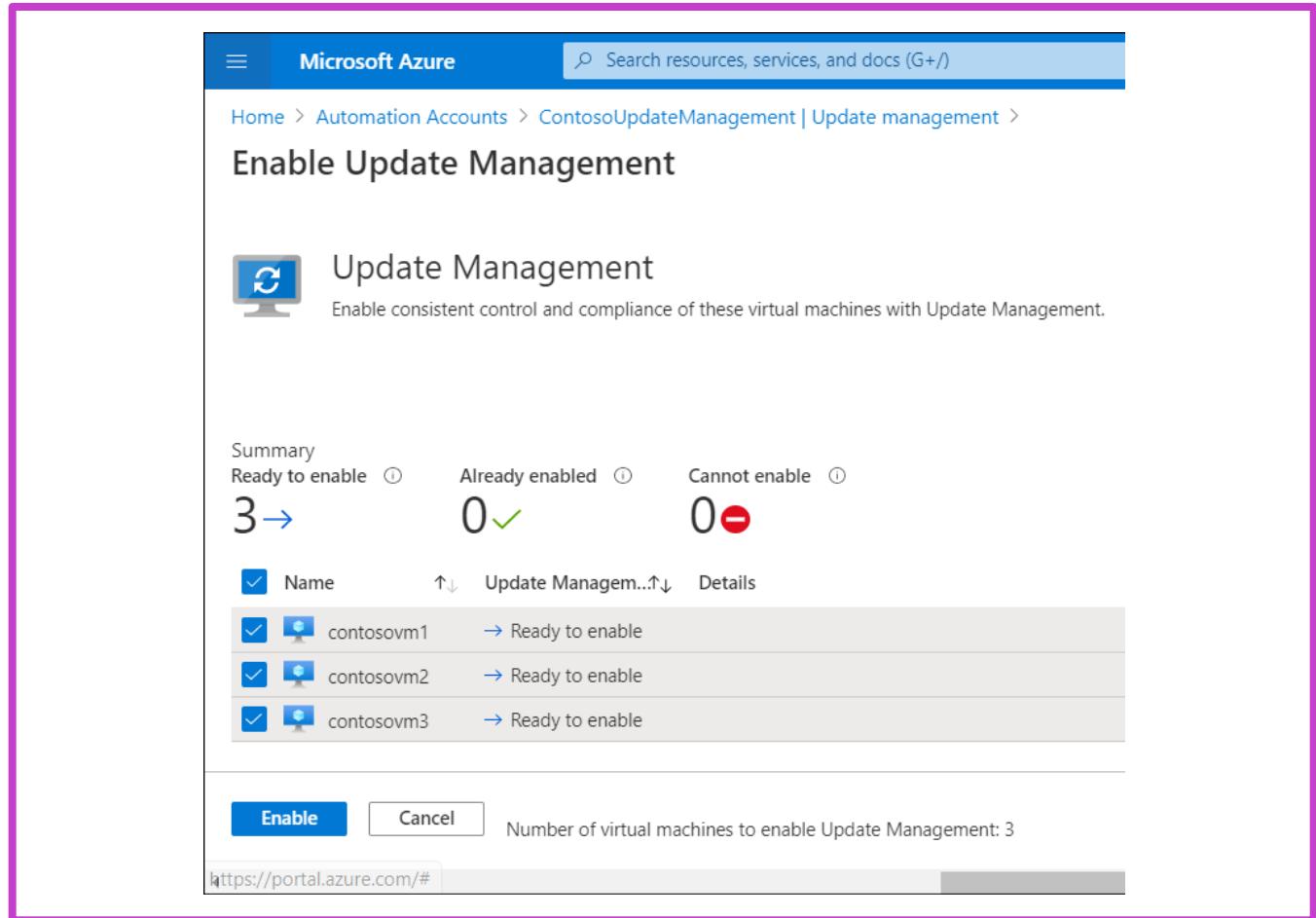
Specify intranet Microsoft Update service location in Group Policy\*



# Enable Update Management

- Create an Automation account
- Enable Update Management
- Onboard Azure VMs
- Onboard your servers
- Onboard on-premises servers
- Schedule updates

You can manually add your on-premises servers to Update Management in Automation by install the Log Analytics.



# Deploy Updates

Setting	Your action
Name	Enter the name of the update deployment.
Operating system	Choose either Windows or Linux.
Groups to update	Select the groups to update.
Machines to update	Select from a list of available machines.
Update classifications	Select from the following list: Critical updates, Security updates, Update rollups, Feature packs, Service packs, Definition updates, Tools, and Updates.
Include/exclude updates	Enter the knowledge base (KB) ID of any updates you want to exclude, or specifically include.
Schedule settings	Specify the start date and time, the time zone, and the recurrence values.
Pre-scripts + Post-scripts	Pre-scripts and Post-scripts are tasks that can be automatically executed before or after an update deployment runs.
Maintenance window (minutes)	Set the maintenance window in minutes.
Reboot options	Choose one from the following list: Reboot if required, Never reboot, Always reboot, and Only reboot – will not install updates.

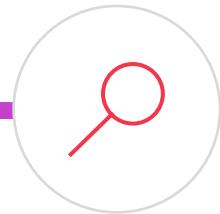
# Demonstration – View Update Assessments



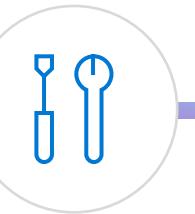
Create an  
automation  
account



Enable Update  
Management on VMs



Create Custom  
Configuration



Enable auto-update  
management

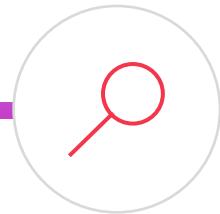
# Demonstration – Manage Updates for your Azure VMs



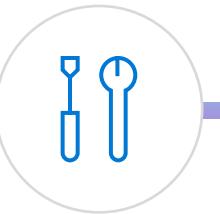
View update  
assessment



Configure action  
groups and alerts



Schedule an update  
deployment



Check deployment  
status

# Managing VM Updates

## Create an assessment for VM updates

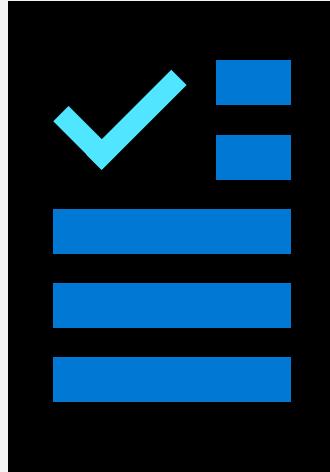
- Create an automation account
- Enable Update Management on VMs
- Create custom configuration
- Enable auto-update management

## Configure alerts and update deployment options

- View update assessment
- Configure action groups and alerts
- Schedule an update deployment
- Check deployment status

# Learning recap – Manage Azure VM updates

## Knowledge Check



**Microsoft Learn Modules ([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))**

Manage Azure VM updates

# Create and implement application allowlists with adaptive application control

# Learning Objectives – Adaptive application control

- Describe adaptive application control
- Enable Update Management
- Configure a new application control policy
- Move a VM from one group to another
- Learning recap

# Describe Adaptive Application Control

Adaptive application control uses machine learning to analyze the applications running on your VMs.

