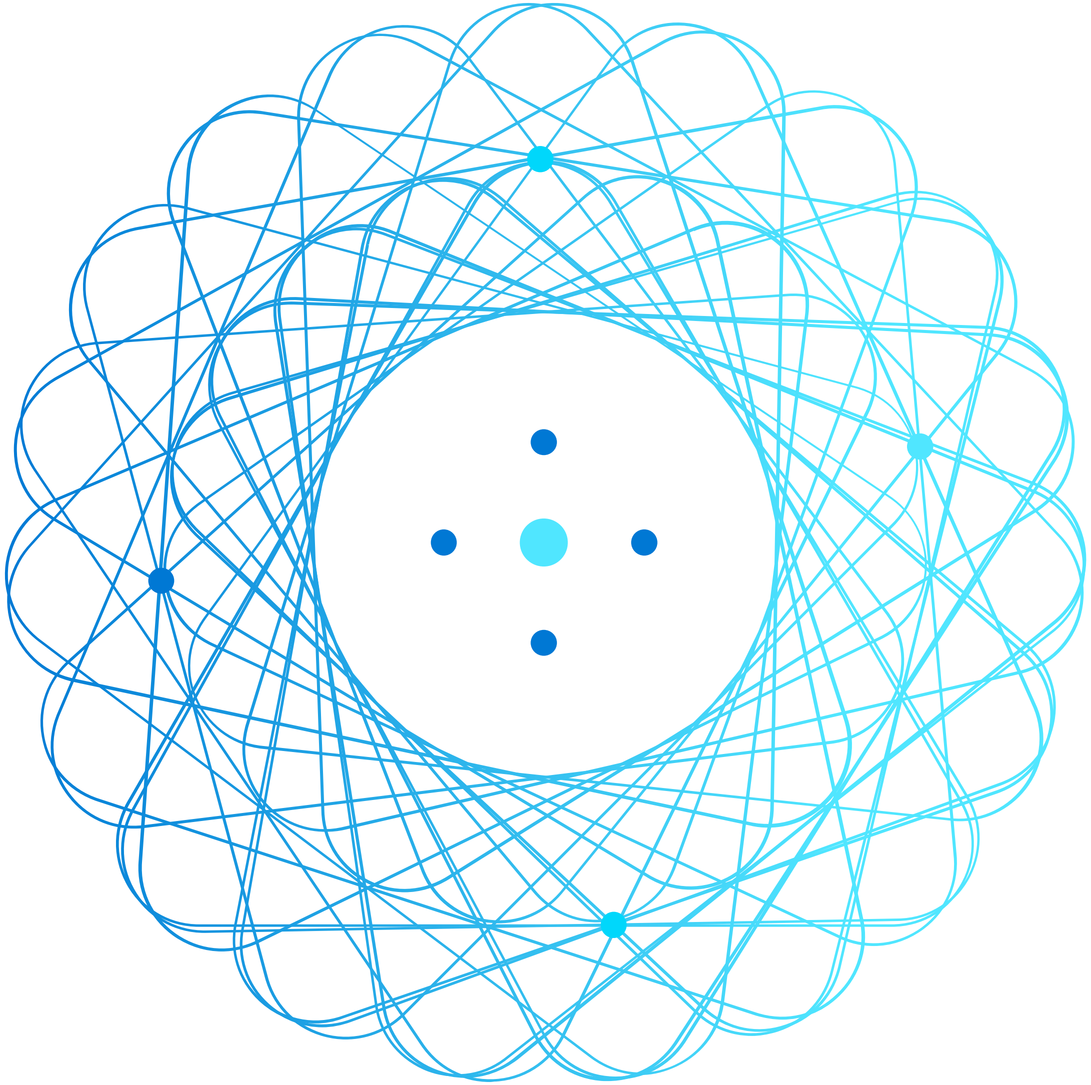
Microsoft Azure

AZ-801T00A
Configuring Windows Server Hybrid Advanced Services



AZ-801

LP 1

Module 01: Windows Server security

Module 02: Implementing security solutions in hybrid scenarios

Module 03: Implementing Windows Server high availability

Module 04: Disaster recovery in Windows Server

Module 05: Implementing recovery services in hybrid scenarios

Module 06: Upgrade and migrate in Windows Server

Module 07: Implementing migration in hybrid scenarios

Module 08: Server and performance monitoring in Windows Server

Module 09: Implementing operational monitoring in hybrid scenarios

Learning Path 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

NSG = Packet Filter

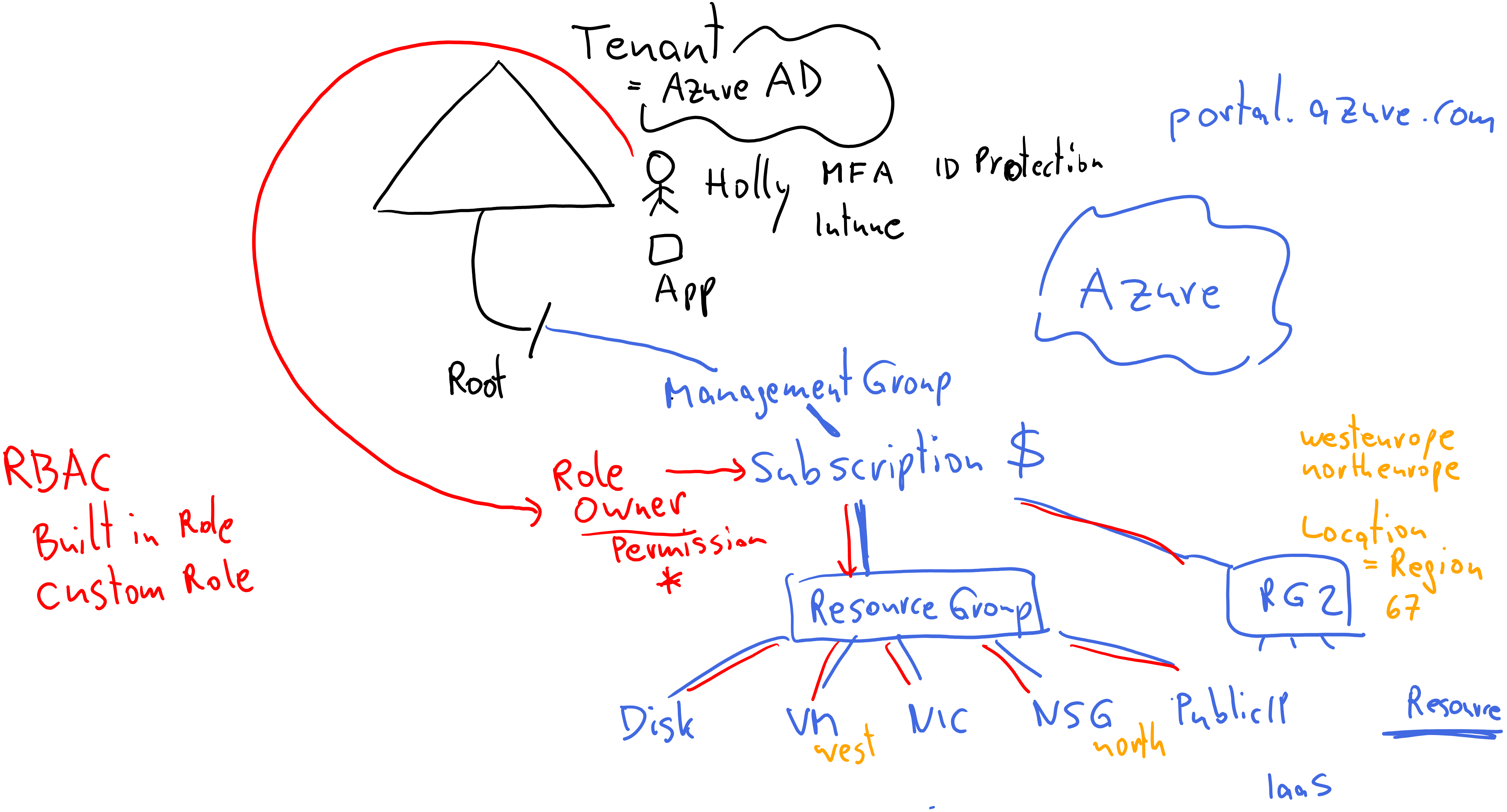
FW = FW

AppGw = WAF

Front Door = WAF + more

© Copyright Microsoft Corporation. All rights reserved.

Module 5: Implement Windows Server IaaS VM network security


Tenant
= Azure AD
Holly
MFA
ID Protection
Intune
App
Root
portal.azure.com
Azure
Management Group
Subscription $
RBAC
Built in Role
Custom Role
Role
Owner
Permission
*
westeurope
northeurope
Location
= Region
67
Resource Group
RG2
Disk
VM
west
NIC
NSG
north
PublicIP
Resource
IaaS

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
- Knowledge check and resources

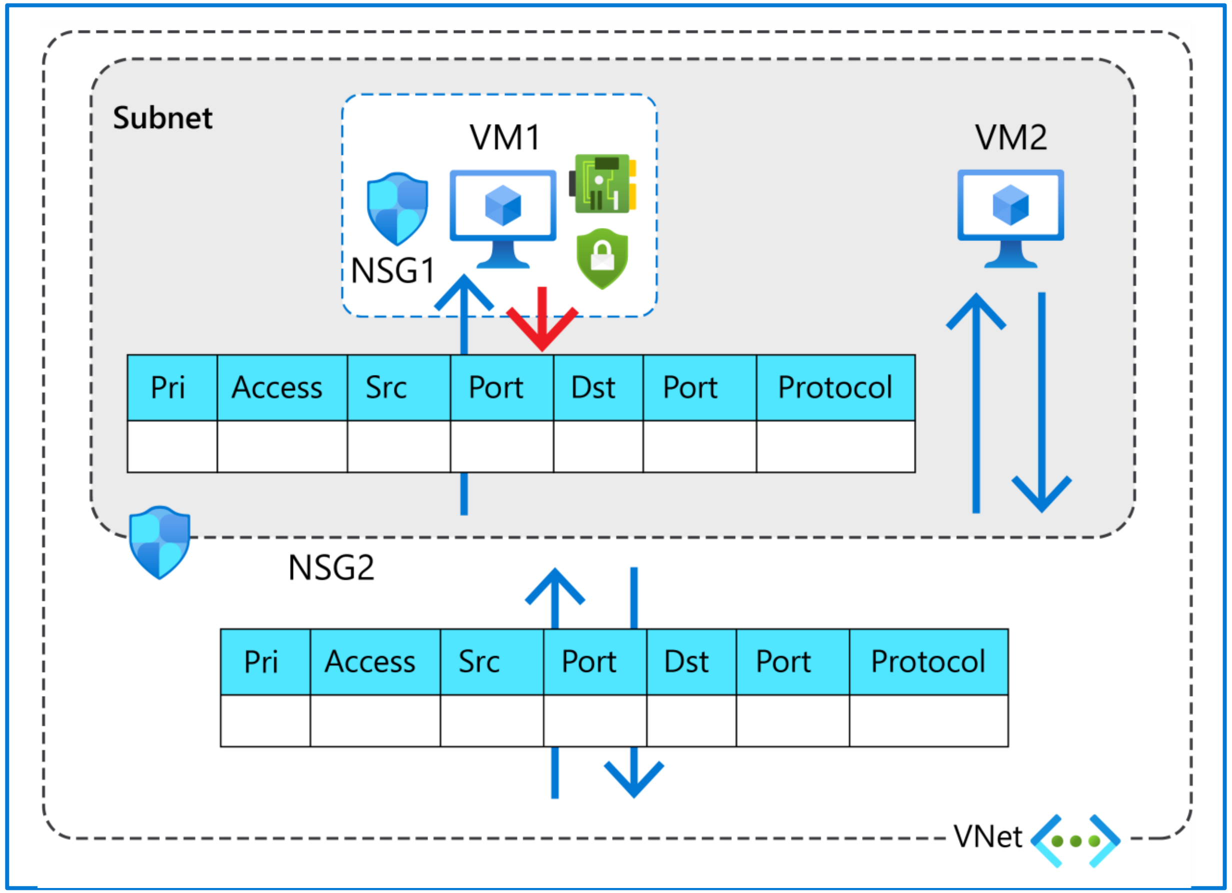
Implement network security groups

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 to applied to the ***subnet*** (NSG2) and ***network interface*** (NSG1).

You can reduce administrative effort by applying the same NSG to many resources



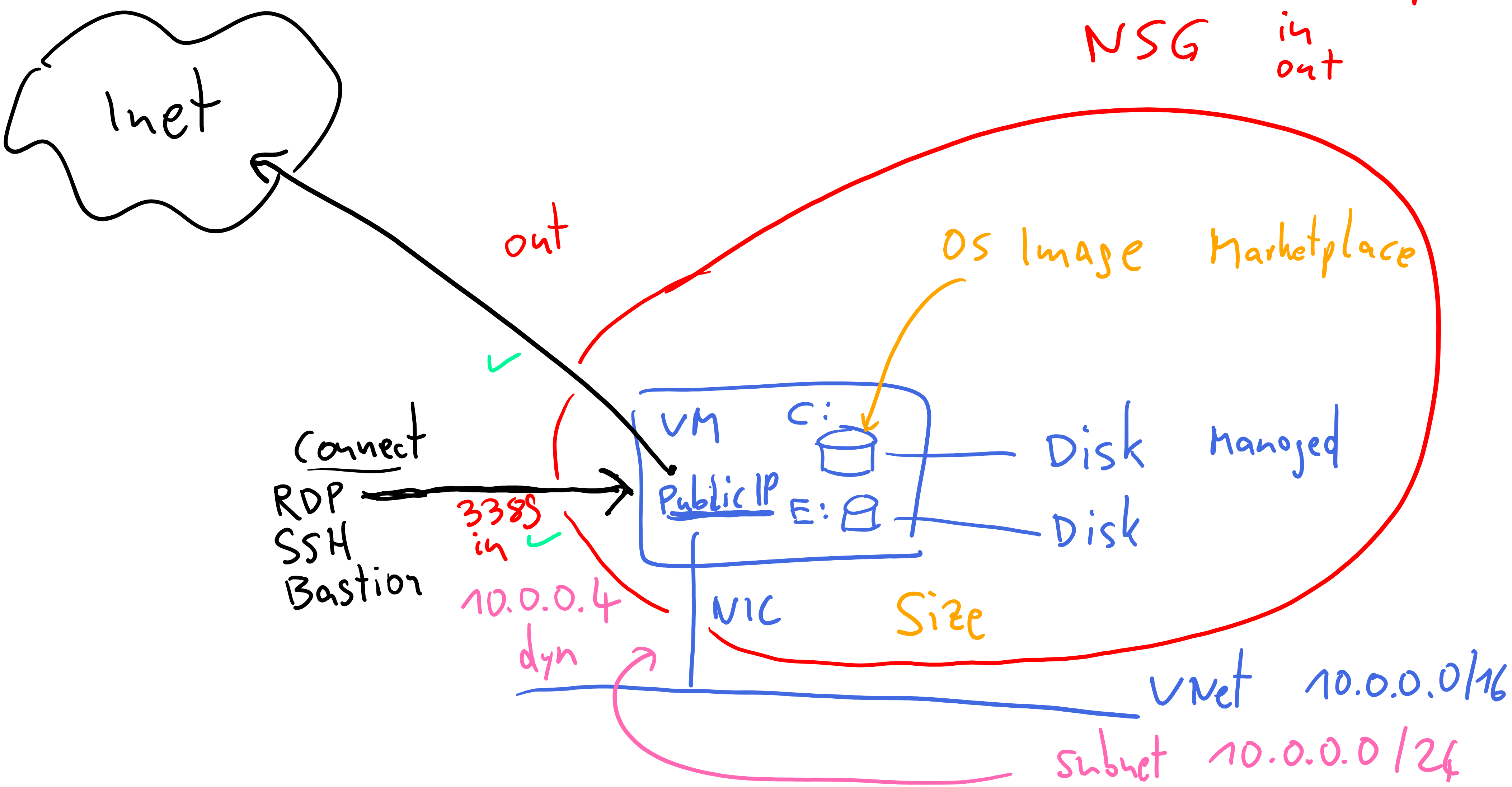
Pri	Access	Src	Port	Dst	Port	Protocol

Pri	Access	Src	Port	Dst	Port	Protocol

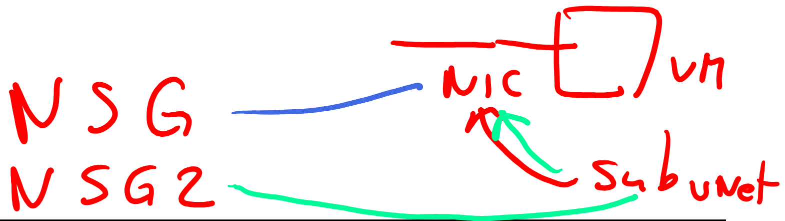
Virtual Machines IaaS

Network Security Group

NSG in out



Security rules for network security groups



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.

