UNIT 2
Implementing Security Solutions in Hybrid Scenarios

1.0 Learning Outcomes

On completion of the module, you should be able to:

a. **Demonstrate an Azure Log Analytics workspace and an Azure Automation account.**
b. **Describe the Azure Security**

1.1 Introduction

Hybrid cloud security describes the coordinated implementation of tools, processes, and technical know-how that an organization uses to protect its infrastructures, applications, and data across multi-cloud environments (public, private) and on-premises network devices.

The building blocks of hybrid cloud security highlight how demanding it is to safeguard these interconnected resources–and the data that travels between them. From policy design to harmonizing security controls, managing cloud providers, and automating workflows to keep up with business needs, the process can stretch security and IT teams to their limits.

2.1 Implement Windows Server IaaS VM Security

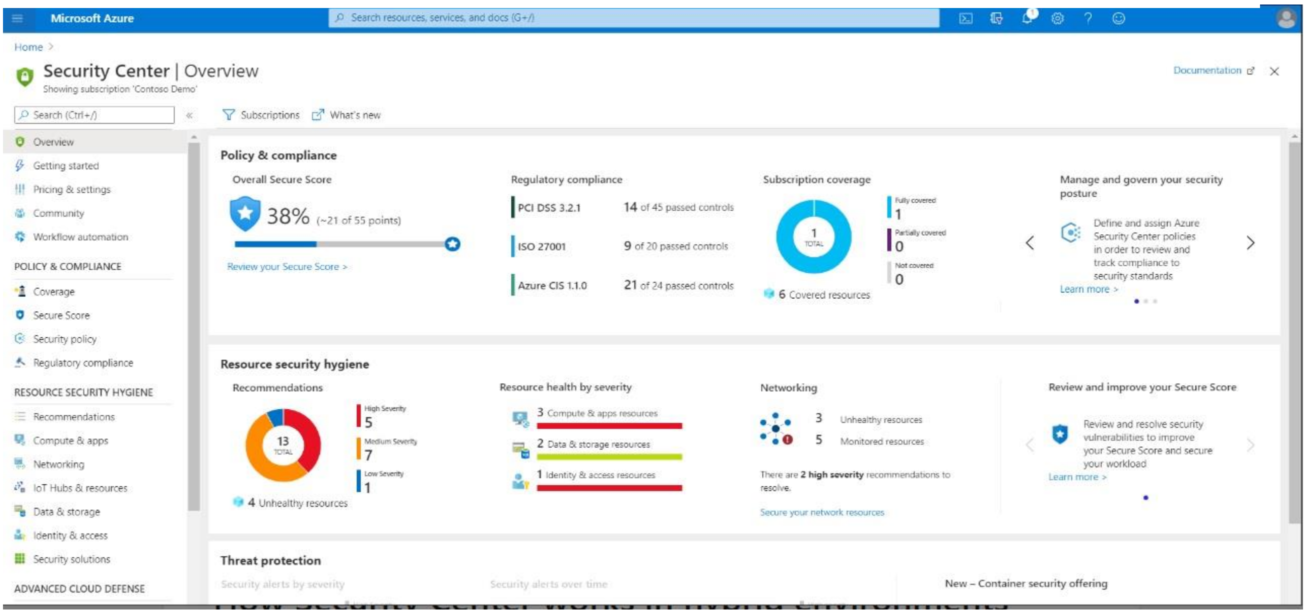
Describe Azure Security Center

Contoso IT personnel requires tools to assess their security posture and detect threats in order to handle the special security problems that a hybrid environment brings, such as quickly changing services, sophisticated assaults, and increased workload. They want to deploy those tools as quickly as possible. They can accomplish all of these goals with the aid of Azure's Security Center.

What is Azure Security Center

A cloud-based tool called Security Center can be used to manage the security of both your on-premises and cloud infrastructure. With the capabilities of Security Center.

- Improve your security position. Use Security Center to implement security best practices across your IaaS, platform as a service (PaaS), data, and on-premises resources. In addition to security best practices, you can also track compliance against regulatory standards.
- Protect your environment. Monitor for security threats to your cloud and on-premises servers, including identifying misconfigurations and providing server Endpoint Detection and Response (EDR) with Microsoft Defender Advanced Threat Protection (ATP).
- Protect your data. Identify suspicious activity such as potential data breaches within your servers, files, databases, data warehouses, and storage accounts. Security Center can also perform automatic data classification in your Azure SQL databases.