By using Adaptive application controls, you can:

- Block attempts to run potentially malicious applications.
- Receive alerts when adaptive application control blocks an application.
- Comply with your organization's requirements that you use only licensed software.
- Avoid using unwanted software, including old or unsupported apps.
- Prevent specific software tools from running.
- Enable IT to control access to sensitive data.

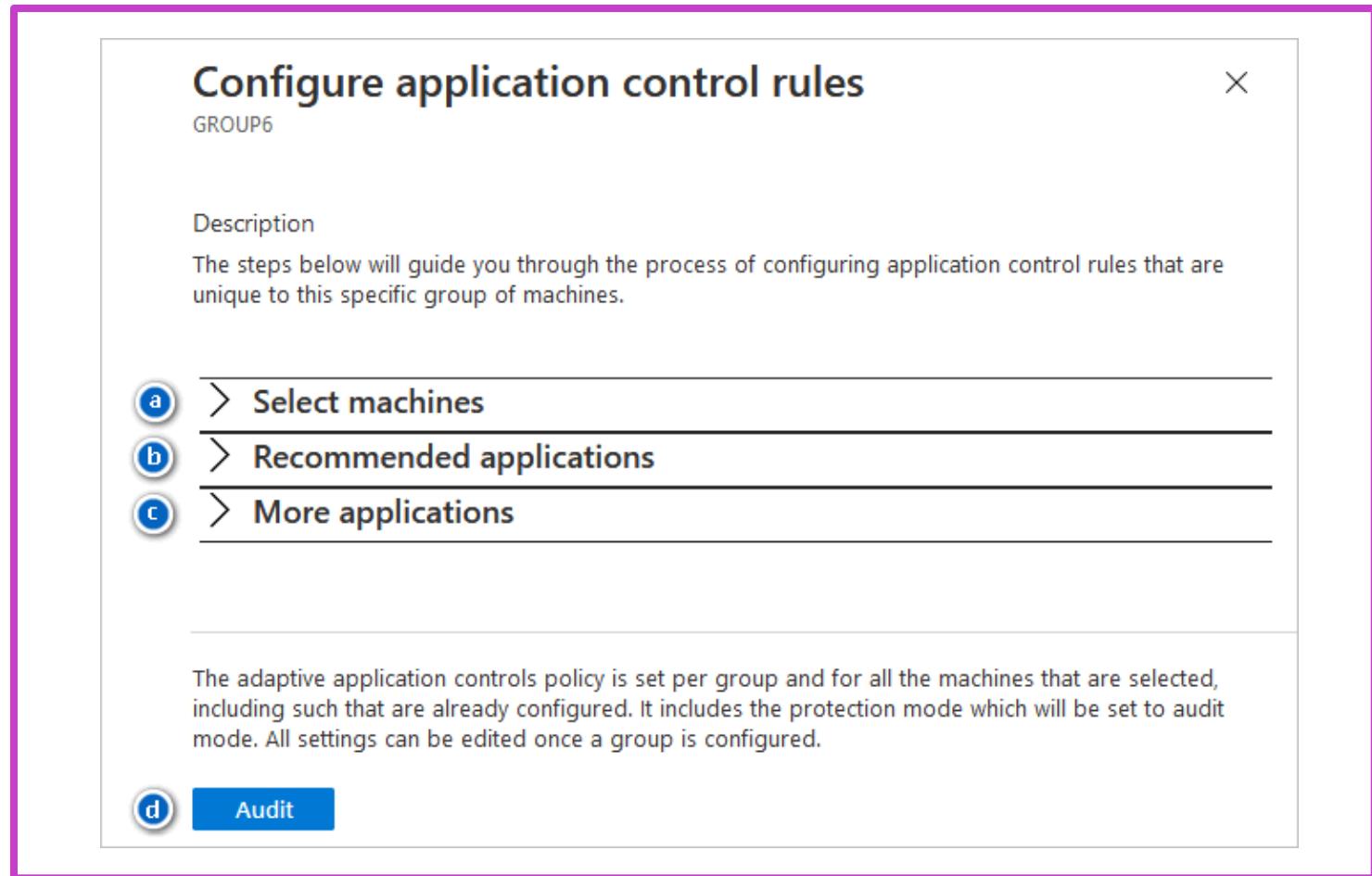
The screenshot shows the 'Adaptive application controls' dashboard with a red box highlighting the 'Recommended' tab. The interface includes a sidebar with a 'Dashboard >' link and a 'Add custom group' button. Below the tabs, there is a message: 'Groups of machines for which we recommend applying application controls to define a list of known-safe applications'. A table lists five groups: 'Contoso Hotels' (19 machines, state: Open - New, severity: High), 'GROUP1' (1 machine, state: Open - New, severity: High), 'GROUP4' (5 machines, state: Open - New, severity: High), 'GROUP6' (11 machines, state: Open - New, severity: High, with a cursor icon over it), 'REVIEWGROUP1' (1 machine, state: Open - New, severity: High), and 'REVIEWGROUP2' (1 machine, state: Open - New, severity: High). The table has columns for Group Name, Machines, State, and Severity.

Group Name	Machines	State	Severity
Contoso Hotels	19	Open - New	High
GROUP1	1	Open - New	High
GROUP4	5	Open - New	High
GROUP6	11	Open - New	High
REVIEWGROUP1	1	Open - New	High
REVIEWGROUP2	1	Open - New	High

# Enable Adaptive Application Control (1 Of 2)

Use the following procedure to begin the process of implementing adaptive application control:

- In the Azure portal, open Defender for Cloud.
- In the navigation pane, in the ADVANCED CLOUD DEFENSE section, select Adaptive application controls.
- In the Adaptive application controls blade, expand How does it work?



# Enable Adaptive Application Control (2 Of 2)

Tab	Description
Configured	This is a list of groups containing the VMs that are already configured with application control.
Recommended	This tab offers a list of groups for which application control is recommended. Defender for Cloud uses machine learning to identify VMs that are good candidates for application control based on whether the VMs consistently run the same applications.
No recommendation	This is a list of groups containing VMs without any application control recommendations—for example, VMs on which applications are always changing and haven't reached a steady state.