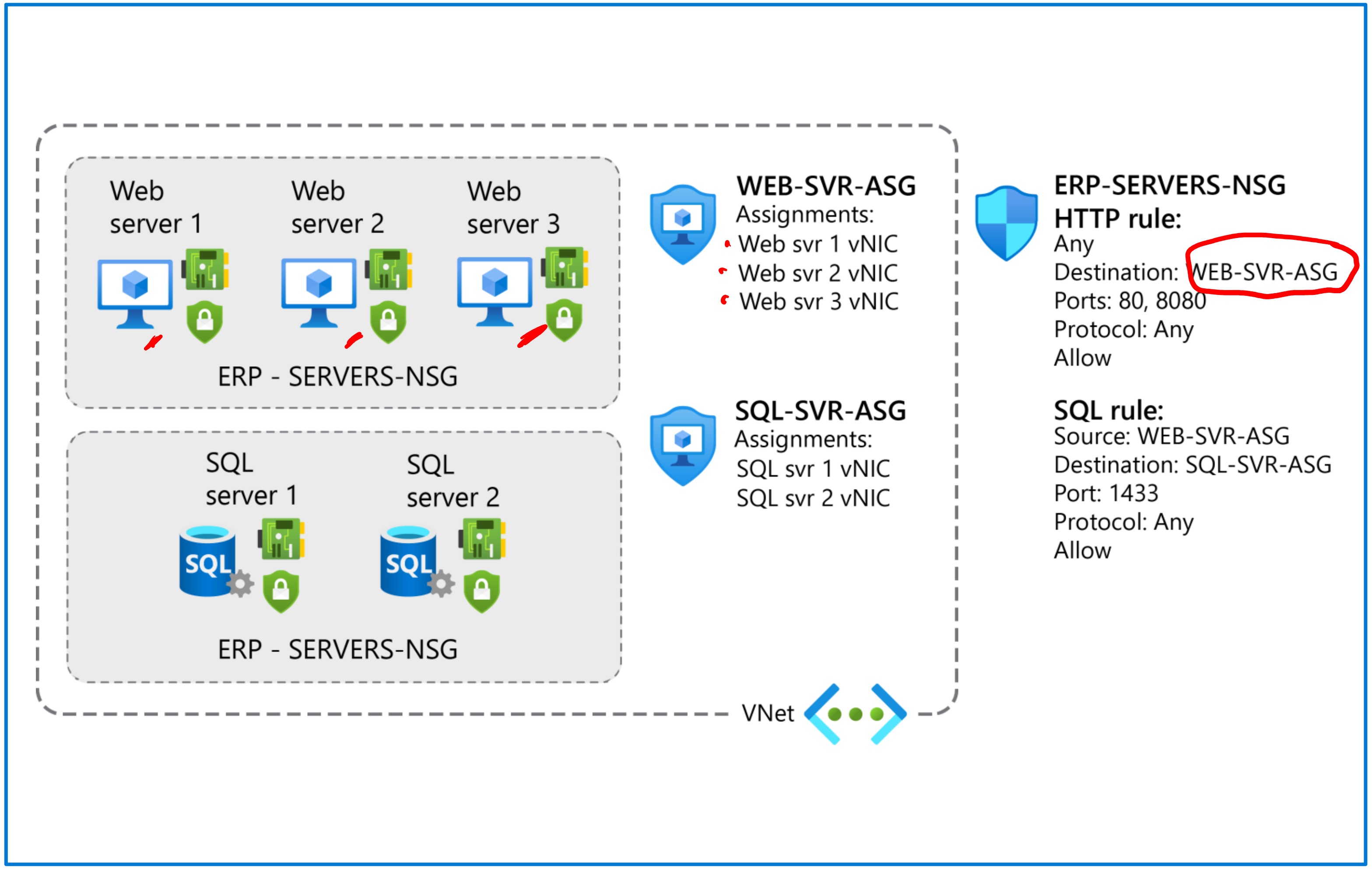
Application security groups

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.



WEB-SVR-ASG
Assignments:
- Web svr 1 vNIC
- Web svr 2 vNIC
- Web svr 3 vNIC

SQL-SVR-ASG
Assignments:
SQL svr 1 vNIC
SQL svr 2 vNIC

ERP-SERVERS-NSG

HTTP rule:
Any
Destination: WEB-SVR-ASG
Ports: 80, 8080
Protocol: Any
Allow

SQL rule:
Source: WEB-SVR-ASG
Destination: SQL-SVR-ASG
Port: 1433
Protocol: Any
Allow

Implement adaptive network hardening

How it works

Reviewing Adaptive Network Hardening alerts and rules

Applying Adaptive Network Hardening recommendations

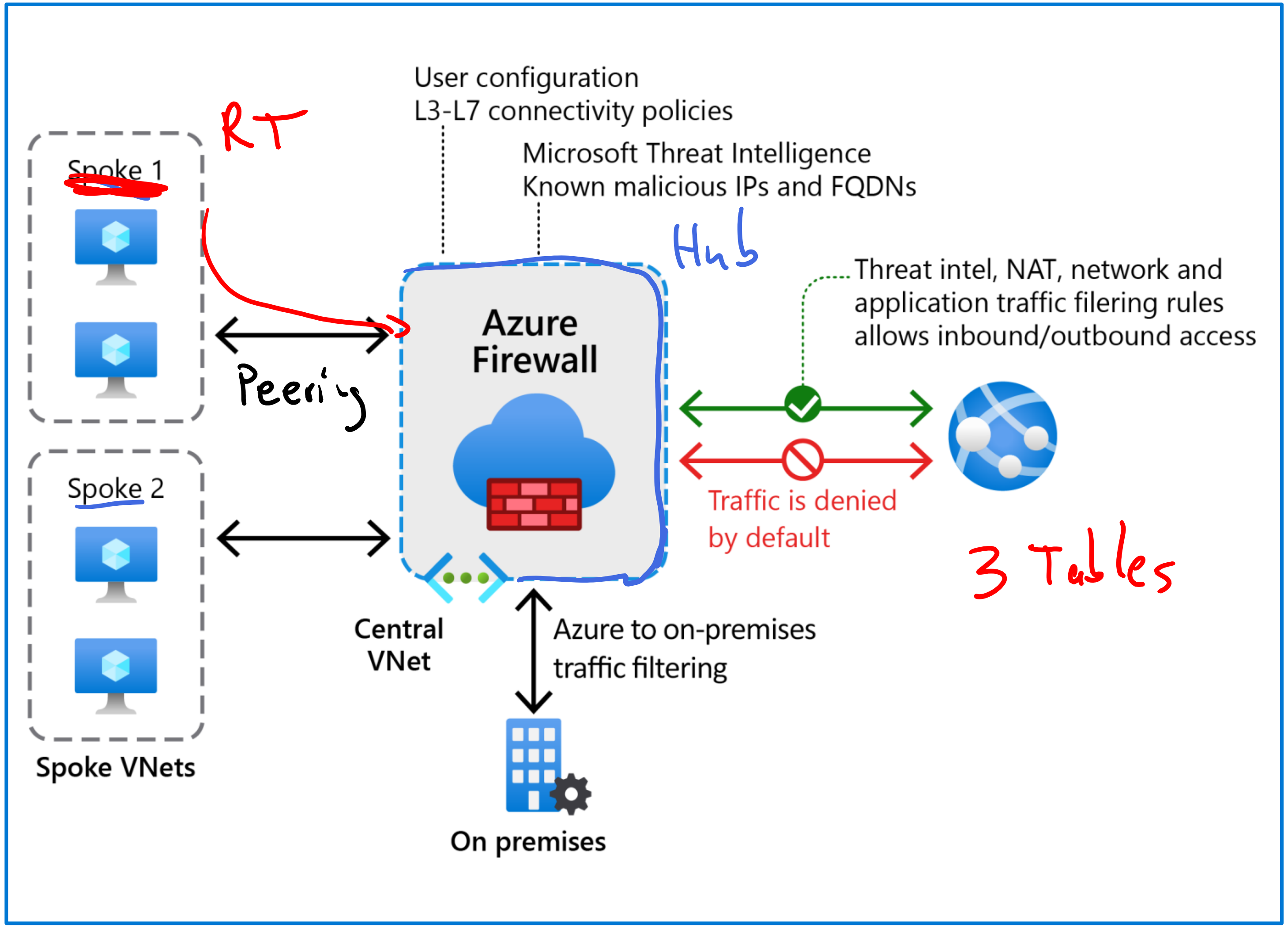
Implement Azure Firewall and Windows IaaS VMs

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.



RT
Spoke 1
Spoke 2
Spoke VNets
Peering
User configuration
L3-L7 connectivity policies
Microsoft Threat Intelligence
Known malicious IPs and FQDNs
Hub
Azure Firewall
Central VNet
Threat intel, NAT, network and application traffic filering rules allows inbound/outbound access
Traffic is denied by default
3 Tables
Azure to on-premises traffic filtering
On premises

Implement Windows firewall with Windows Server IaaS VMs

What is Windows Defender Firewall with Advanced Security?

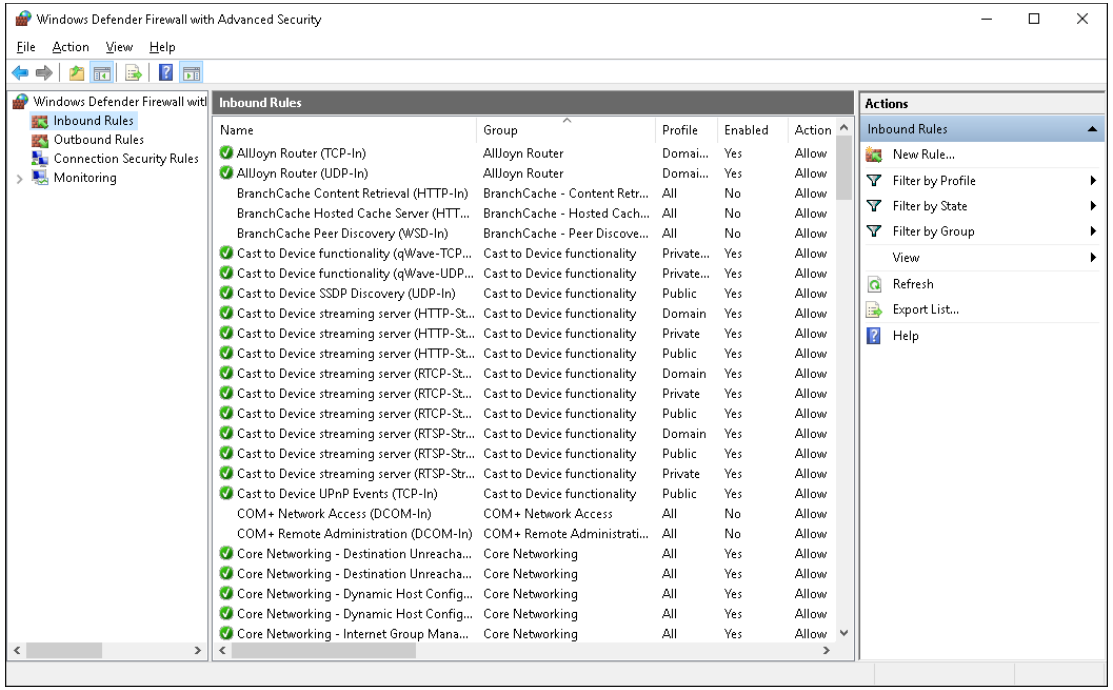
- **Windows Defender Firewall** with Advanced Security is a host-based firewall for enhancing the security of Windows Server.
- **Windows Defender Firewall** with Advanced Security is more than just a simple firewall, because it includes features such as firewall profiles and connection security rules.