Define and assign Azure Security Center policies in order to review and track compliance to security standards

There are 2 high severity recommendations to resolve.

Review and resolve security vulnerabilities to improve your Secure Score and secure your workload

How Security Center works in hybrid environments

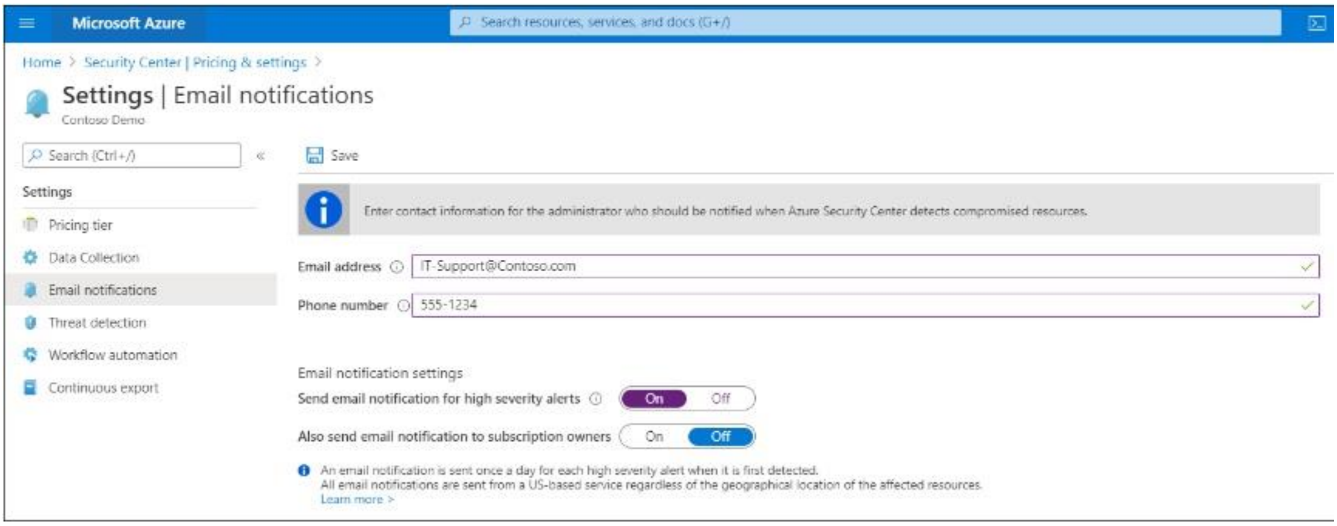
Along with monitoring and securing Azure IaaS, PaaS, and data resources, Security Center also aids in securing servers not hosted by Azure. You can install the Log Analytics agent on your on-premises Windows Server and Linux server VMs as well as non-Azure cloud VMs using the Azure portal. The agent then gathers the information required by Security Center for managing and monitoring those resources.

Events from Windows Event Tracing and event logs are gathered by Security Center from agents. Then it checks native Azure events and configurations related to security. The Log Analytics agent also enables command-line auditing and gathers crash dumps when applications fail. It analyzes various data sources and provides security alerts that may be forwarded to your SIEM system along with a personalized list of hardening actions that it advises you carry out.

Note: In addition to the Log Analytics agent, the Microsoft Defender ATP sensor is automatically enabled on Windows Server computers that are on boarded to Security Center.

Notifications

Providing contact information during Security Center onboarding is one of the initial steps so that Security Center can contact you in the event that it discovers resources that have been hacked. On the Pricing & settings page of Security Center, choose Email notifications, and then input your email address and phone number. Select whether to receive notifications for all users who have the Owner role in the subscription as well as alerts for high-severity occurrences.



Enter contact information for the administrator who should be notified when Azure Security Center detects compromised resources.

Email address: IT-Support@Contoso.com ✓

Phone number: 555-1234 ✓

Email notification settings

Send email notification for high severity alerts: [✓ On] Off

Also send email notification to subscription owners: On [✓ Off]

An email notification is sent once a day for each high severity alert when it is first detected.
All email notifications are sent from a US-based service regardless of the geographical location of the affected resources.
Learn more >

Security Center feature coverage for VMs

Some of the many functions offered by Security Center are available for Azure VMs and PaaS services as part of the Free service tier, while others are only offered as part of the Standard tier.