Configured   Recommended   No recommendation

Groups of machines for which we recommend applying application controls to define a list of known-safe applications

Group Name	↑↓	Machines	↑↓	State	↑↓	Severity
Contoso Demo	3					
REVIEWGROUP4	1		Open - New	High		
REVIEWGROUP5	2		Open - New	High		

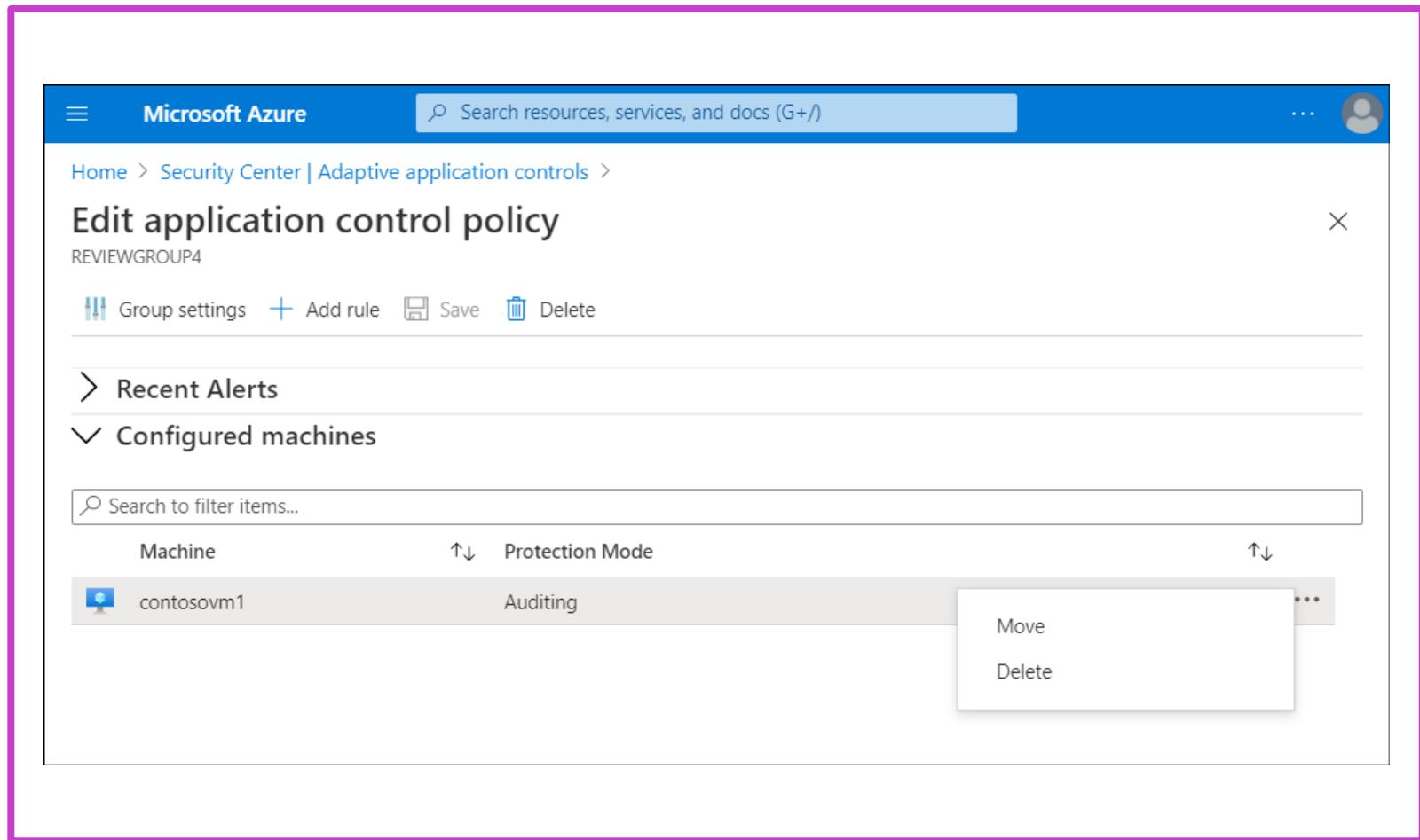
# Configure a New Application Control Policy

- 1 Select the **Recommended** tab for a list of groups with application control recommendations
- 2 After selecting a group, review the **Configure application control rules** blade.
- 3 In the **Select Machines** section, review the list of recommended VMs, and deselect those to which you don't want to apply an application allow policy.
- 4 Within the Recommended applications section are two sections as described in the following table.
- 5 Review the applications in each list and clear the check boxes of those that you don't want to apply. The following table describes the information that the lists contain.
- 6 After you complete your selections, select **Audit**.

# Move a VM from one Group to Another

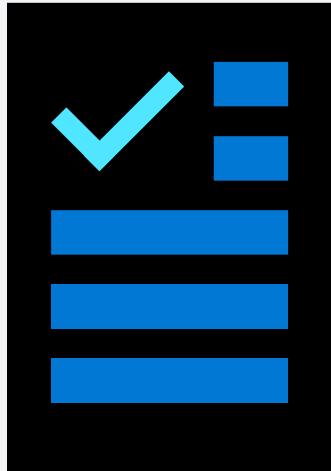
To move a VM from one group to another, perform the following procedure:

- From Adaptive application controls blade, on the Configured tab, select the group which the VM currently belongs to.
- Select Configured machines.
- Select the ellipsis, and then select Move.
- In the Move computer to different group window, select the group to move the VM to, select Move Computer, and then select Save.