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

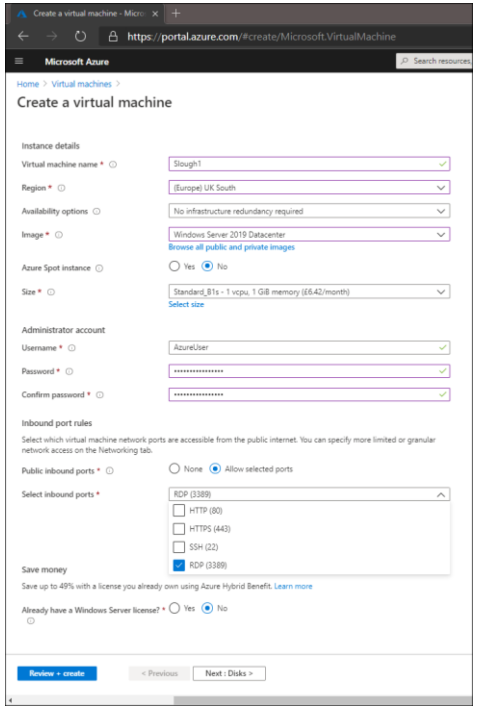
Administering Windows Defender Firewall



Inbound Rules

Name	Group	Profile	Enabled	Action
✓ AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow
✓ AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
✓ Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow
✓ Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow
✓ Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow
✓ Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Domain	Yes	Allow
✓ Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Private	Yes	Allow
✓ Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public	Yes	Allow
✓ Cast to Device streaming server (RTCP-St...	Cast to Device functionality	Domain	Yes	Allow
✓ Cast to Device streaming server (RTCP-St...	Cast to Device functionality	Private	Yes	Allow
✓ Cast to Device streaming server (RTCP-St...	Cast to Device functionality	Public	Yes	Allow
✓ Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Domain	Yes	Allow
✓ Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Public	Yes	Allow
✓ Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Private	Yes	Allow
✓ Cast to Device UPnP Events (TCP-In)	Cast to Device functionality	Public	Yes	Allow
COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow
COM+ Remote Administration (DCOM-In)	COM+ Remote Administrati...	All	No	Allow
✓ Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
✓ Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
✓ Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
✓ Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
✓ Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow

Creating firewall rules when creating a VM in Azure



https://portal.azure.com/#create/Microsoft.VirtualMachine

Create a virtual machine

Instance details

Virtual machine name * Slough1

Region * (Europe) UK South

Availability options No infrastructure redundancy required

Image * Windows Server 2019 Datacenter

Browse all public and private images

Azure Spot instance ○ Yes ● No

Size * Standard_B1s - 1 vcpu, 1 GiB memory (£6.42/month)

Select size

Administrator account

Username * AzureUser

Password * ••••••••••••••••

Confirm password * ••••••••••••••••

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ○ None ● Allow selected ports

Select inbound ports * RDP (3389)

□ HTTP (80)
□ HTTPS (443)
□ SSH (22)
☑ RDP (3389)

Save money

Save up to 49% with a license you already own using Azure Hybrid Benefit. Learn more

Already have a Windows Server license? * ○ Yes ● No

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?

Monitoring 、Diagnosing

Reviewing metrics、

Managing logs

Monitoring

Use Azure Network Watcher to monitor communications between VMs and endpoints.

Diagnosing

Network Watcher provides a number of 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

Knowledge Check and Resources – Implement Windows Server IaaS VM network security

Knowledge Check

Microsoft Learn Modules (docs.microsoft.com/Learn)

Implement Windows Server IaaS VM network security

Module 2: Audit the security of Windows Server IaaS Virtual Machines

Audit the security of Windows Server IaaS Virtual Machines

- Describe ~~Azure Security Center~~ Defender for Cloud
- Enable Azure Security Center in hybrid environments
- Audit your VM’s regulatory compliance
- Implement and assess security policies
- Demonstration – Protect your resources with Azure Security Center
- What is ~~Azure~~ Sentinel?
  MS
- Implement SIEM and SOAR solutions in Azure Sentinel
  SPLUNK
- Knowledge check and resources

What is Azure Security Center?

Defender for Cloud

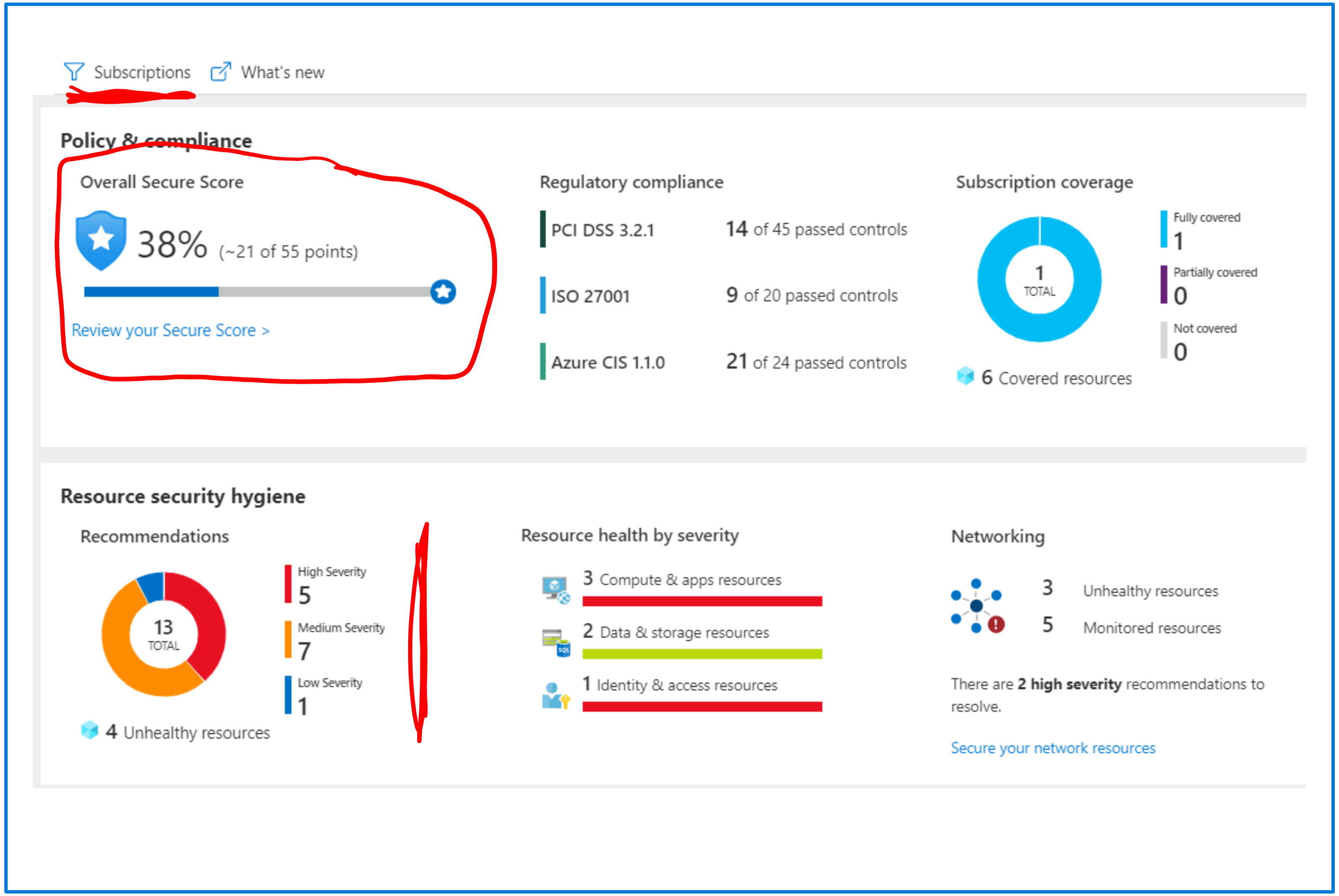
free

cost Plan

30 free

With Security Center 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. Security Center can also perform automatic data classification in your Azure SQL databases.



Subscriptions   What's new

Policy & compliance

Overall Secure Score

38% (~21 of 55 points)

Review your Secure Score >

Regulatory compliance

PCI DSS 3.2.1	14 of 45 passed controls
ISO 27001	9 of 20 passed controls
Azure CIS 1.1.0	21 of 24 passed controls

Subscription coverage

1 TOTAL

Fully covered 1

Partially covered 0

Not covered 0

6 Covered resources

Resource security hygiene

Recommendations

13 TOTAL

High Severity 5

Medium Severity 7

Low Severity 1

4 Unhealthy resources

Resource health by severity

3 Compute & apps resources

2 Data & storage resources

1 Identity & access resources

Networking

3 Unhealthy resources

5 Monitored resources

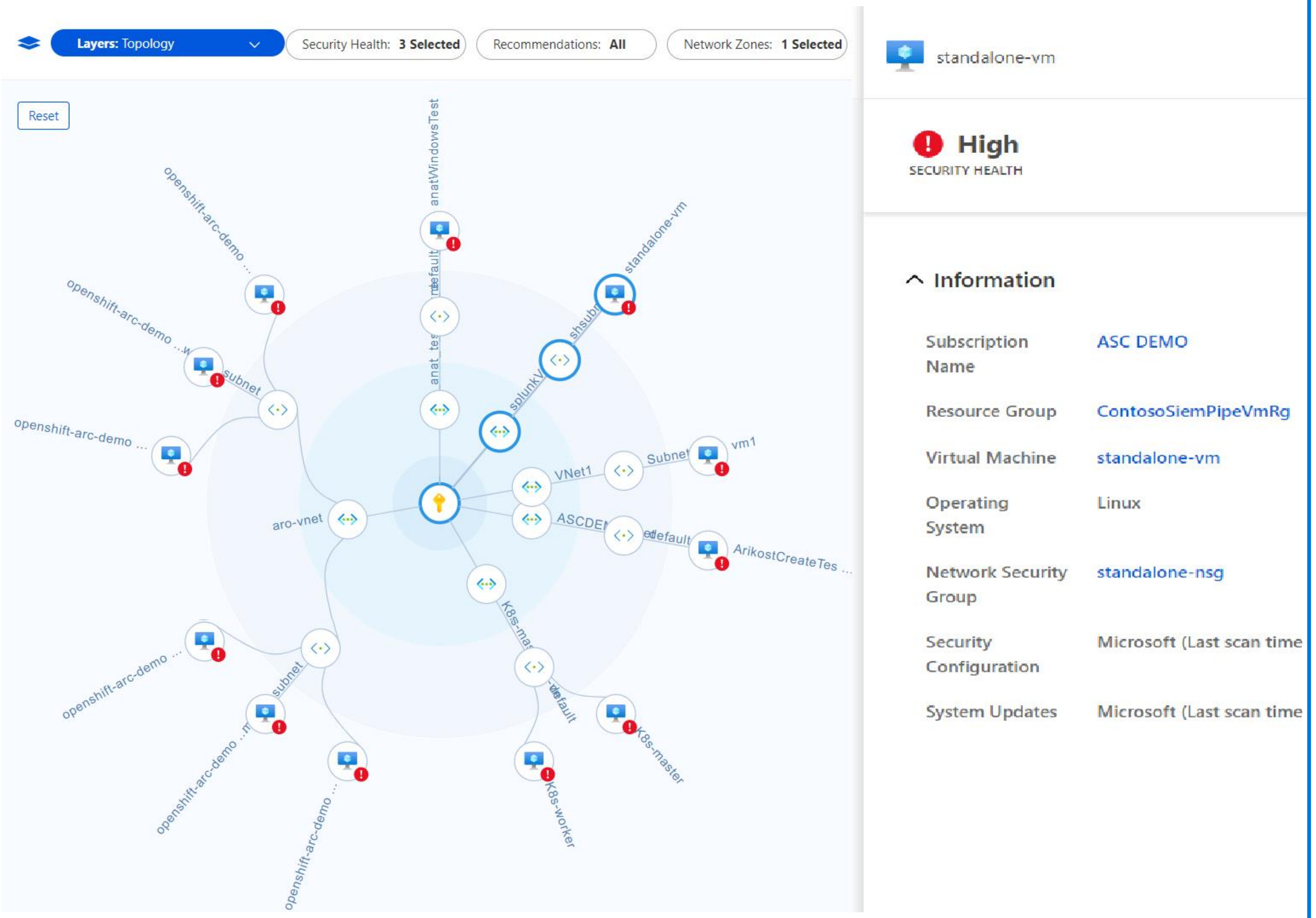
There are **2 high severity** recommendations to resolve.

Secure your network resources

Security Center feature coverage for VMs

- Microsoft Intune Endpoint Protection assessment
- Missing operating system patches assessment, VM behavioral analytics and security alerts
- Security misconfigurations assessment ˎ
- 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

Network map: view of the topology map with security health



Layers: Topology

Security Health: 3 Selected

Recommendations: All

Network Zones: 1 Selected

standalone-vm

High

SECURITY HEALTH

Information

Subscription Name	ASC DEMO
Resource Group	ContosoSiemPipeVmRg
Virtual Machine	standalone-vm
Operating System	Linux
Network Security Group	standalone-nsg
Security Configuration	Microsoft (Last scan time
System Updates	Microsoft (Last scan time

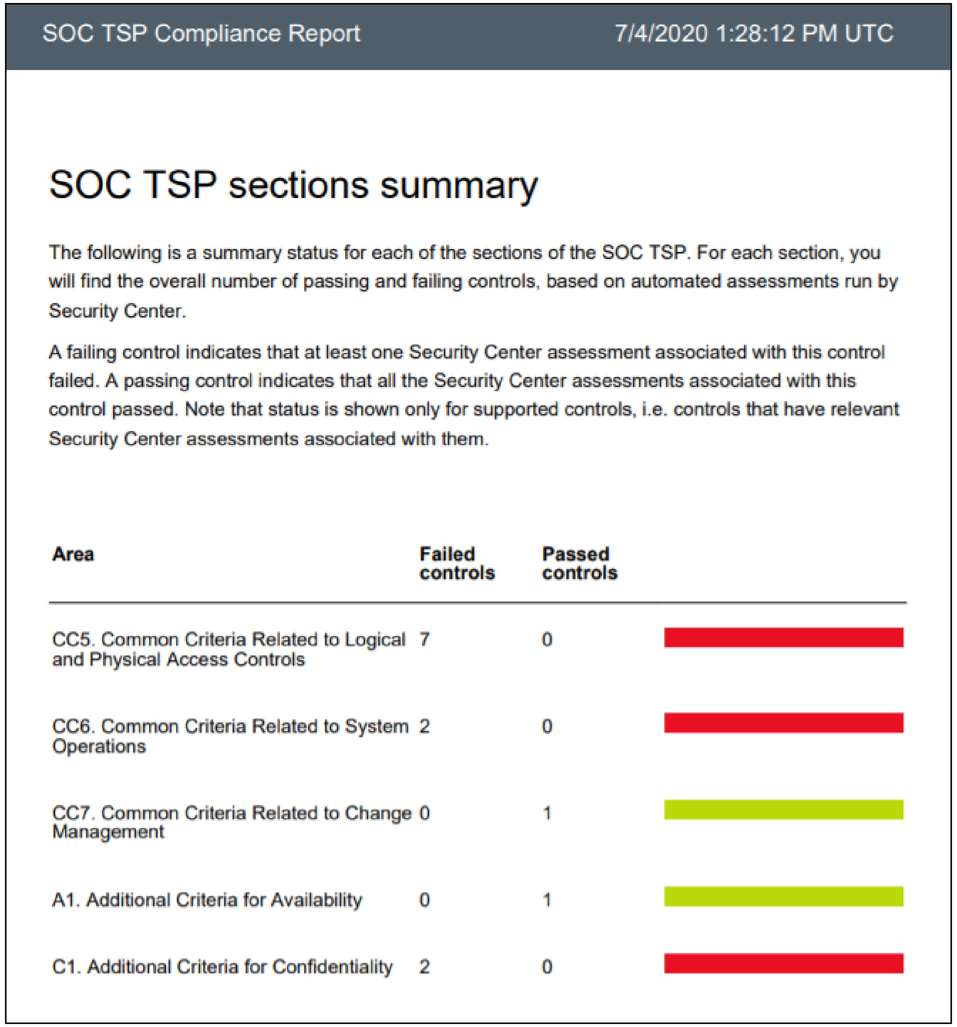
© Copyright Microsoft Corporation. All rights reserved.