The following list are some of the common Security Center features:

- Microsoft Intune Endpoint Protection assessment
- Missing operating system patches assessment
- Security misconfigurations assessment
- Disk encryption assessment
- Network security assessment
- Third-party vulnerability assessment
- VM behavioral analytics and security alerts
- Adaptive application controls
- File integrity monitoring
- Fileless security alerts
- Defender ATP
- Regulatory compliance dashboard and reports

- Adaptive network controls
- Adaptive network hardening
- Just-in-time (JIT) VM access
- Native vulnerability assessment
- Network map
- Network-based security alerts

Enable Azure Security Center in hybrid environments

IT staff at Contoso want to use Security Center to help secure their VM workloads and their on-premises servers. To onboard their VMs and on-premises servers to Security Center, they must complete the following tasks.

- Enable the Standard pricing tier
- Enable automatic provisioning
- Onboard their VMs and servers

Audit the security of Windows Server IaaS Virtual Machines

You'll learn about Azure Security Center and how to onboard Windows Server computers to Security Center. You'll also learn about Azure Sentinel, security information and event management (SIEM), and security orchestration, automation and response (SOAR).

You can use the Azure Security Center to assess the security configuration of your Azure VM resources and the Windows Server operating system (OS) that's running on the VM.

Contoso is a medium-sized financial services provider with headquarters in London and a location in New York. Windows Server is used for the majority of its on-premises compute environment. Workloads that are virtualized on Windows Server 2012 R2 machines are included. The Windows Server 2019 migration of Contoso servers is now being carried out by Contoso IT personnel.

Contoso's IT director is aware that the company relies on antiquated technology and has an outmoded operational model with no automation. The Contoso IT Engineering team has begun investigating Azure's features. They want to know if using automation and virtualization with Azure services could help update the operating model as it is today.

The Contoso IT team requested that you, as their lead system engineer and server administrator, set up a proof of concept environment as part of the initial design. The ability of Azure services to achieve business objectives and update the IT infrastructure must be tested in this context.

The Contoso IT team places a high priority on protecting VM resources both on-premises and in Azure. You will discover more about Azure Security Center and how to use it in hybrid environments in this module. You'll discover how to add Windows Server machines to Security Center and how to use it to safeguard your resources. Additionally, you'll learn about Azure Sentinel, security orchestration, automation, and response (SOAR), and security information and event management (SIEM).

Describe Azure Security Center

To address the unique security challenges that a hybrid environment presents, such as rapidly changing services, sophisticated attacks, and increased workload, Contoso IT staff need tools to help assess their security posture and identify risks. Ideally, they want to deploy those tools with minimal effort. Azure's Security Center can help them meet all these requirements.

What is Azure Security Center

Security Center is a cloud-based tool for managing the security of your cloud and on-premises infrastructure. With Security Center capabilities, you can:

- Improve your security position. Use Security Center to implement security best practices across your IaaS, platform as a service (PaaS), data, and on-premises resources. In addition to security best practices, you can also track compliance against regulatory standards.
- Protect your environment. Monitor for security threats to your cloud and on-premises servers, including identifying misconfigurations and providing server Endpoint Detection and Response (EDR) with Microsoft Defender Advanced Threat Protection (ATP).
- Protect your data. Identify suspicious activity such as potential data breaches within your servers, files, databases, data warehouses, and storage accounts. Security Center can also perform automatic data classification in your Azure SQL databases.

Manage Azure updates

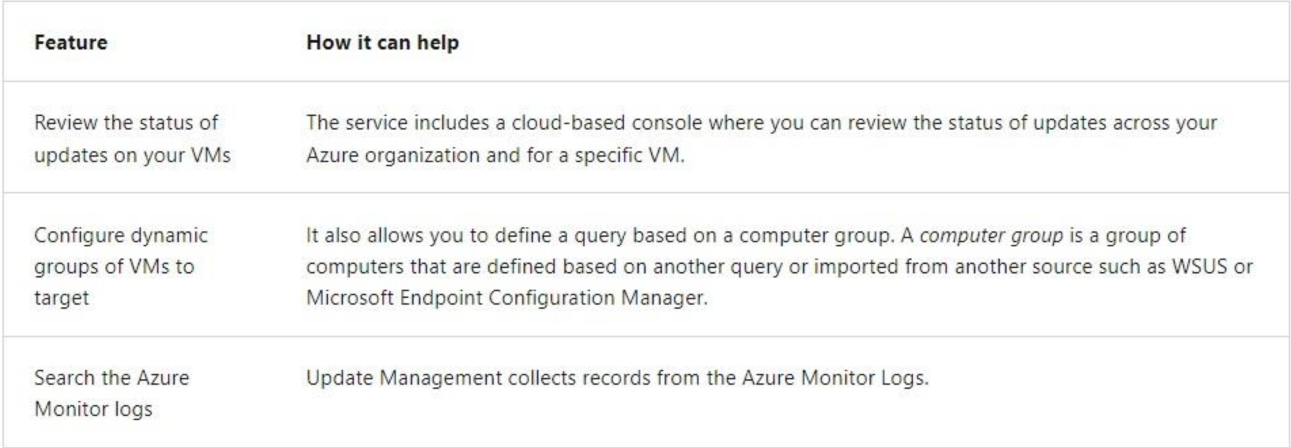
Updates to Windows are, of course, a recurring series of events. Updates can come quickly and frequently when newly discovered security flaws or attack vectors are addressed. Updates also arrive periodically based on events such as changes in device drivers or planned roll-outs of new system features.