# Learning recap – Adaptive application control

## Knowledge Check



### Microsoft Learn Modules ([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))

Create and implement application allowlists with adaptive application control

# 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

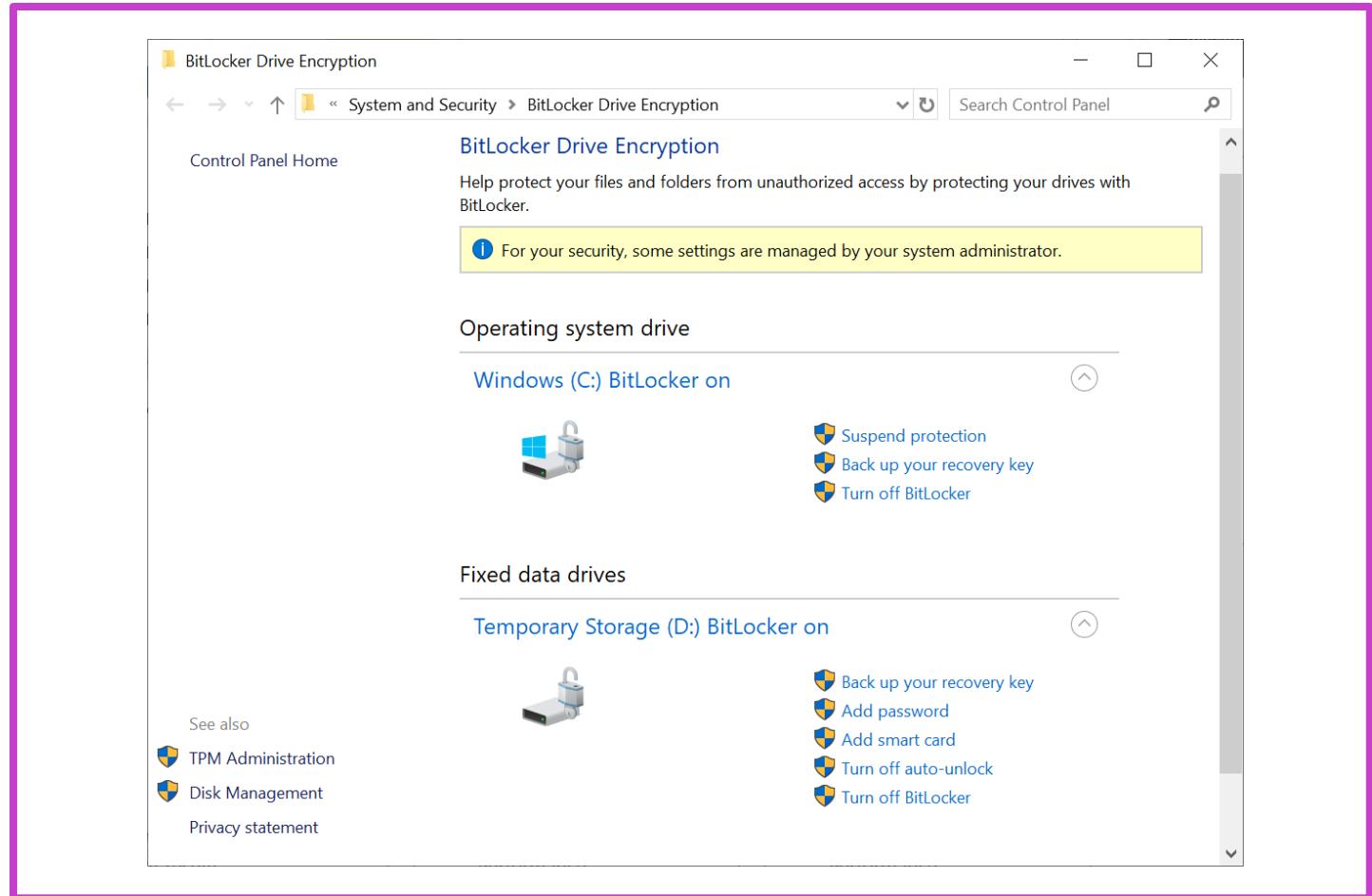
# Describe Azure Disk Encryption and server-side encryption

## 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:

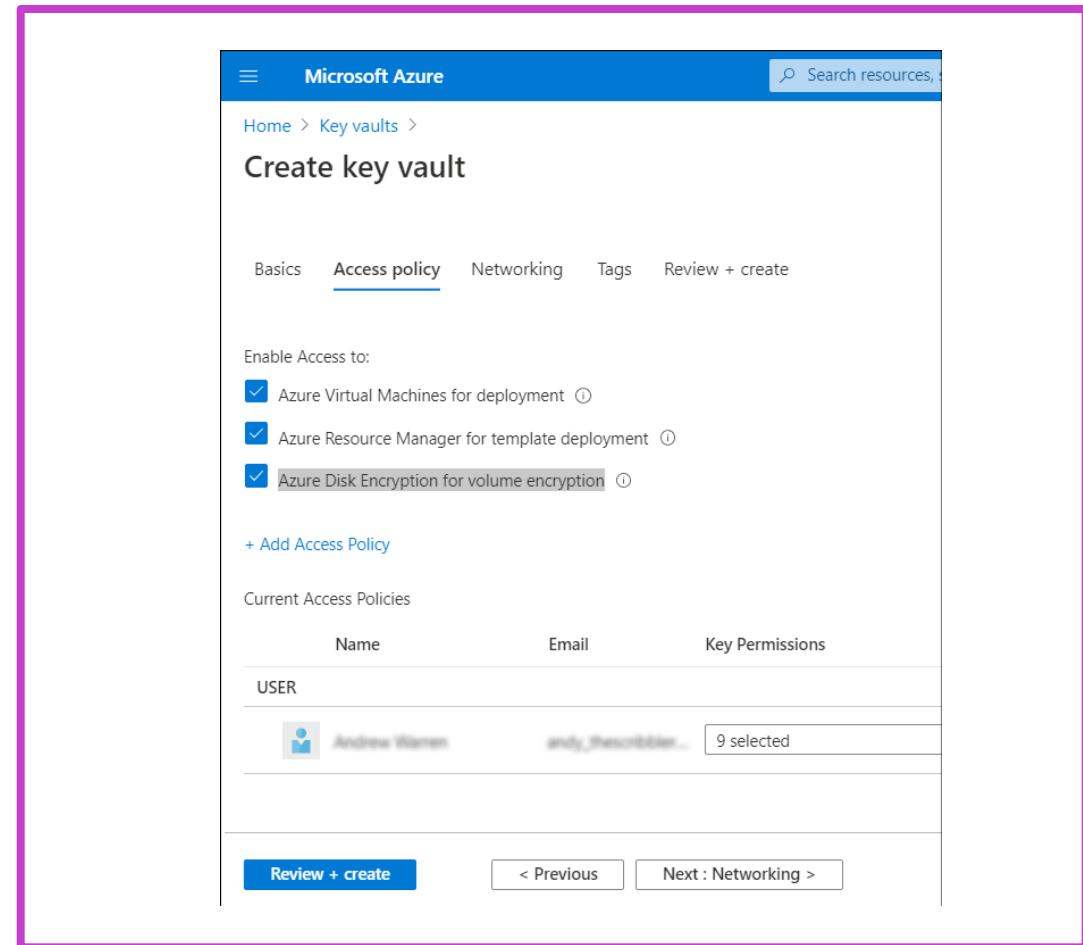
- Supports Generation 2 Azure VMs and all existing Azure VM sizes
- It is automatic