Enable Azure Security Center in hybrid environments

- Enable the Security Center 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 **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	Part of the **International Standards Organization** (ISO) 27000 family of standards, 27001 defines a system that can bring management to IT systems.
Azure CIS 1.1.0	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 Security Center, select the Overall Secure Score tile.

Run a vulnerability assessment against your Windows Server IaaS VM

- You can use Security Center 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 Azure Security Center

Access to Security center

Explore Policy and Compliance

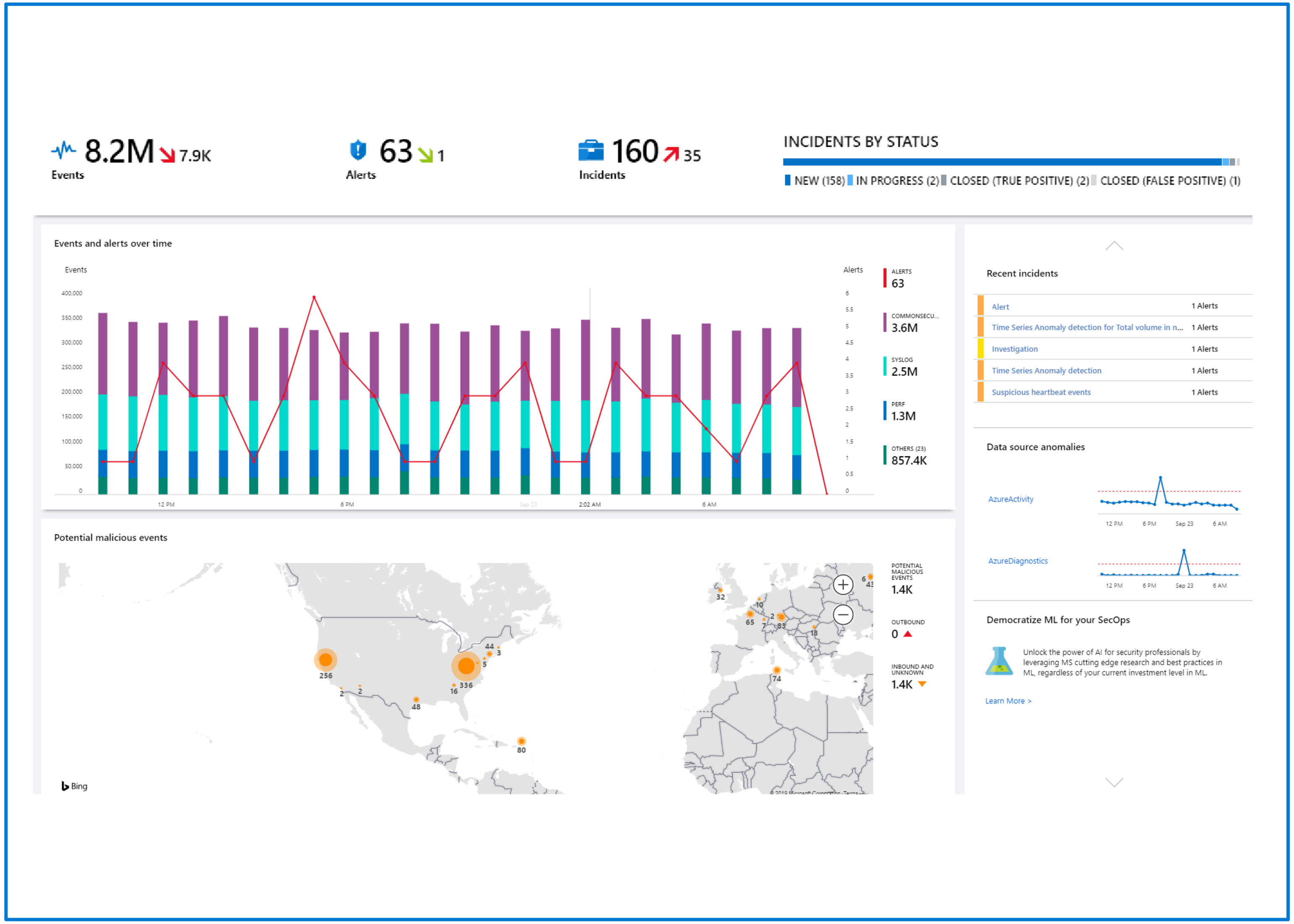
Select Windows Server VM

Install Endpoint protection and enable JIT

What is ~~Azure~~ 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.



8.2M 7.9K Events | 63 1 Alerts | 160 35 Incidents

INCIDENTS BY STATUS
NEW (158) IN PROGRESS (2) CLOSED (TRUE POSITIVE) (2) CLOSED (FALSE POSITIVE) (1)

Recent incidents

Alert	1 Alerts
Time Series Anomaly detection for Total volume in n...	1 Alerts
Investigation	1 Alerts
Time Series Anomaly detection	1 Alerts
Suspicious heartbeat events	1 Alerts

Democratize ML for your SecOps

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML.

Learn More >

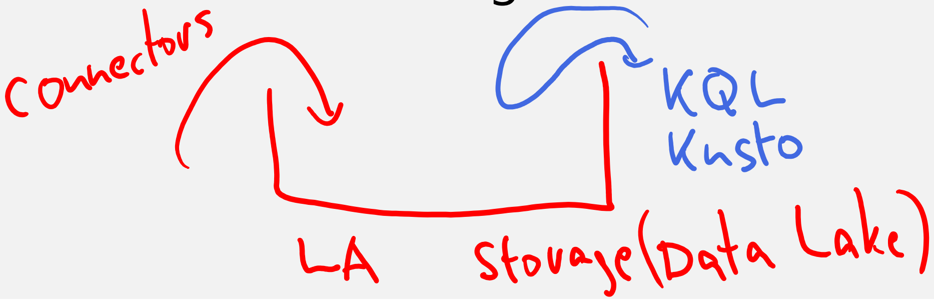
Implement SIEM and SOAR solutions in Azure Sentinel

What is SIEM?

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

To implement SIEM functionality in Sentinel:

- Enable Azure 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.

Knowledge Check and Resources – Audit the security of Windows Server IaaS Virtual Machines

Knowledge Check

Microsoft Learn Modules (docs.microsoft.com/Learn)

Audit the security of Windows Server IaaS Virtual Machines

IaaS
(VM)

PaaS
(App Service, Container)

"Server Less"

Customer

Hyper-V

Azure

Module 3: Manage Azure updates

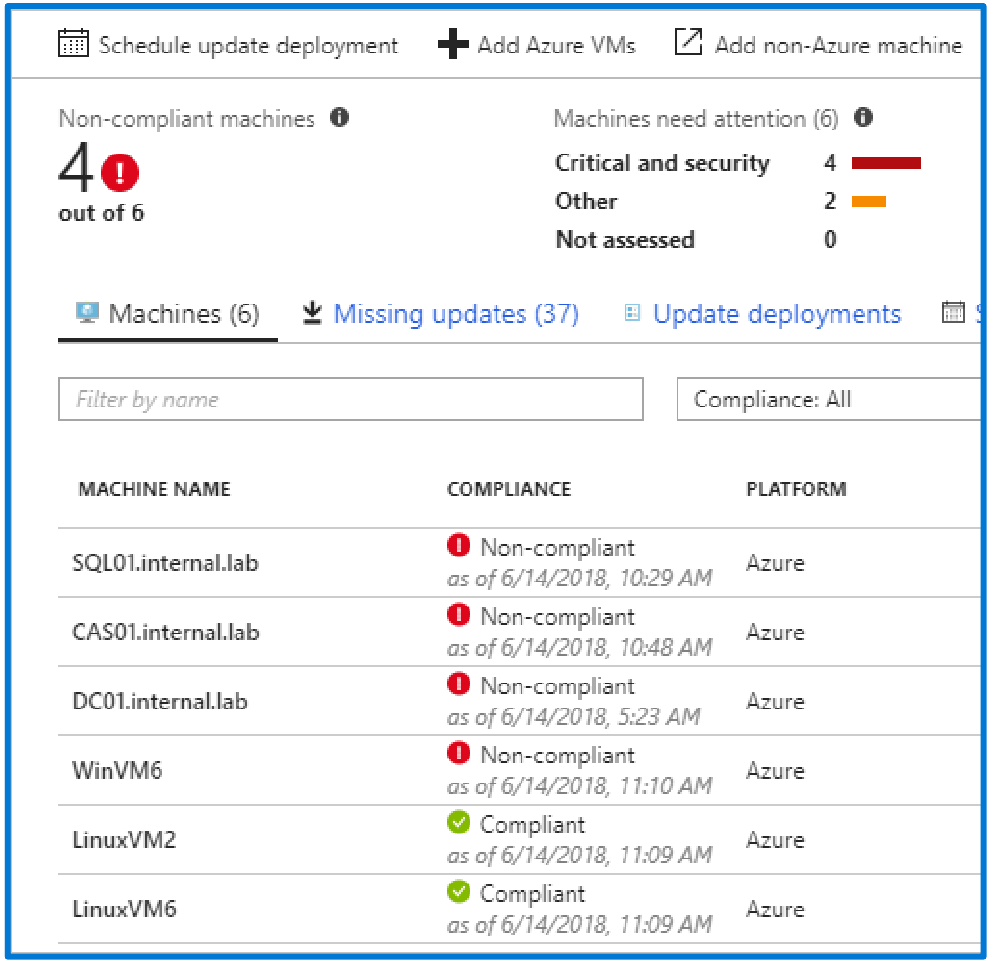
Manage Azure updates

- Describe Azure updates
- Enable Update Management
- Deploy updates
- Review an update assessment
- Manage updates for your Azure VMs
- Knowledge check and resources

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.



Non-compliant machines

4

out of 6

Machines need attention (6)

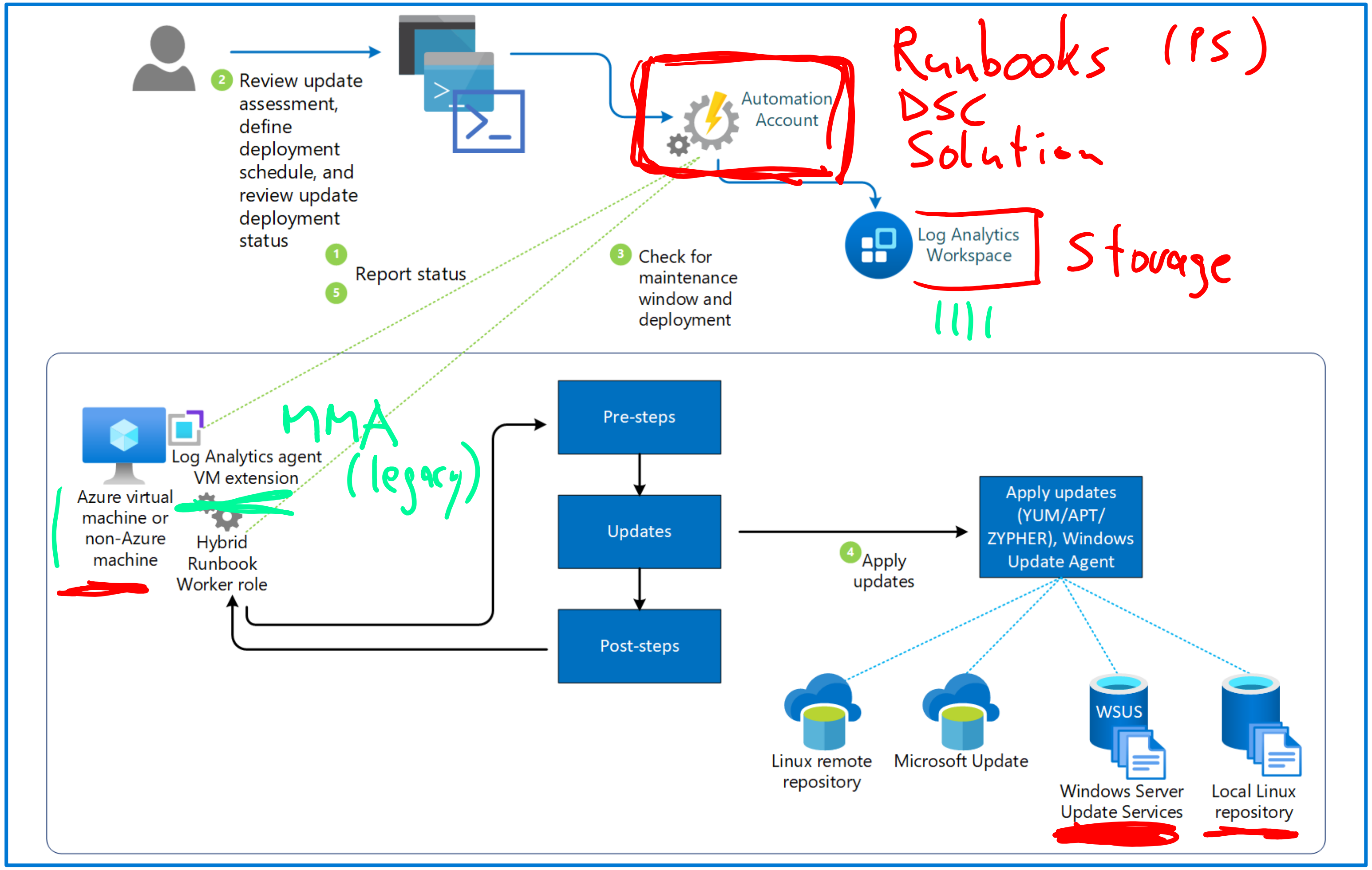
Critical and security	4
Other	2
Not assessed	0

MACHINE NAME	COMPLIANCE	PLATFORM
SQL01.internal.lab	Non-compliant *as of 6/14/2018, 10:29 AM*	Azure
CAS01.internal.lab	Non-compliant *as of 6/14/2018, 10:48 AM*	Azure
DC01.internal.lab	Non-compliant *as of 6/14/2018, 5:23 AM*	Azure
WinVM6	Non-compliant *as of 6/14/2018, 11:10 AM*	Azure
LinuxVM2	Compliant *as of 6/14/2018, 11:09 AM*	Azure
LinuxVM6	Compliant *as of 6/14/2018, 11:09 AM*	Azure