Contoso IT support staff realize that there is no set time that an urgent security update might become available, and it's imperative in many cases to deploy such an update as soon as possible. This approach applies whether the system is a physical host, an on-premises VM, or an Azure VM. They must be vigilant when reviewing Windows Updates to their Azure VMs.

Azure Automation and Update Management

Azure Automation helps you manage OS updates for Azure VMs running the Windows operating system. The Update Management feature is free, and the only cost is the cost of log storage in Azure Log Analytics.

The following table describes how Update Management features can help with updates for your 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.

To implement Azure Update Management in your hybrid environment, you must complete the following high-level steps:

1. Create an Azure Automation account.
2. Enable Update Management.
3. Onboard your on-premises servers.
4. Select the machines to manage.
5. Schedule updates

Interaction with Windows Update

Azure Automation Update Management relies on the Windows Update client to download and install Windows updates. There are specific settings that are used by the Windows Update client when connecting to WSUS or Windows Update. You can manage many of these settings by:

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

Create and implement application allow lists with adaptive application control

Describe adaptive application control

Adaptive application control can help Contoso IT operations staff determine which applications are allowed to run on their Azure (and non-Azure) VMs. Being able to control applications in this way can help harden their VMs against malware.

What is adaptive application Control

Adaptive application control uses machine learning to analyze the applications running on your VMs. You configure and manage adaptive application controls in Security Center. Once enabled, the Adaptive application controls feature creates an allow list from its machine-learning analysis.

Using Adaptive application controls can help simplify the process of configuring and maintaining application policies. By using Adaptive application controls, you can:

- Block attempts to run potentially malicious applications.
- Receive alerts when adaptive application control blocks an application.

  Note

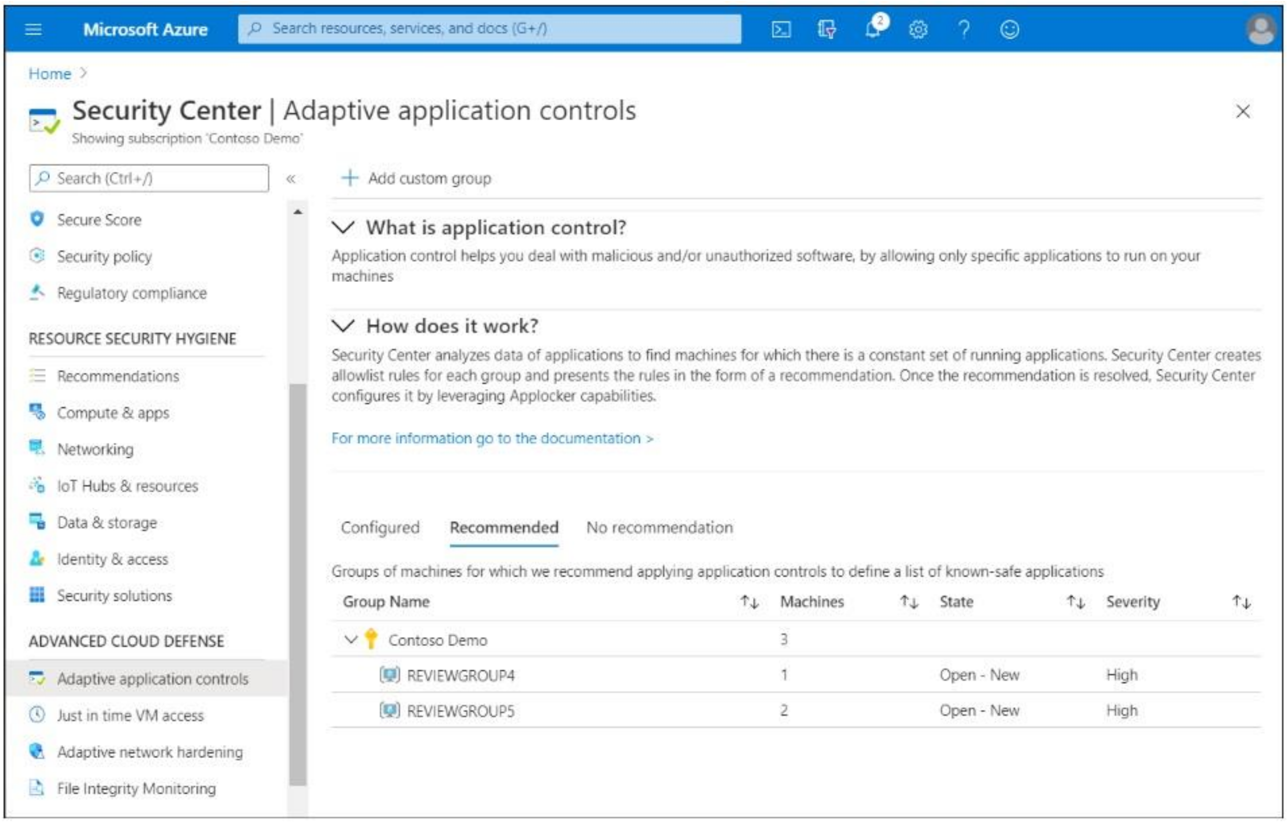
  These blocks and alerts might be generated by attempts to run applications that could otherwise be missed by antimalware solutions.