# 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**'.

## Use Azure CLI to encrypt a VM

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

## Use PowerShell to encrypt a VM

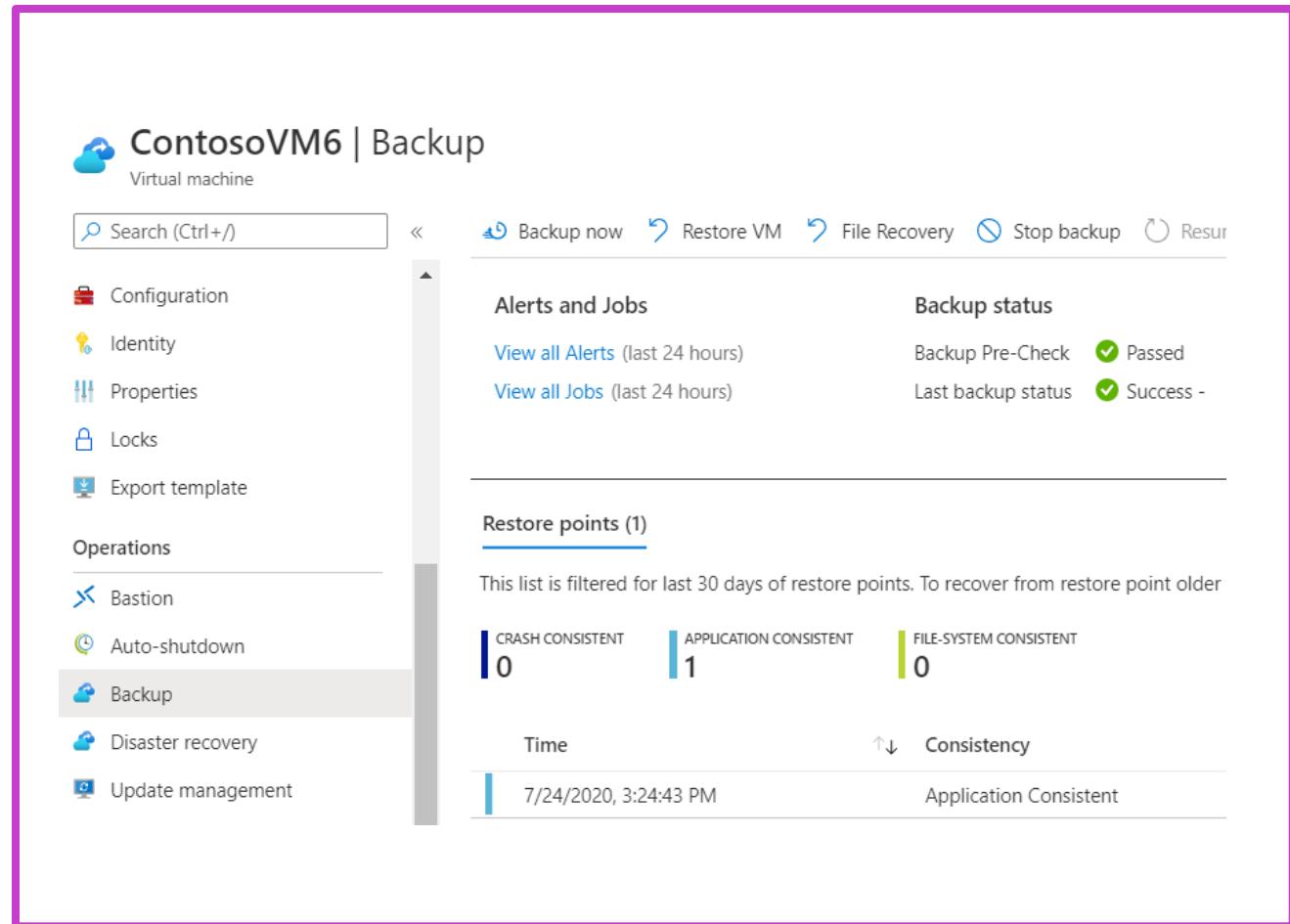
```
$KeyVault = Get-AzKeyVault
  -VaultName ContosoADEKeyVault
  -ResourceGroupName ContosoResourceGroup
```

## Set-AzVMDiskEncryptionExtension

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

# Back up your Azure Disk Encryption-protected VMs

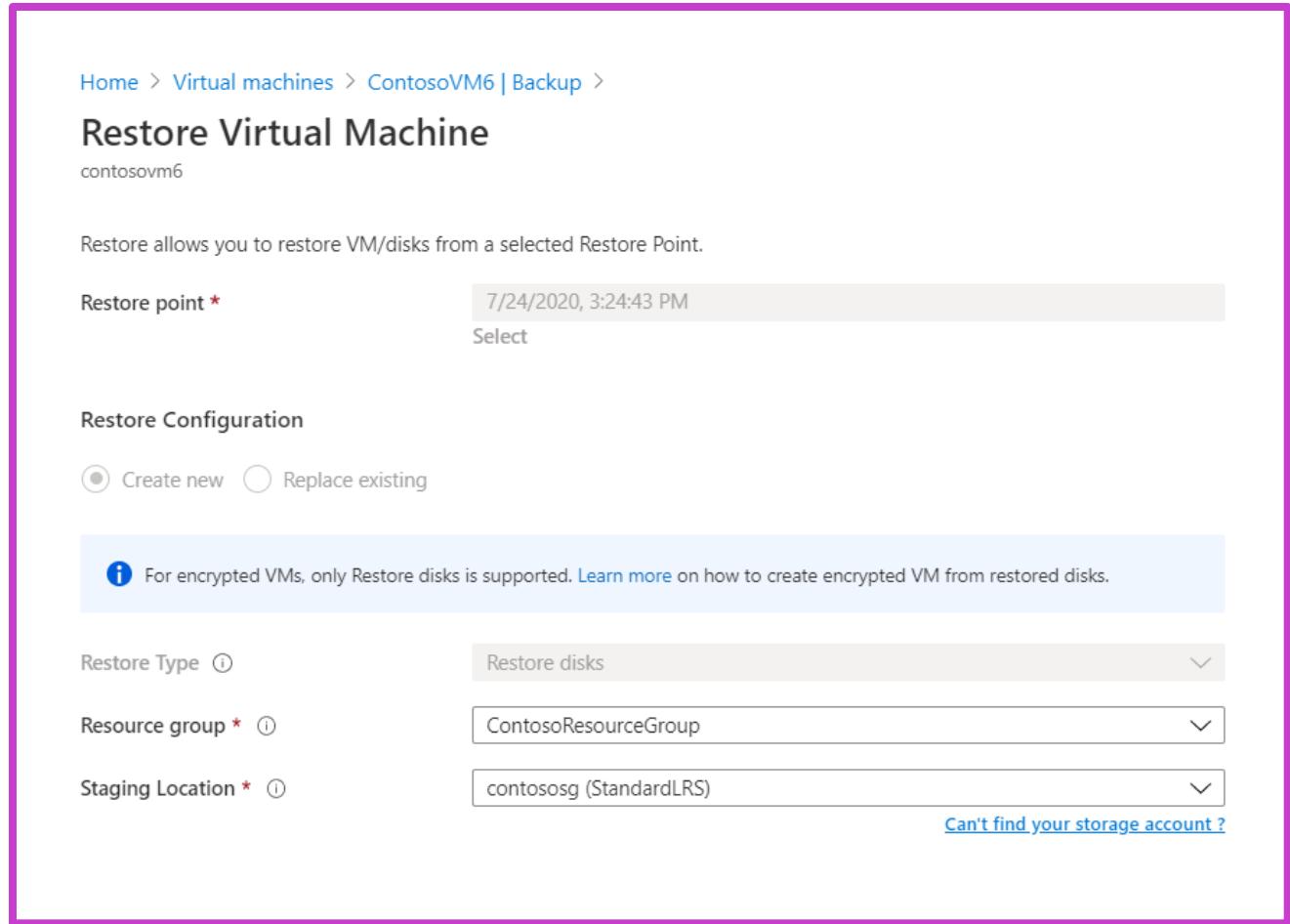
- On the **Recovery Services Vault** blade, select **Backup**.
- On the **Backup Goal** blade, specify the location of your workload.
- On the **Backup** blade, in the Policy section, select a **backup policy**
- In the **Virtual Machines** section, select **Add**.
- In the **Select virtual machine** 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**.