Azure Update Management

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



2 Review update assessment, define deployment schedule, and review update deployment status
Automation Account
Runbooks (PS)
DSC
Solution
Log Analytics Workspace
Storage
1 Report status
5
3 Check for maintenance window and deployment
Log Analytics agent VM extension
MMA (legacy)
Azure virtual machine or non-Azure machine
Hybrid Runbook Worker role
Pre-steps
Updates
Post-steps
4 Apply updates
Apply updates (YUM/APT/ ZYPHER), Windows Update Agent
Linux remote repository
Microsoft Update
WSUS
Windows Server Update Services
Local Linux repository

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

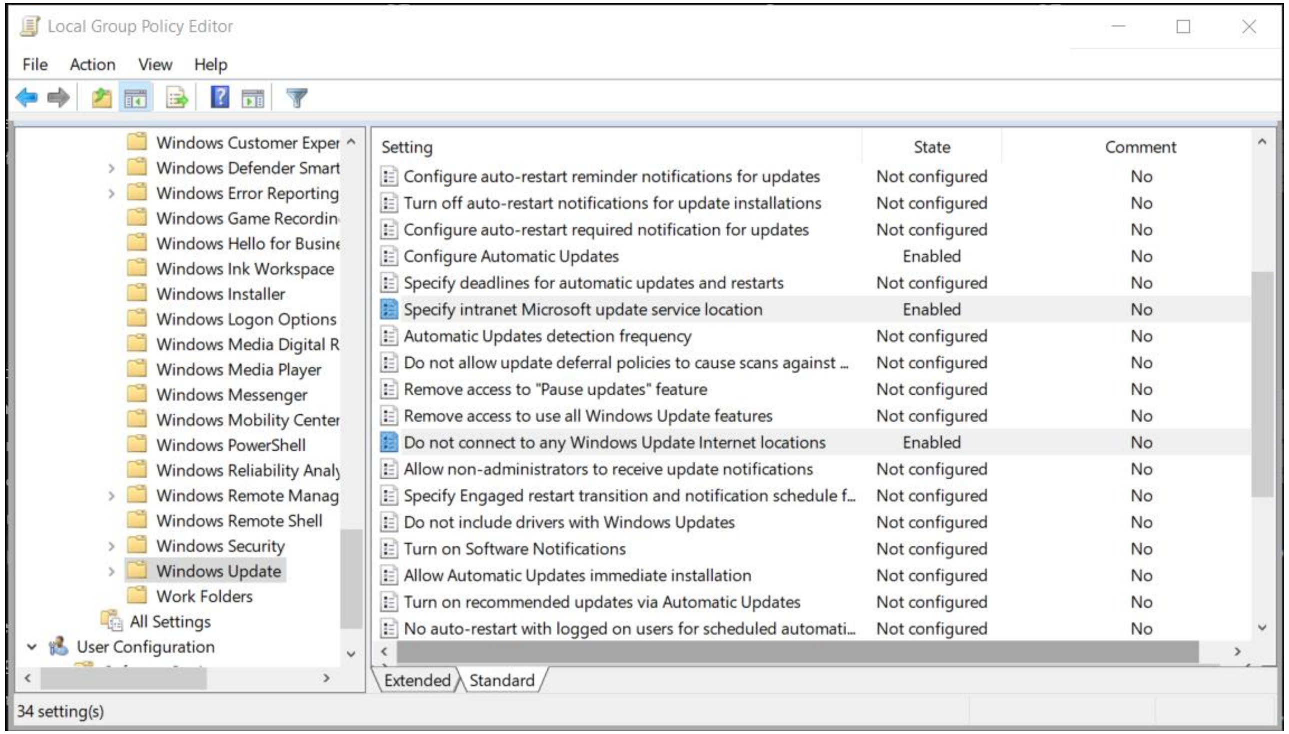
Update Management respects many of the settings specified to control the Windows Update client.

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*

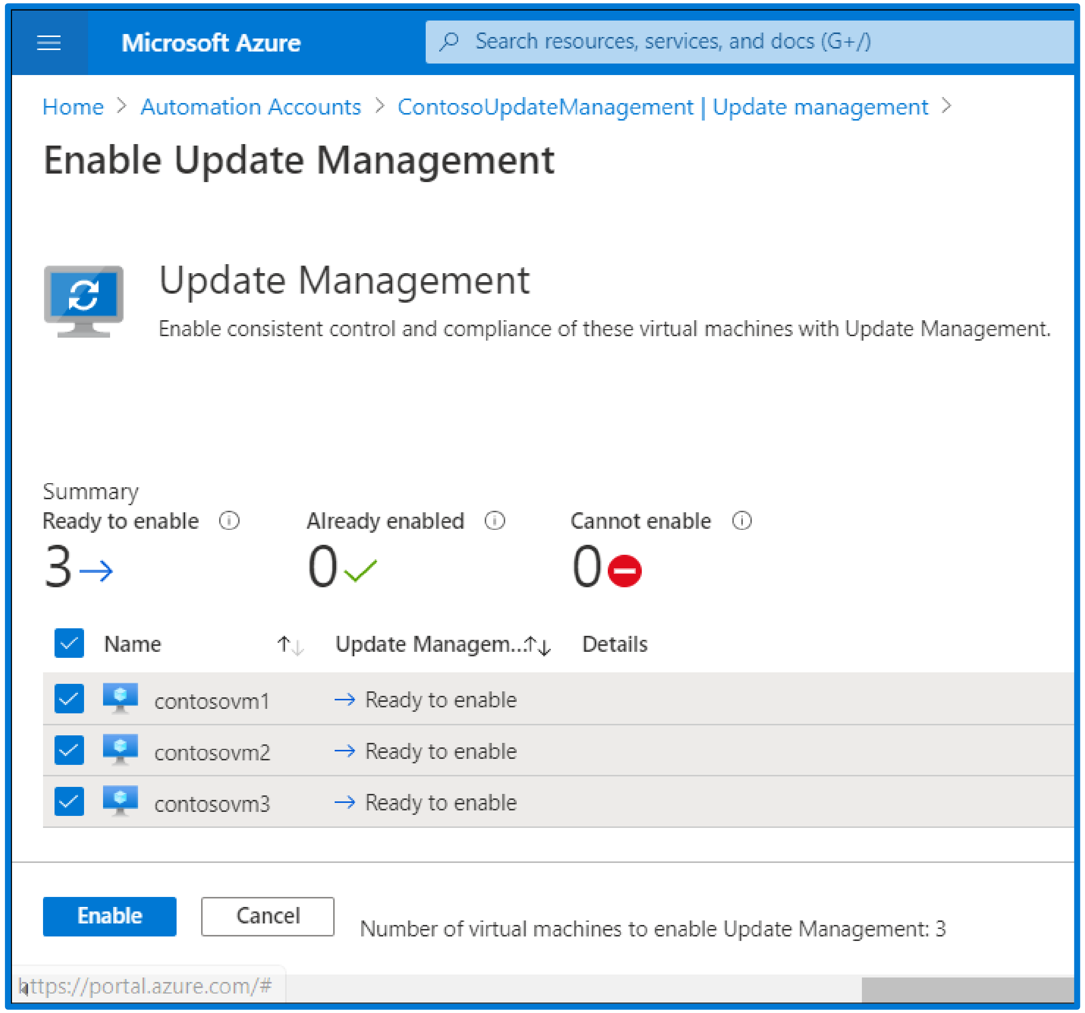


Setting	State	Comment
Configure auto-restart reminder notifications for updates	Not configured	No
Turn off auto-restart notifications for update installations	Not configured	No
Configure auto-restart required notification for updates	Not configured	No
Configure Automatic Updates	Enabled	No
Specify deadlines for automatic updates and restarts	Not configured	No
Specify intranet Microsoft update service location	Enabled	No
Automatic Updates detection frequency	Not configured	No
Do not allow update deferral policies to cause scans against ...	Not configured	No
Remove access to "Pause updates" feature	Not configured	No
Remove access to use all Windows Update features	Not configured	No
Do not connect to any Windows Update Internet locations	Enabled	No
Allow non-administrators to receive update notifications	Not configured	No
Specify Engaged restart transition and notification schedule f...	Not configured	No
Do not include drivers with Windows Updates	Not configured	No
Turn on Software Notifications	Not configured	No
Allow Automatic Updates immediate installation	Not configured	No
Turn on recommended updates via Automatic Updates	Not configured	No
No auto-restart with logged on users for scheduled automati...	Not configured	No

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.



Home > Automation Accounts > ContosoUpdateManagement | Update management >

Enable Update Management

Update Management

Enable consistent control and compliance of these virtual machines with Update Management.

Summary

Ready to enable	Already enabled	Cannot enable
3 →	0 ✓	0 ⛔

☑	Name	Update Managem...	Details
☑	contosovm1	→ Ready to enable	
☑	contosovm2	→ Ready to enable	
☑	contosovm3	→ Ready to enable	

Number of virtual machines to enable Update Management: 3

https://portal.azure.com/#

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

Knowledge Check and Resources – Manage Azure updates

Knowledge Check

Microsoft Learn Modules (docs.microsoft.com/Learn)

Manage Azure updates

Module 4: Create and implement application allowlists with adaptive application control

Adaptive application control

Describe adaptive application control

Enable adaptive application control

Configure a new application control policy

Move a VM from one group to another

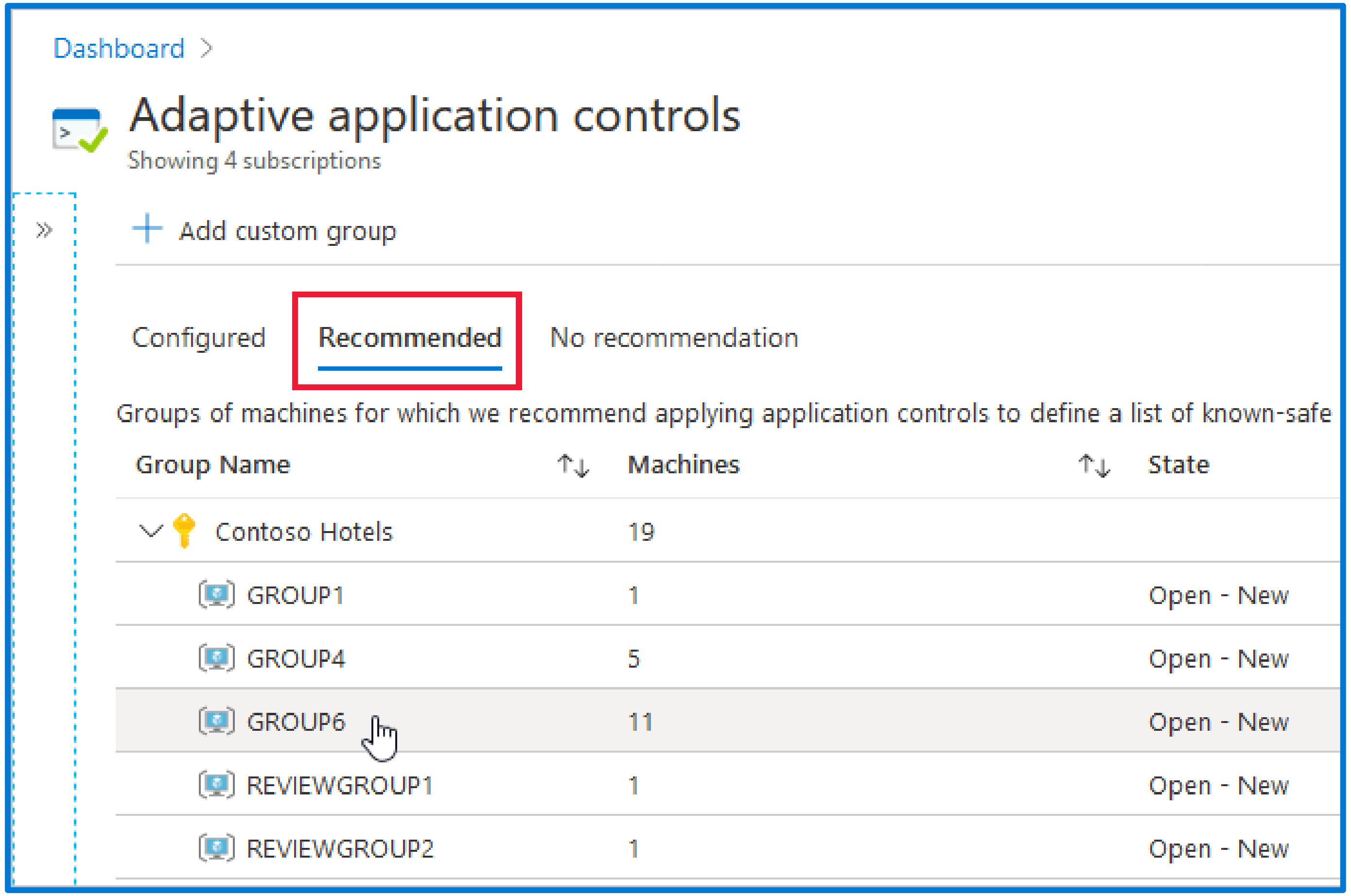
Knowledge check and resources

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.



Adaptive application controls

Showing 4 subscriptions

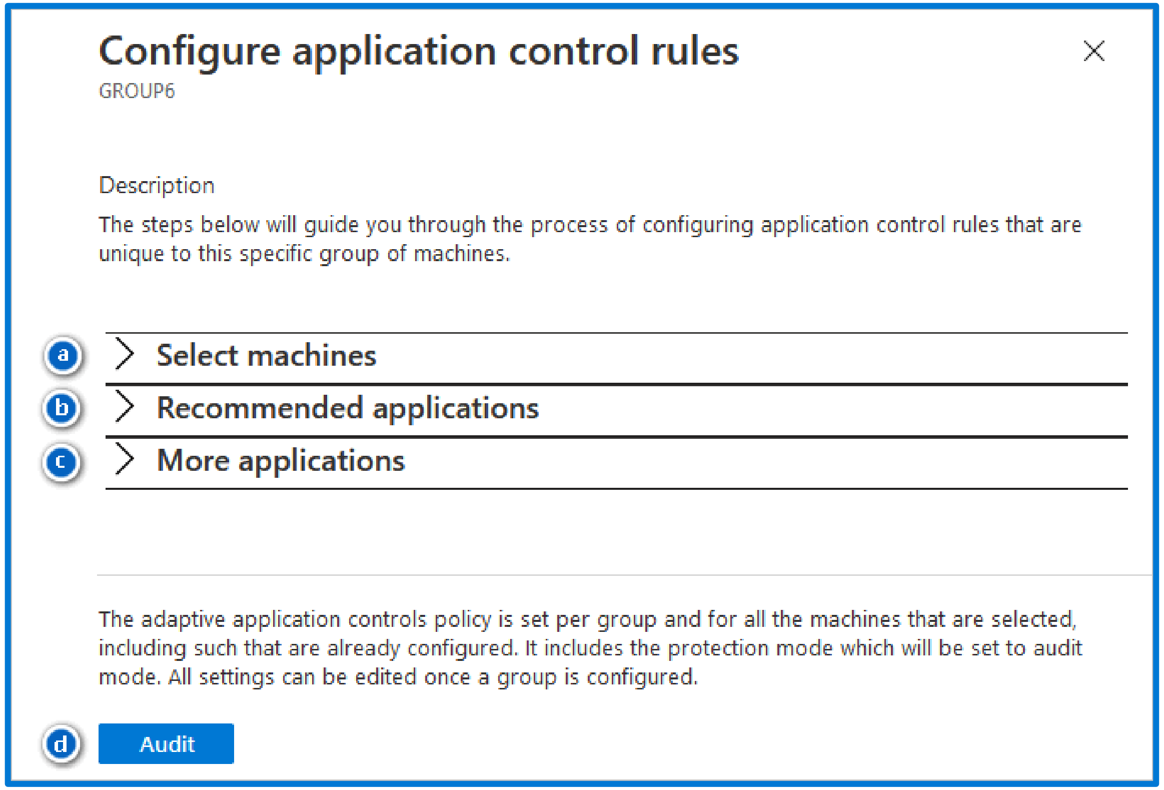
Groups of machines for which we recommend applying application controls to define a list of known-safe

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

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 Security Center.
- 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?