- 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.

Enable adaptive application control

To implement adaptive application control, you must use Security Center. Use the following procedure to begin the process of implementing adaptive application control:

1. In the Azure portal, open **Security Center**.
2. In the navigation pane, in the **ADVANCED CLOUD DEFENSE** section, select **Adaptive application controls**.
3. In the **Adaptive application controls** blade, expand **How does it work !**



Security Center | Adaptive application controls

Showing subscription 'Contoso Demo'

What is application control?

Application control helps you deal with malicious and/or unauthorized software, by allowing only specific applications to run on your machines

How does it work?

Security Center analyzes data of applications to find machines for which there is a constant set of running applications. Security Center creates allowlist rules for each group and presents the rules in the form of a recommendation. Once the recommendation is resolved, Security Center configures it by leveraging Applocker capabilities.

For more information go to the documentation >

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

Within *How does it work* are three tabs: Configured, Recommended, **and** No recommendation**. These are described in the following table:**

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.

Configure BitLocker disk encryption for Windows IaaS Virtual Machines

Describe Azure Disk Encryption and server-side encryption

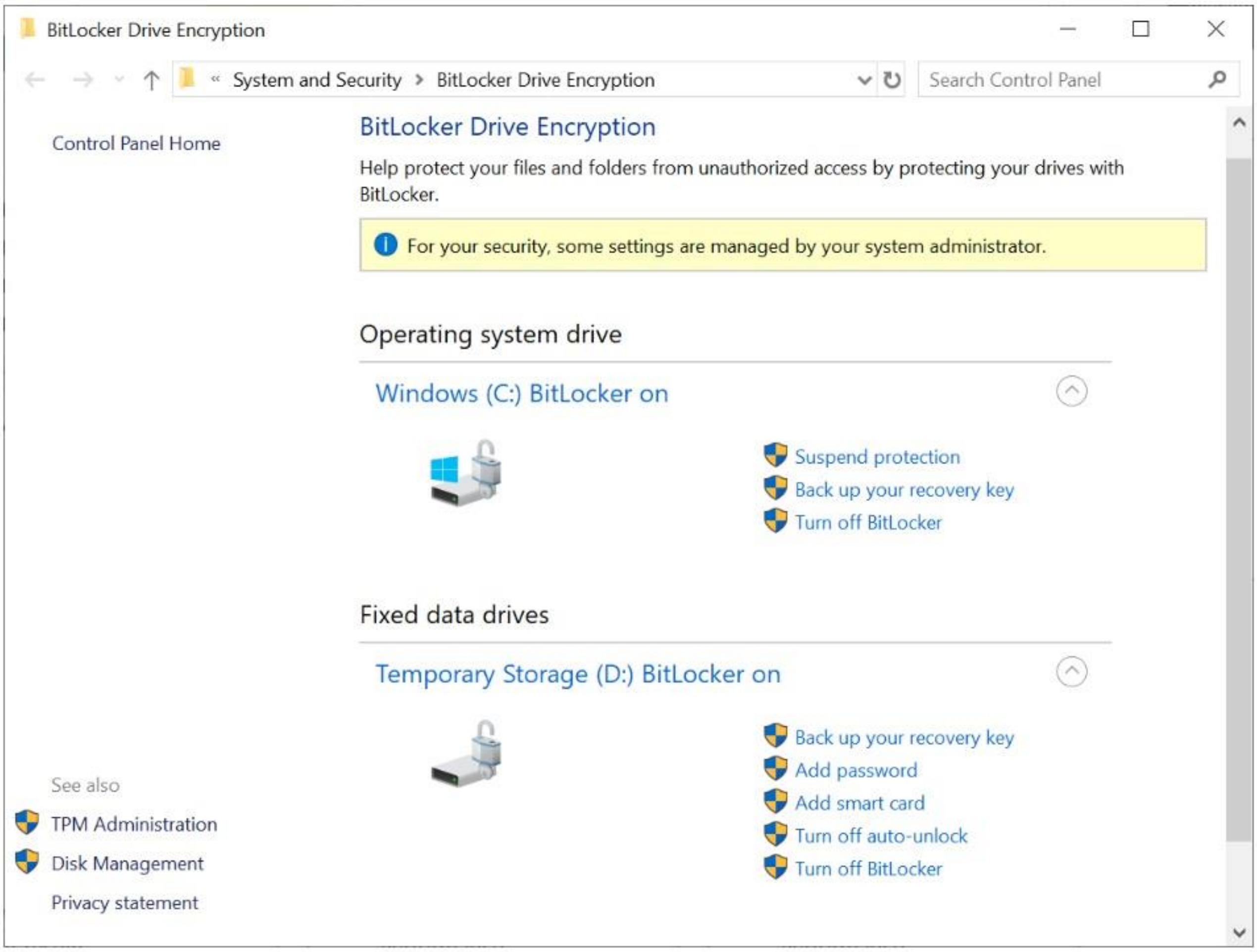
In the context of Azure VMs, storage-level security is provided through encryption of the VMs' virtual disk files. When considering options to enable storage-level security, in general, there are two primary mechanisms that the Contoso IT security team needs to research:

- Azure Disk Encryption
- Server-side encryption of Azure Managed Disks

What is Azure Disk Encryption?

Azure Disk Encryption is a capability built into the Azure platform that enables you to encrypt file system volumes residing on Windows and Linux Azure VM disks. Azure Disk Encryption uses existing file system–based encryption technologies:

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



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

Suspend protection

Back up your recovery key

Turn off BitLocker

Fixed data drives

Temporary Storage (D:) BitLocker on

Back up your recovery key

Add password

Add smart card

Turn off auto-unlock

Turn off BitLocker

See also

TPM Administration

Disk Management

Privacy statement

Azure Disk Encryption uses these technologies to provide encryption of volumes hosting the operating system and data.

Caution

Although you can review BitLocker settings in Windows, notice the warning message in the screenshot: *For your security, some settings are managed by your system administrator.* Therefore, you shouldn't reconfigure BitLocker settings directly within a VM.

Note:

Key Vault stores the cryptographic keys that BitLocker uses.

Key Vault maintains its content in an encrypted form. To provide additional layers of security, you have the option to encrypt the volume encryption keys as well, by utilizing Key Vault's key encryption key functionality.

Azure Disk Encryption can automatically encrypt:

- The operating system disk
- Data disks
- The temporary disk

It also supports both managed and unmanaged disks.

You can use Azure Disk Encryption in three scenarios:

- Enabling encryption on new Azure VMs that were created from Azure Marketplace images
- Enabling encryption on existing Azure VMs that are already running in Azure
- Enabling encryption on new Azure VMs created from a customer-encrypted .vhd file by using existing encryption keys

Azure Disk Encryption requires additional steps to provide the Azure platform with access to the key vault where secrets and encryption keys will reside. In particular, you must enable the access policy setting **Enable Access to Azure Disk Encryption for volume encryption** for the vault.

When applying encryption to a new VM, you must:

1. Configure the vault access policy to enable the Microsoft. Compute resource provider and Azure Resource Manager to retrieve its secrets during VM deployments.