# 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
```

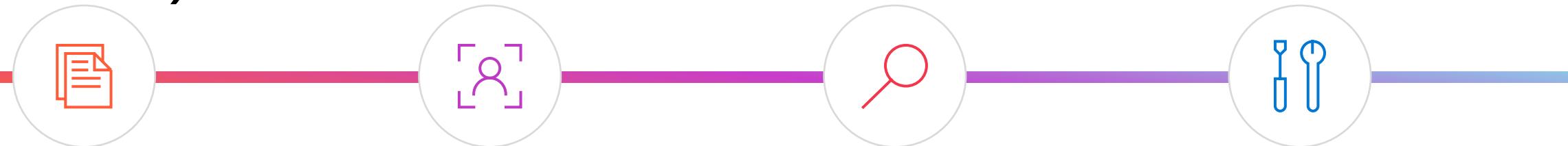
## Use PowerShell

```
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

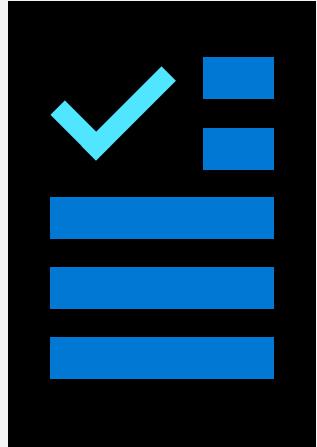
Provision KeyVault  
with enabled Disk  
Encryption

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 ([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))**

Configure BitLocker disk encryption for Windows IaaS Virtual Machines

# Implement change tracking and file integrity monitoring for Windows IaaS VMs

# Learning Objectives – Change Tracking and File Integrity Monitoring

- Implement Change Tracking and Inventory
- Requirements for Change Tracking and Inventory
- Enable Change Tracking and Inventory
- Manage Change Tracking and Inventory
- Manage tracked files
- Implement File Integrity Monitoring
- Configure File Integrity Monitoring
- Learning recap

# Implement Change Tracking and Inventory

**Change Tracking and Inventory** is a feature that allowed to track changes in both VMs and server infrastructure.

The following Linux components can be tracked:

- Linux daemons
- Linux software (packages)
- Linux files

The following Windows Server components can be tracked:

- Windows software
- Windows files
- Windows registry keys
- Microsoft services

**Change Tracking and Inventory** does not support, or has the following limitations:

- Recursion for Windows registry tracking
- Network file systems
- Different installation methods
- \*.exe files stored on Windows
- The Max File Size column and values are unused in the current implementation.
- If you are tracking file changes, it is limited to a file size of 5 MB or less.
- If you try to collect more than 2500 files in a 30-minute collection cycle, Change Tracking and Inventory performance might be degraded.