Configure application control rules

GROUP6

Description

The steps below will guide you through the process of configuring application control rules that are unique to this specific group of machines.

a Select machines

b Recommended applications

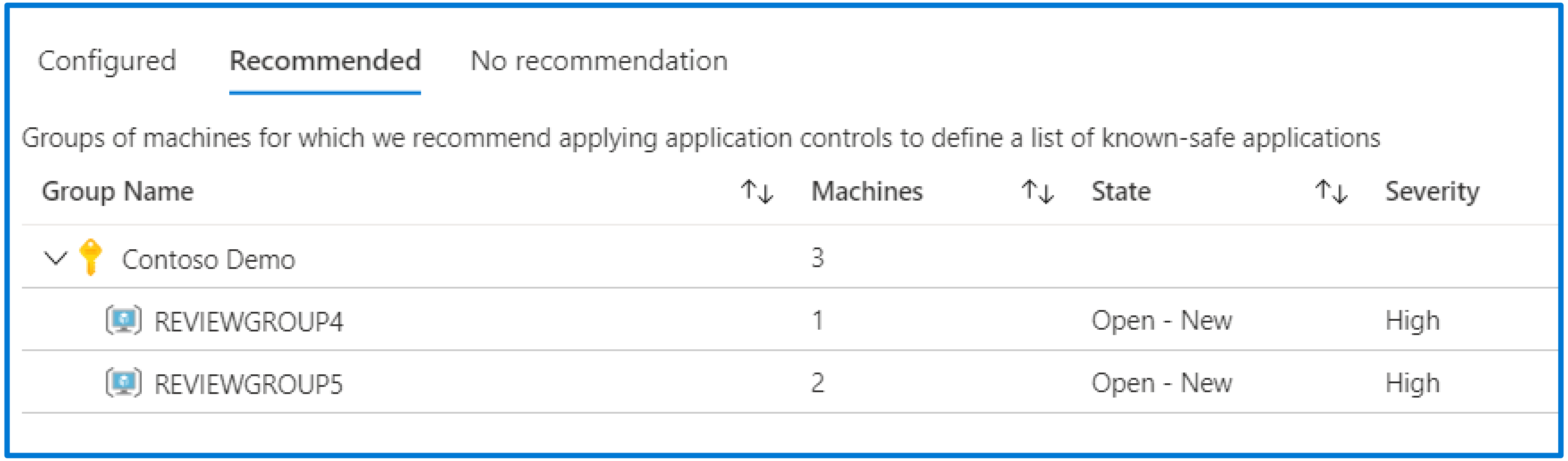
c More applications

The adaptive application controls policy is set per group and for all the machines that are selected, including such that are already configured. It includes the protection mode which will be set to audit mode. All settings can be edited once a group is configured.

d Audit

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. Security Center 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.



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

Select the **Recommended** tab for a list of groups with application control recommendations

After selecting a group, review the **Configure application control rules** blade.

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.

Within the Recommended applications section are two sections as described in the following table.

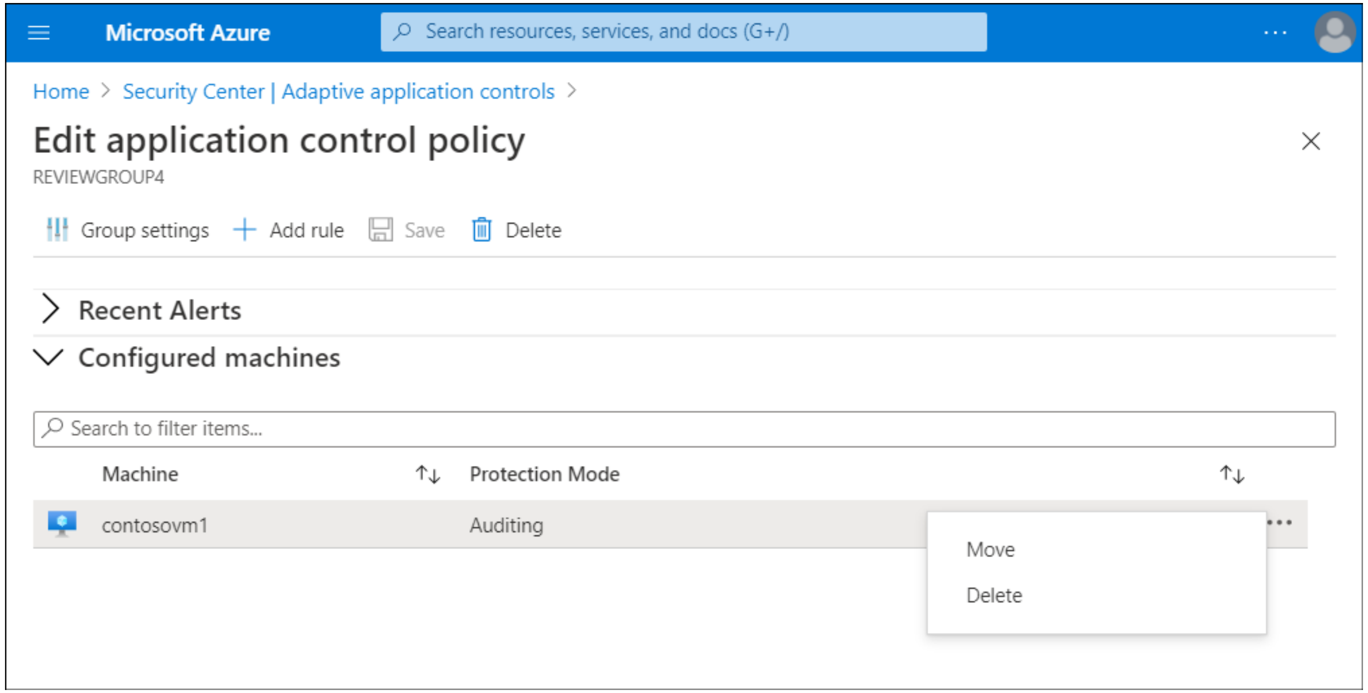
Review the applications in each list and clear the check boxes of those that you don't want to apply. The following table describes the information that the lists contain.

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.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Security Center | Adaptive application controls >
Edit application control policy
REVIEWGROUP4
Group settings
Add rule
Save
Delete
Recent Alerts
Configured machines
Search to filter items...
Machine
Protection Mode
contosovm1
Auditing
Move
Delete

Knowledge Check and Resources – Adaptive application control

Knowledge Check

Microsoft Learn Modules (docs.microsoft.com/Learn)

Create and implement application allowlists with adaptive application control

Module 5: Configure BitLocker disk encryption for Windows IaaS Virtual Machines

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
- Knowledge check and resources

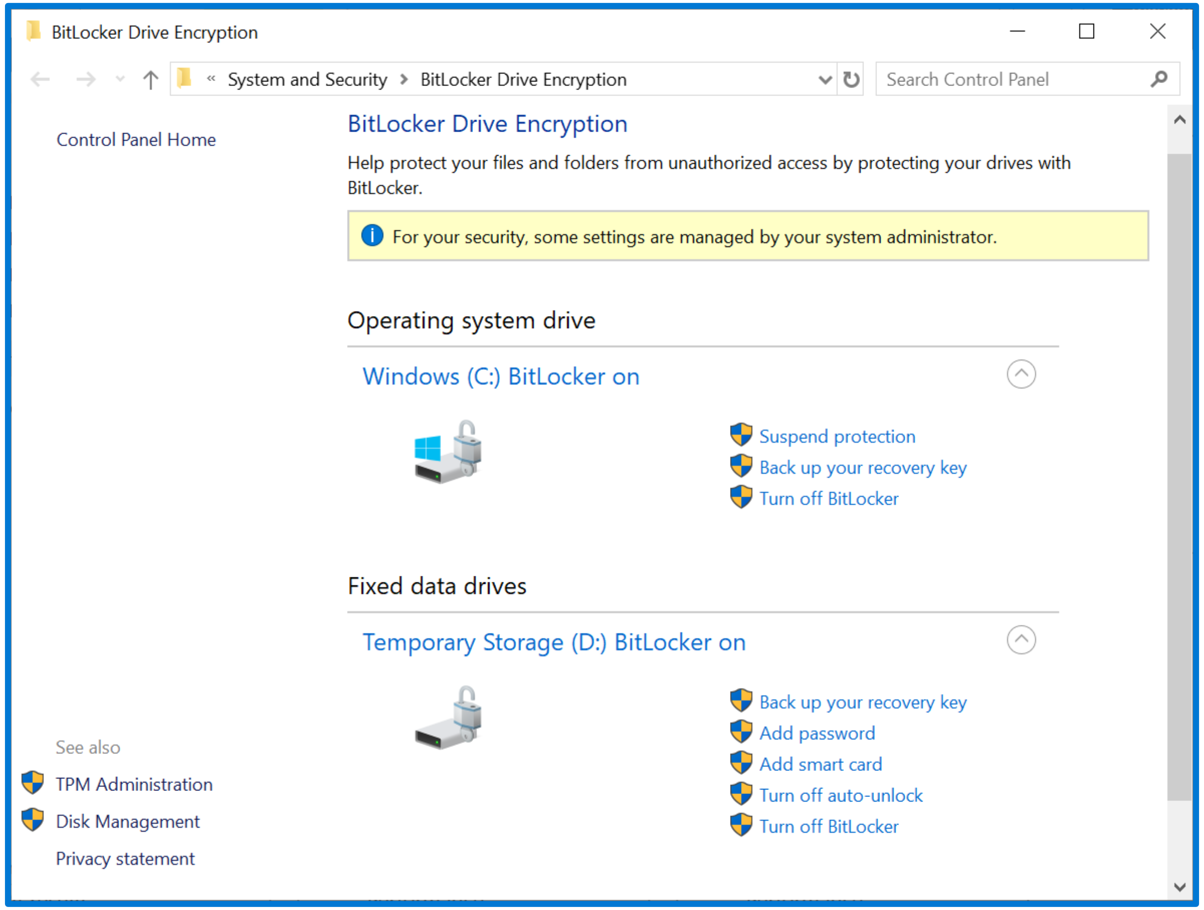
Describe Azure Disk Encryption and server-side encryption

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



BitLocker Drive Encryption
« System and Security › BitLocker Drive Encryption
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

For your security, some settings are managed by your system administrator.

Operating system drive

Windows (C:) BitLocker on

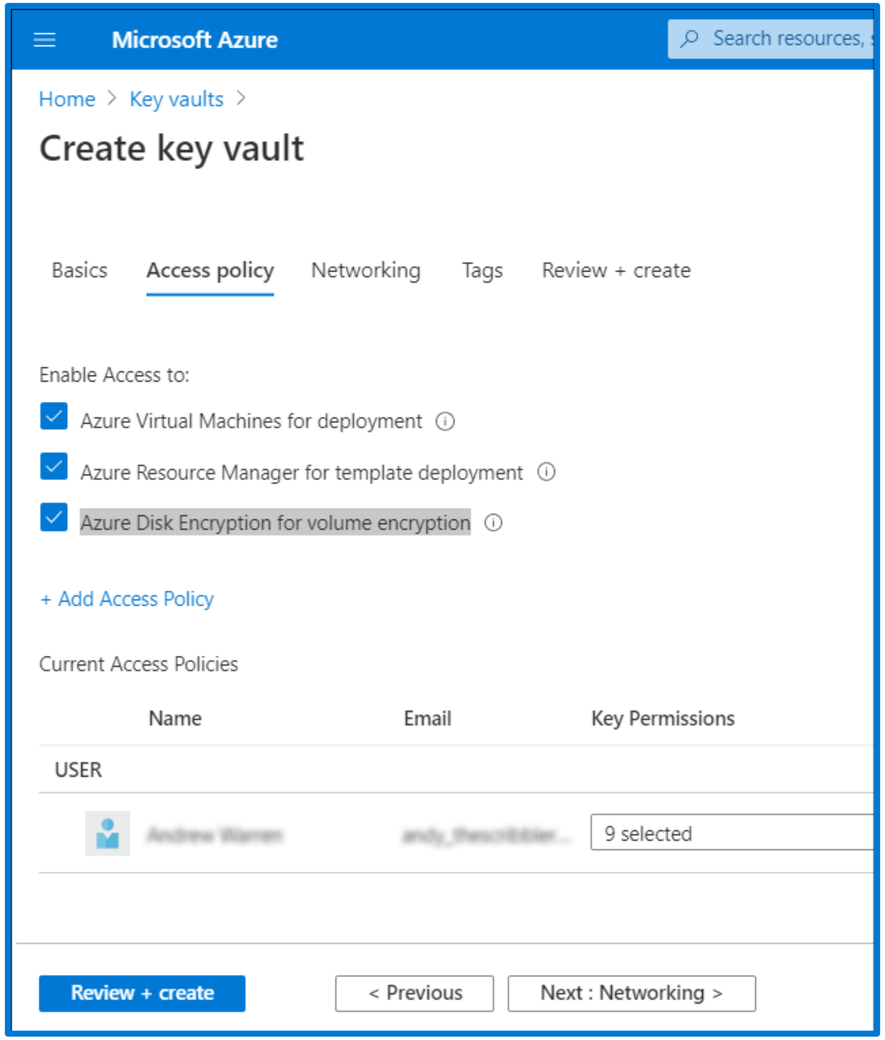
Fixed data drives

Temporary Storage (D:) BitLocker on

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.