Note:

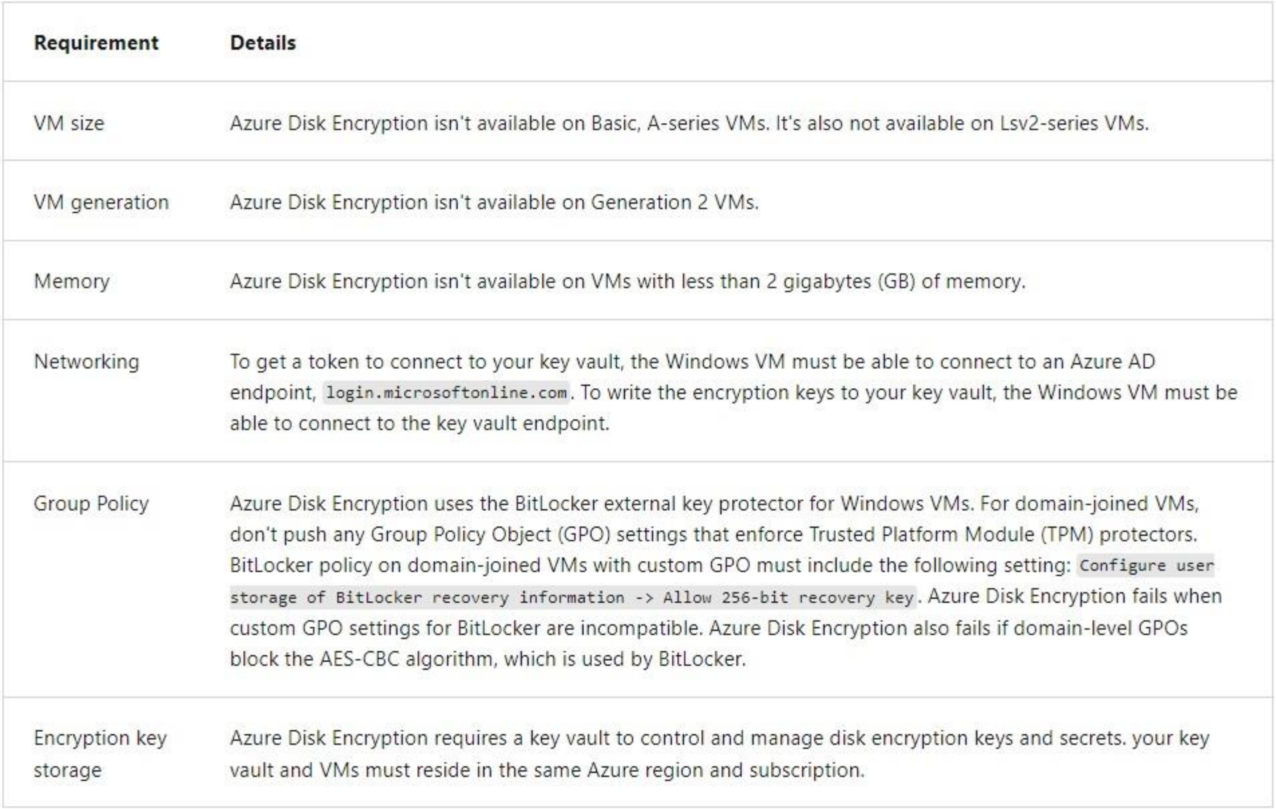
This step only applies when you plan to deploy VMs using Resource Manager templates.

2. Enable encryption on new or existing Resource Manager VMs. Details of this step depend on which of the three scenarios you're implementing and which deployment methodology you're using.

Requirements

To implement Azure Disk Encryption, your environment must meet certain requirements. These include operating system, VM generation, networking, and Group Policy requirements, in addition to certain SKU requirements.

The requirements for Azure Disk Encryption are described in the following table.



Requirement	Details
VM size	Azure Disk Encryption isn't available on Basic, A-series VMs. It's also not available on Lsv2-series VMs.
VM generation	Azure Disk Encryption isn't available on Generation 2 VMs.
Memory	Azure Disk Encryption isn't available on VMs with less than 2 gigabytes (GB) of memory.
Networking	To get a token to connect to your key vault, the Windows VM must be able to connect to an Azure AD endpoint, `login.microsoftonline.com`. To write the encryption keys to your key vault, the Windows VM must be able to connect to the key vault endpoint.
Group Policy	Azure Disk Encryption uses the BitLocker external key protector for Windows VMs. For domain-joined VMs, don't push any Group Policy Object (GPO) settings that enforce Trusted Platform Module (TPM) protectors. BitLocker policy on domain-joined VMs with custom GPO must include the following setting: `Configure user storage of BitLocker recovery information -> Allow 256-bit recovery key`. Azure Disk Encryption fails when custom GPO settings for BitLocker are incompatible. Azure Disk Encryption also fails if domain-level GPOs block the AES-CBC algorithm, which is used by BitLocker.
Encryption key storage	Azure Disk Encryption requires a key vault to control and manage disk encryption keys and secrets. your key vault and VMs must reside in the same Azure region and subscription.