# Requirements for Change Tracking and Inventory

## 1. Automation account

## 2. Supported operating systems

- Windows Server 2012 , 2016, 2019, Win 8.1 & 10

## 3. Azure region requirements

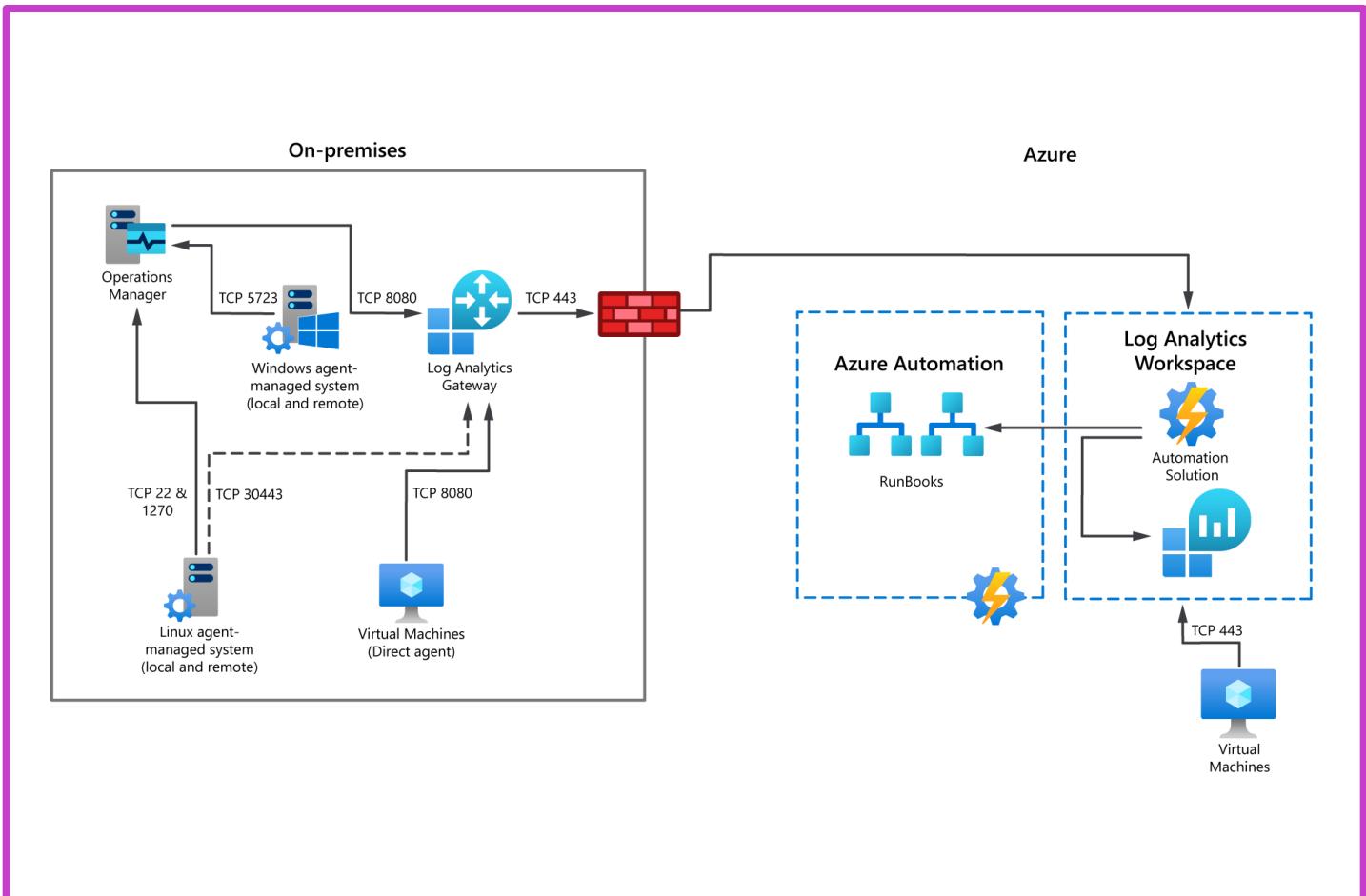
- Only certain regions are supported

## 4. Firewall requirements

- requires access through your firewall to certain resources

## 5. Network requirements

- Number of network requirements based on the requirement for Log Analytics and Windows/Linux agents



# Enable Change Tracking and Inventory

You can enable Change Tracking and Inventory in a number of ways:

- By using the Azure portal
- By using an Azure VM
- From an Automation account
- From a runbook

*The setup can take up to 15 minutes to complete.*

The screenshot shows the 'Enable Change Tracking' dialog box. At the top, there's a section titled 'Change Tracking' with the sub-section 'Subscription'. It lists 'Visual Studio Enterprise Subscription (virtual machines: 3)' under 'Subscription', 'East US (virtual machines: 3)' under 'Location', and 'contosoresourcegroup' under 'Resource groups'. Below this, there are two radio button options: 'AUTO: Auto-configure Log Analytics workspace and Automation account based on VMs subscription and location' (selected) and 'CUSTOM: Choose existing Log Analytics workspace and Automation account'. Under 'Log Analytics workspace:', it shows 'DefaultWorkspace-9b603186-feca-4a76-90a3-1472bf4fd7d3-EUS'. Under 'Automation account:', it shows 'Automate-9b603186-feca-4a76-90a3-1472bf4fd7d3-EUS'. A 'Summary' section indicates 'Ready to enable' (3), 'Already enabled' (0), and 'Cannot enable' (0). The main list shows three virtual machines: 'contosovm1', 'contosovm2', and 'contosovm3', each with a status of 'Ready to enable'. At the bottom, there are 'Enable' and 'Cancel' buttons, and a note stating 'Number of virtual machines to enable Change Tracking: 3'.

# Manage Change Tracking and Inventory



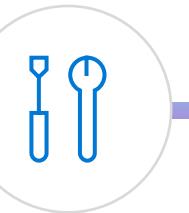
How to modify  
Change Tracking and  
Inventory settings?



How to track  
Windows files?



How to track  
Windows Registry  
changes?



How to search logs  
for change records?

# Manage Tracked Files

Enable file content tracking requires configuration of a storage account

The screenshot shows the Microsoft Azure workspace configuration for change tracking. It includes fields for Storage Account Name (cs2100300008ba01a72), Primary Write Only SAS URL (https://cs2100300008ba01a72.blob.core.windows.net/changetrackingblob?sv=2015-04), and Secondary Write Only SAS URL (https://cs2100300008ba01a72.blob.core.windows.net/changetrackingblob?sv=2015-04). Buttons for 'Unlink' and 'Regenerate' are present.

Review the contents of a tracked file in a side-by-side layout

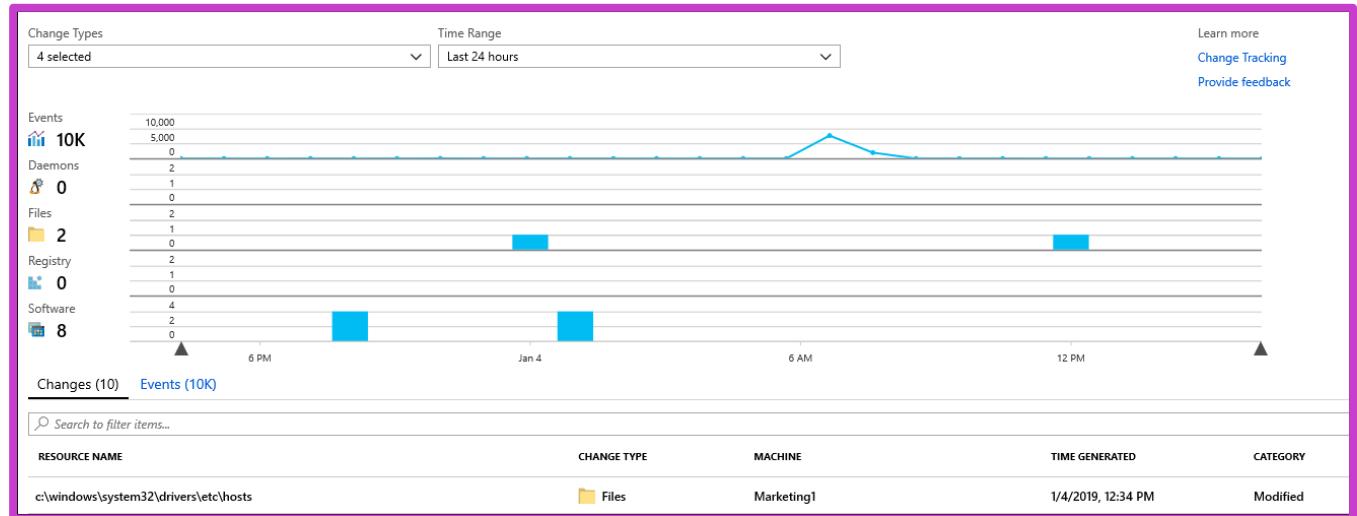
A code editor interface showing two versions of a file. The left pane shows the original file content:

```
3
4
5 # The following lines are desirable for IPv6 capable hosts
6
7 ::1 ip6-localhost ip6-loopback
8
9 fe00::0 ip6-localnet
10
11 ff00::0 ip6-mcastprefix
12
13 ff00::0 ip6-mcastprefix
```

The right pane shows the updated file content with changes highlighted in green:

```
3 + 5.6.7.8 badhost
4 +
5
6
7 # The following lines are desirable for IPv6 capable hosts
8
9 ::1 ip6-localhost ip6-loopback
10
11 fe00::0 ip6-localnet
12
13 ff00::0 ip6-mcastprefix
```

Events automatically display on the timeline



# Implement File Integrity Monitoring

## What is File Integrity Monitoring?

- Known as change monitoring, examines files and registries of operating system, application software, and others for changes that might indicate an attack.