Create key vault

Enable Access to:

☑ Azure Virtual Machines for deployment

☑ Azure Resource Manager for template deployment

☑ Azure Disk Encryption for volume encryption

Current Access Policies

Name	Email	Key Permissions
USER		
[redacted]	[redacted]	9 selected

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**

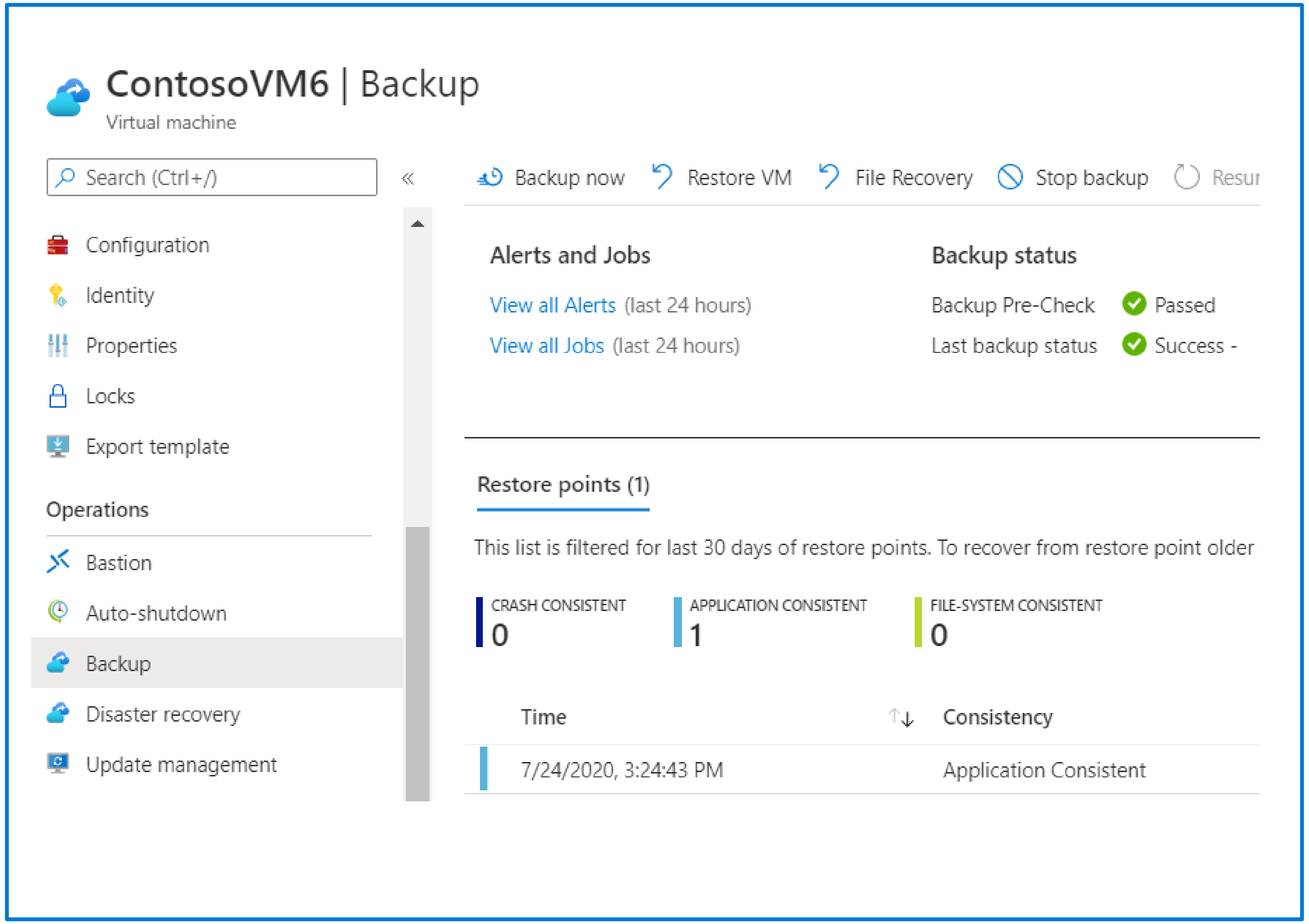
In the **Virtual Machines** section, select **Add**.

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.



Backup status

Backup Pre-Check ✓ Passed

Last backup status ✓ Success -

This list is filtered for last 30 days of restore points. To recover from restore point older

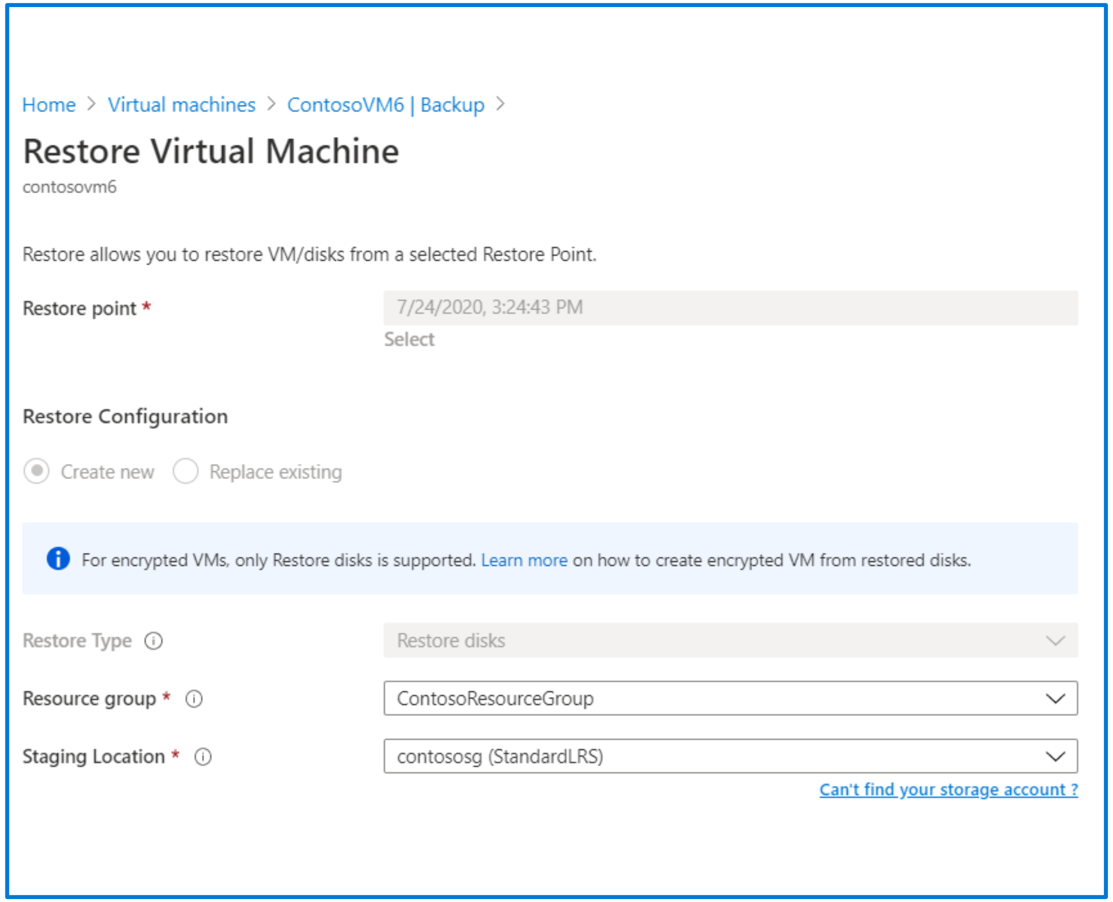
CRASH CONSISTENT	APPLICATION CONSISTENT	FILE-SYSTEM CONSISTENT
0	1	0

Time ↑↓	Consistency
7/24/2020, 3:24:43 PM	Application Consistent

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**.



Restore Virtual Machine

contosovm6

Restore allows you to restore VM/disks from a selected Restore Point.

Restore point * 7/24/2020, 3:24:43 PM

Select

Restore Configuration

● Create new ○ Replace existing

For encrypted VMs, only Restore disks is supported. Learn more on how to create encrypted VM from restored disks.

Restore Type: Restore disks

Resource group *: ContosoResourceGroup

Staging Location *: contososg (StandardLRS)

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

Knowledge Check and Resources – Configure BitLocker disk encryption for Windows IaaS Virtual Machines

Knowledge Check

Microsoft Learn Modules (docs.microsoft.com/Learn)

Configure BitLocker disk encryption for Windows IaaS Virtual Machines

Module 6: Implement change tracking and file integrity monitoring for Windows IaaS VMs

Implement change tracking and file integrity monitoring for Windows IaaS VMs

- 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
- Knowledge check and resources

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

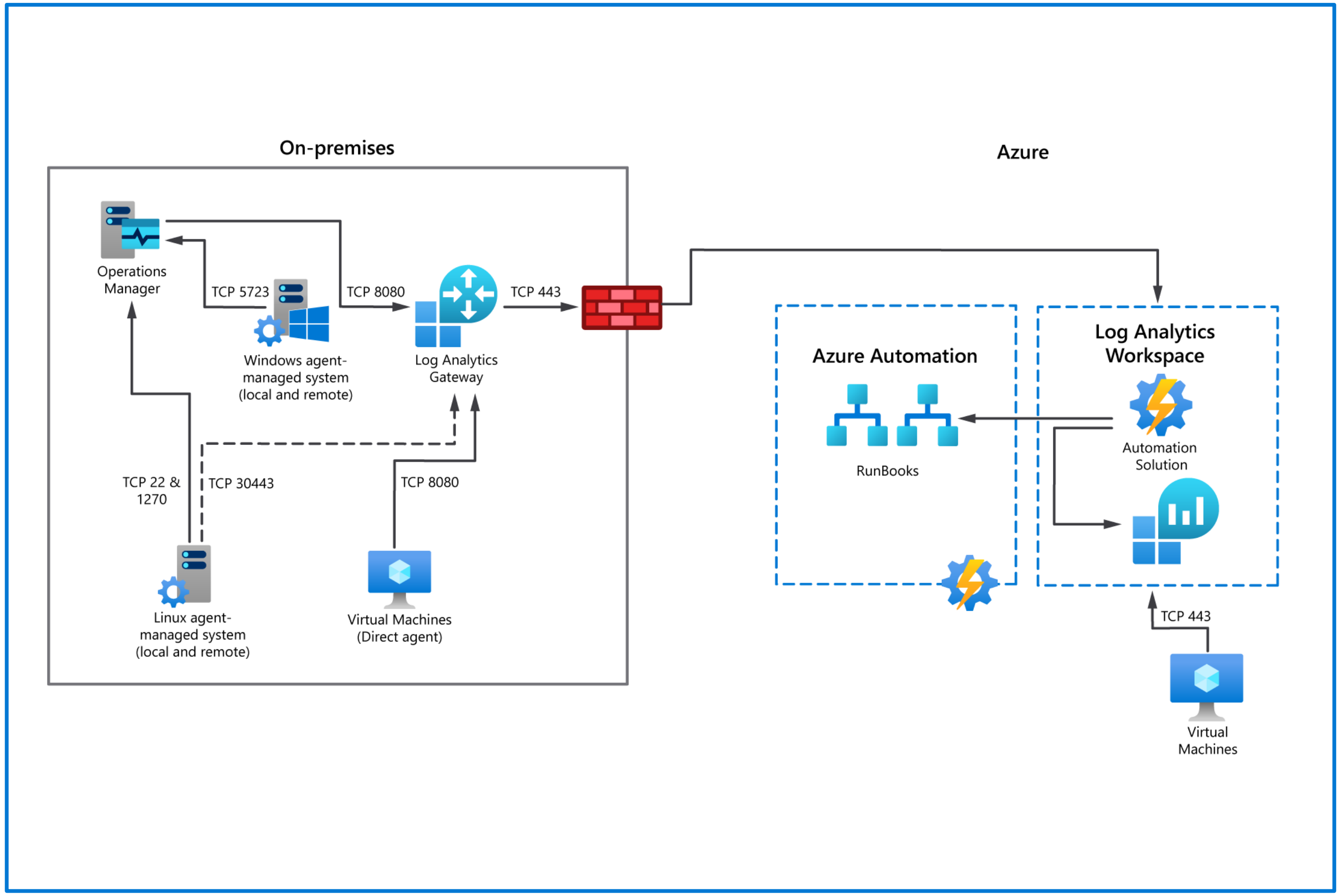
- Only certain regions are supported

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

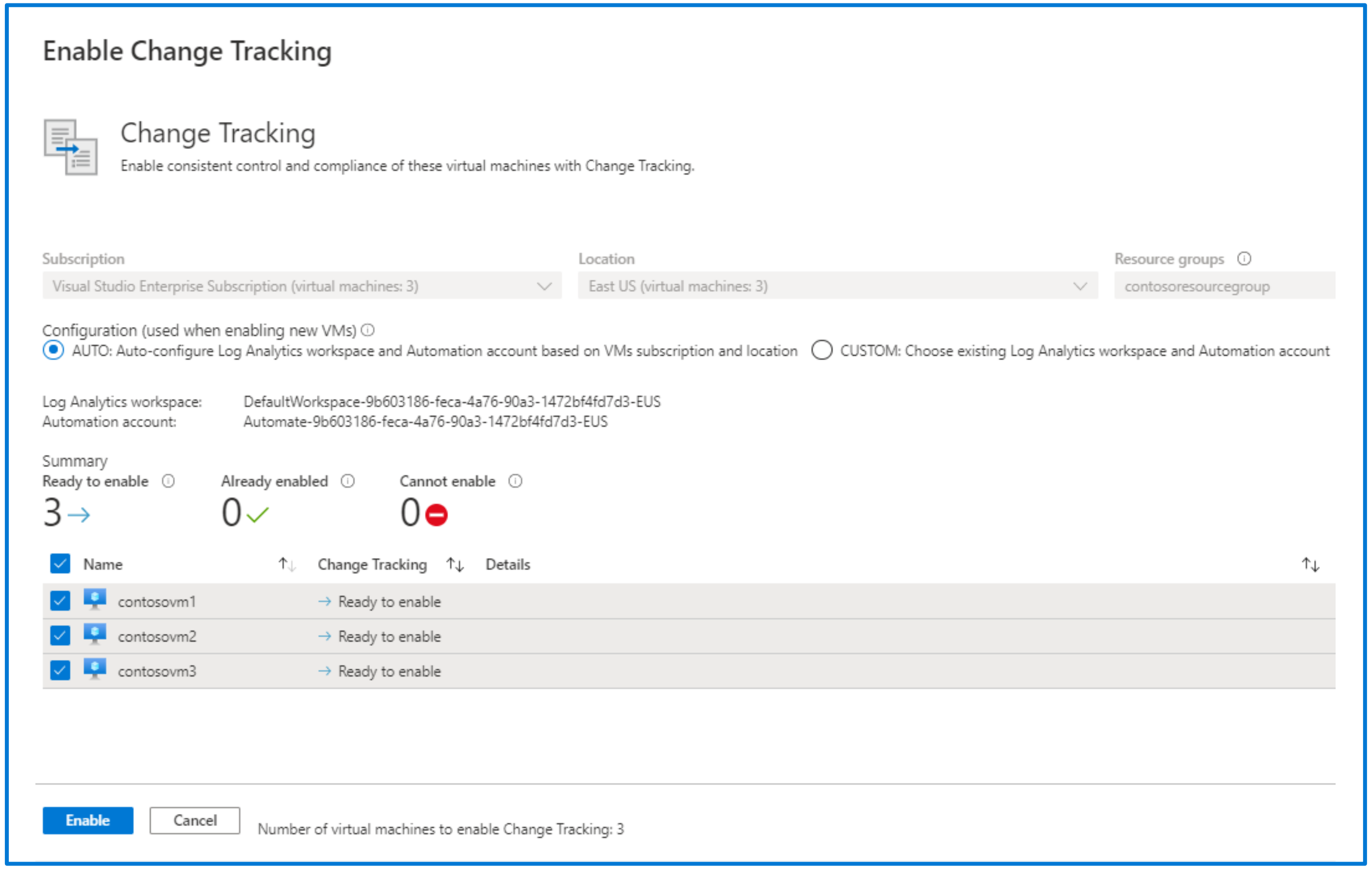


Enable Change Tracking and Inventory

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.



Enable Change Tracking

Change Tracking

Enable consistent control and compliance of these virtual machines with Change Tracking.

Subscription: Visual Studio Enterprise Subscription (virtual machines: 3)

Location: East US (virtual machines: 3)

Resource groups: contosoresourcegroup

Configuration (used when enabling new VMs)

● AUTO: Auto-configure Log Analytics workspace and Automation account based on VMs subscription and location ○ CUSTOM: Choose existing Log Analytics workspace and Automation account

Log Analytics workspace: DefaultWorkspace-9b603186-feca-4a76-90a3-1472bf4fd7d3-EUS
Automation account: Automate-9b603186-feca-4a76-90a3-1472bf4fd7d3-EUS

Summary

Ready to enable	Already enabled	Cannot enable
3 →	0 ✓	0 ⛔

☑	Name	Change Tracking	Details
☑	contosovm1	→ Ready to enable	
☑	contosovm2	→ Ready to enable	
☑	contosovm3	→ Ready to enable	

Number of virtual machines to enable Change Tracking: 3

Manage Change Tracking and Inventory

How to modify Change Tracking and Inventory settings?

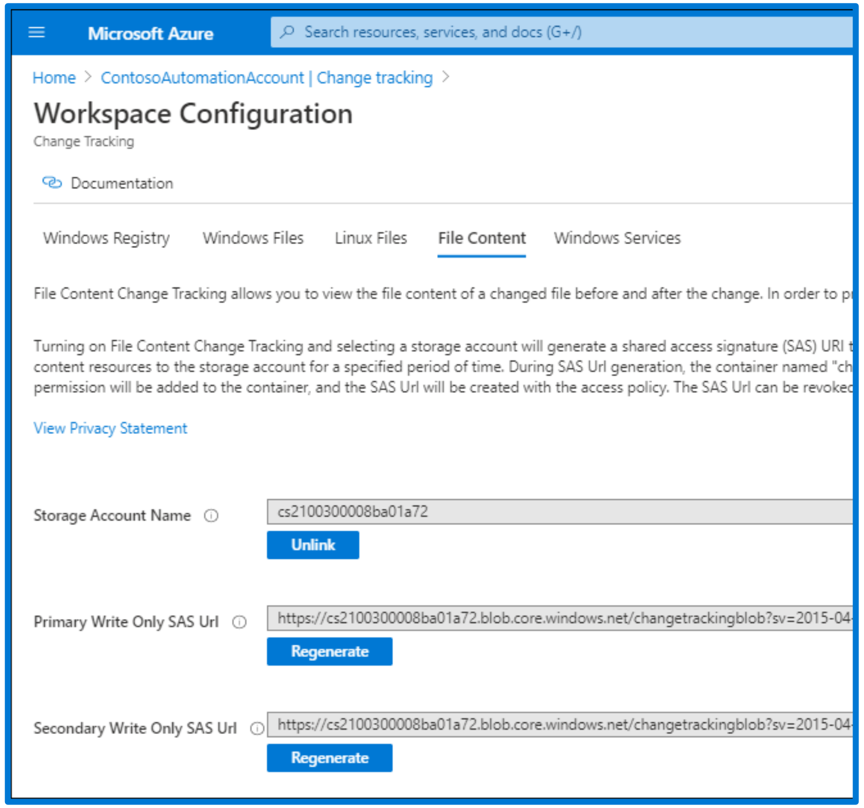
How to track Windows files?

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



Microsoft Azure
Search resources, services, and docs (G+/)
Home > ContosoAutomationAccount | Change tracking >

Workspace Configuration

Change Tracking

File Content Change Tracking allows you to view the file content of a changed file before and after the change. In order to p

Turning on File Content Change Tracking and selecting a storage account will generate a shared access signature (SAS) URI t content resources to the storage account for a specified period of time. During SAS Url generation, the container named "ch permission will be added to the container, and the SAS Url will be created with the access policy. The SAS Url can be revoked

View Privacy Statement

Storage Account Name: cs2100300008ba01a72

Unlink

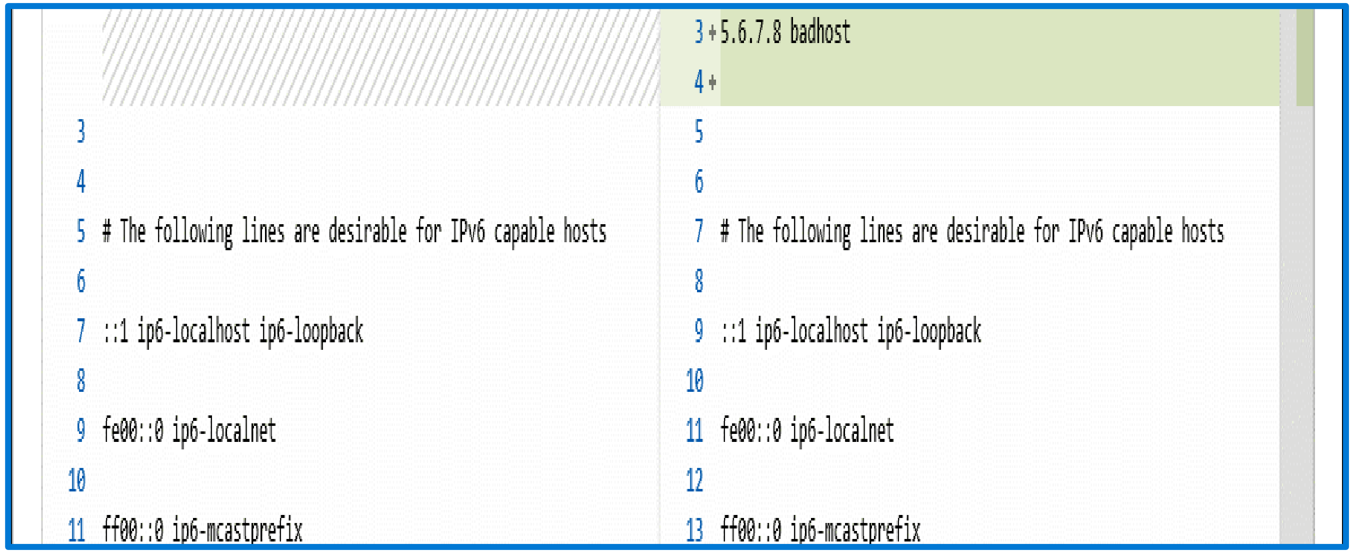
Primary Write Only SAS Url: https://cs2100300008ba01a72.blob.core.windows.net/changetrackingblob?sv=2015-04

Regenerate

Secondary Write Only SAS Url: https://cs2100300008ba01a72.blob.core.windows.net/changetrackingblob?sv=2015-04

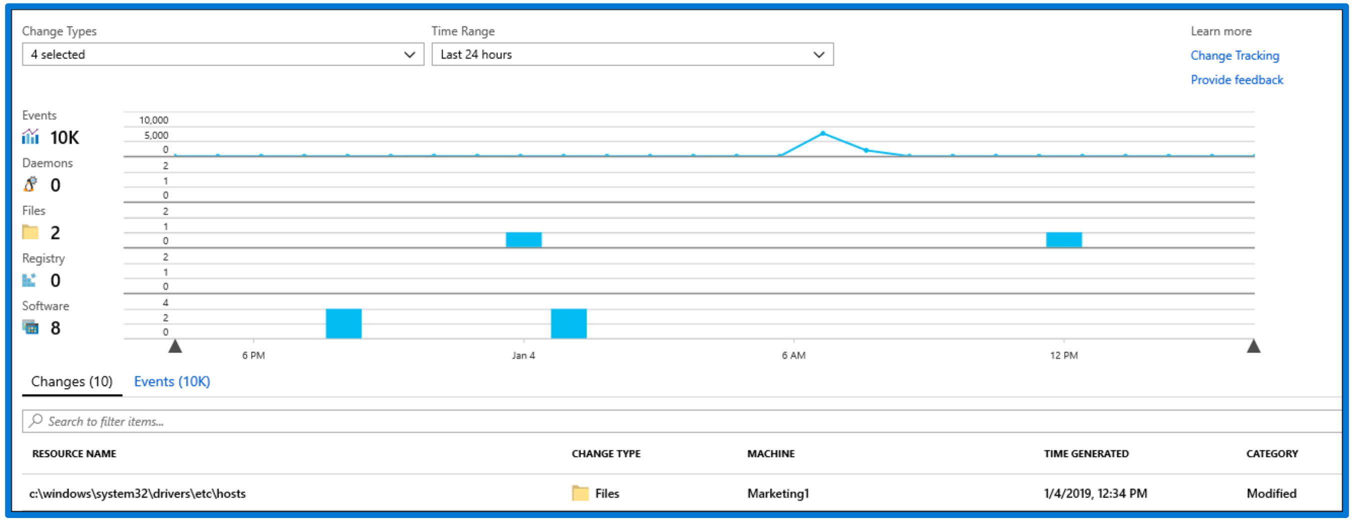
Regenerate

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



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

Events automatically display on the timeline



Change Types: 4 selected

Time Range: Last 24 hours

Learn more

Change Tracking

Provide feedback

RESOURCE NAME	CHANGE TYPE	MACHINE	TIME GENERATED	CATEGORY
c:\windows\system32\drivers\etc\hosts	Files	Marketing1	1/4/2019, 12:34 PM	Modified

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

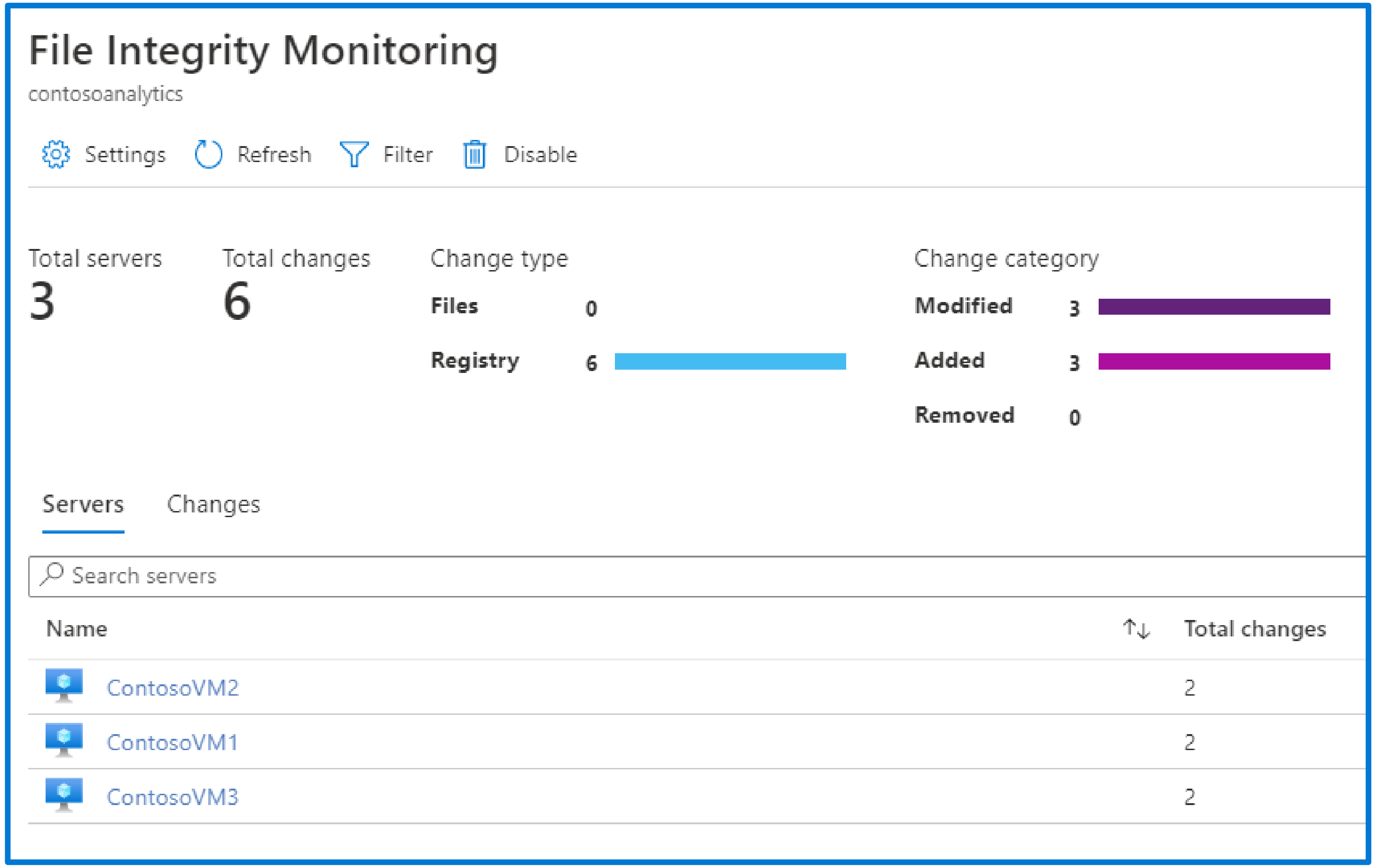
- If you no longer want to use File Integrity Monitoring, you can disable it.

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



File Integrity Monitoring

contosoanalytics

Total servers 3

Total changes 6

Change type	
Files	0
Registry	6

Change category	
Modified	3
Added	3
Removed	0

Name	Total changes
ContosoVM2	2
ContosoVM1	2
ContosoVM3	2

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

Knowledge Check and Resources – Implement change tracking and file integrity monitoring for Windows IaaS VMs

Knowledge Check

Microsoft Learn Modules (docs.microsoft.com/Learn)

Implement change tracking and file integrity monitoring for Windows IaaS VMs

Lab 02

Lab 02 – Using Microsoft Defender for Cloud 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