## Enable File Integrity Monitoring

- You should upgrade the required workspace before enabling File Integrity Monitoring

## Configure File Integrity Monitoring

- To review any changes in detail, select the appropriate VM. The logs detail displays. On this page, you can review the changes. You can also modify the query used to return the list of changes to suit your requirements.

## Disable File Integrity Monitoring

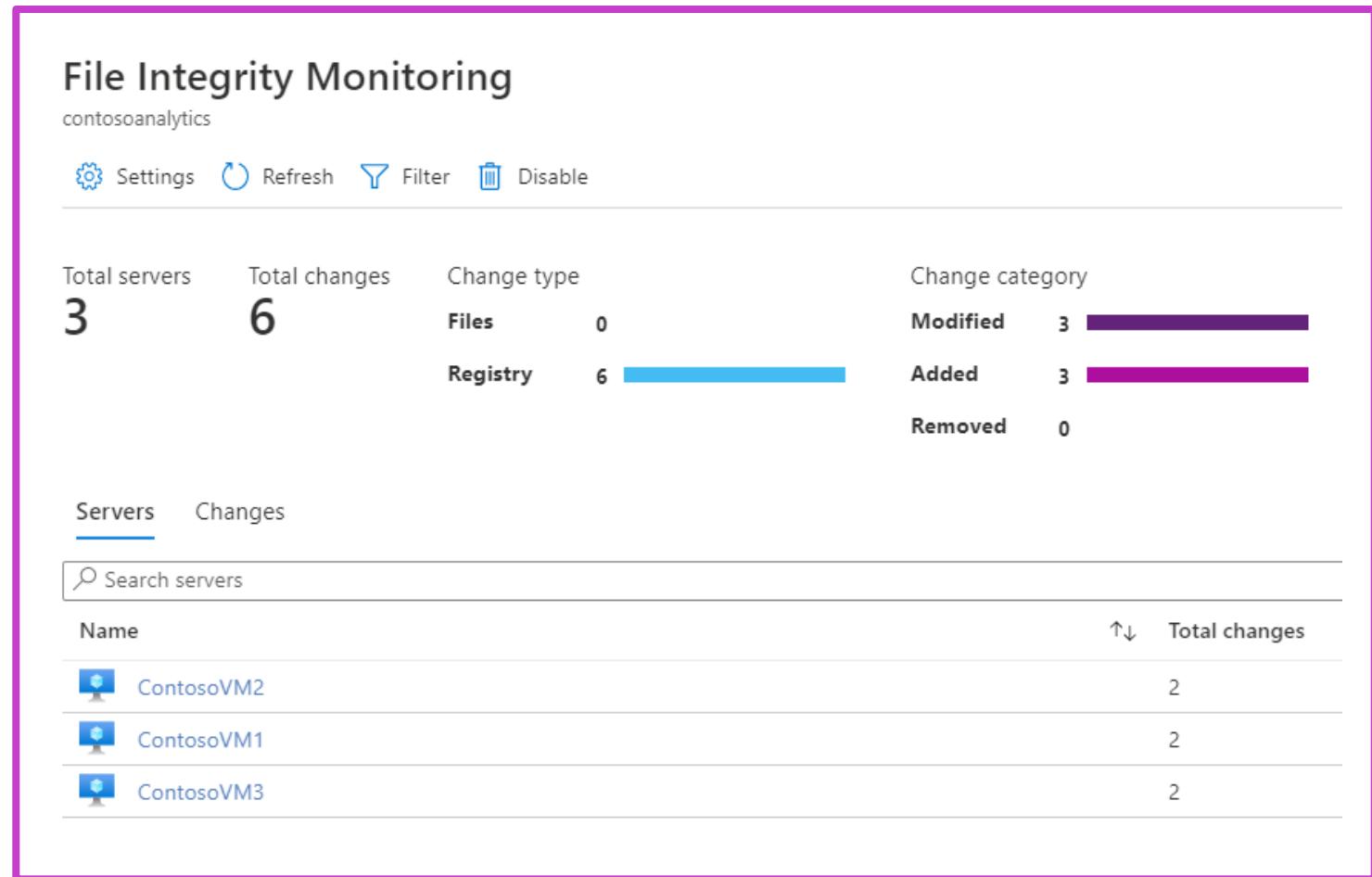
- If you no longer want to use File Integrity Monitoring, you can disable it.

# Configure File Integrity Monitoring

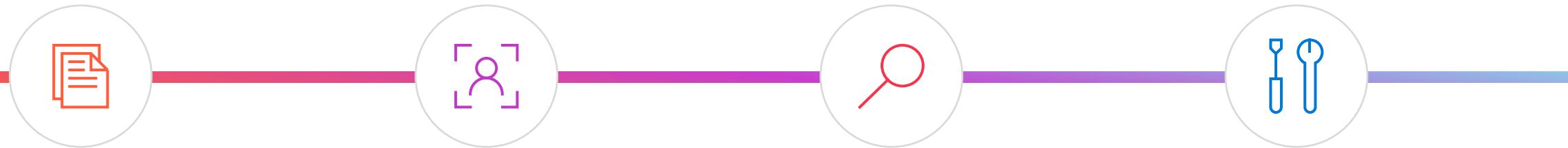
On File Integrity Monitoring dashboard, the following information is provided:

- Total number of changes that occurred in the last week
- Total number of computers and VMs reporting to the workspace
- Geographic location of the workspace
- Azure subscription that the workspace is under

You can Enable and Disable File Integrity



# Demonstration – Use File Integrity Monitoring



Explore File Integrity Monitoring dashboard

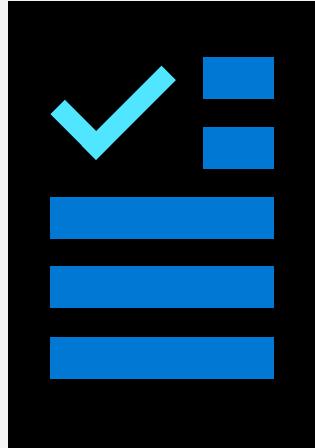
Enable File Integrity and edit monitored entities

Implement folder and path monitoring using wildcards

Disable monitored entities and File Integrity Monitoring

# Learning recap – Implement change tracking and file integrity monitoring for Windows IaaS VMs

## Knowledge Check



**Microsoft Learn Modules ([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))**

Implement change tracking and file integrity monitoring for Windows IaaS VMs

# 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 Azure Automation-based solutions, including Inventory, Change tracking, and Update management.

## Objectives

- Create an Azure Log Analytics workspace and an Azure Automation account.
- Configure Microsoft Defender for Cloud.
- Provision Azure VMs running Windows Server.
- Onboard on-premises Windows Server into Microsoft Defender for Cloud and Azure Automation.
- Verify the hybrid capabilities of Microsoft Defender for Cloud and Azure Automation solutions.

# End of presentation