What is server-side encryption of Azure-managed disks

By using platform-managed encryption keys, server-side encryption of Azure-managed disks automatically applies encryption to:

- All managed disks
- Managed disk snapshots
- Managed images

Note:

Unlike Azure Disk Encryption, server-side encryption doesn't apply to a temporary disk and doesn't provide support for unmanaged disks.

However, server-side encryption supports Generation 2 Azure VMs and all existing Azure VM sizes. Effectively, all Azure VM–managed disks are automatically protected, even if Azure Disk Encryption isn't being used.

Note:

If you decide to implement Azure-managed disks with your own keys rather than using the platform-provided keys, server-side encryption of Azure managed disks will be incompatible with Azure Disk Encryption.

As previously mentioned, server-side encryption of Azure-managed disks is automatic. If you want to implement it with your own keys, you have to add the keys to a key vault that's in the same region and the same Azure subscription where the Azure VM disks reside. You also have to create a Disk Encryption Set resource that references the keys in the key vault, and then point to the Disk Encryption Set when deploying the Azure VM with managed disks or when configuring encryption of a managed disk.

Implement change tracking and file integrity monitoring for Windows IaaS VMs

Implement Change Tracking and Inventory

Any VMs that you deploy as part of Contoso's Azure subscription need to be secure. You can use the Change Tracking and Inventory feature, part of Azure Automation, to help secure Contoso's Windows Server IaaS VMs **in Azure**.

What is Change Tracking and Inventory

Azure Change Tracking and Inventory is a feature that enables you to track changes in both your VMs and your server infrastructure. This can help you to pinpoint operational and environmental issues with software managed by the Distribution Package Manager. You can track the following Windows Server items using Change Tracking and Inventory:

- Windows software
- Windows files

- Windows registry keys
- Microsoft services

In addition, you can track the following Linux components:

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

Azure Tracking and Inventory relies on Log Analytics to collect information on monitoring components to a Log Analytics workspace. If you connect your VMs to a Log Analytics workspace, on monitored servers, you can use Log Analytics agents to collect data about changes to:

- Installed software
- Microsoft services
- Windows registry and files

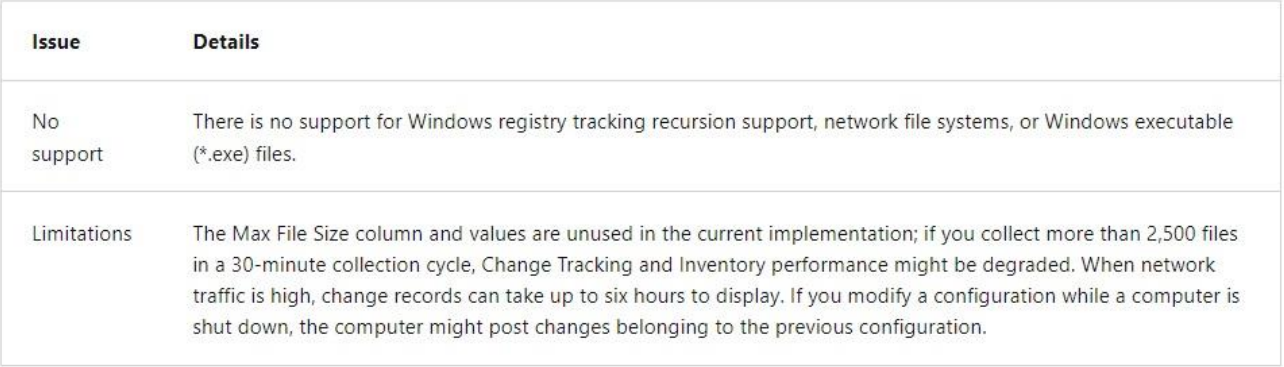
The Log Analytics agents send collected data to Azure Monitor for processing. Azure Monitor then applies logic to the that data, records the data and makes it available to you.

Note:

Change Tracking and Inventory obtains its data from **Azure Monitor**.

Limitations:

Change Tracking and Inventory doesn't support certain items and has some limitations, as detailed in the following table.

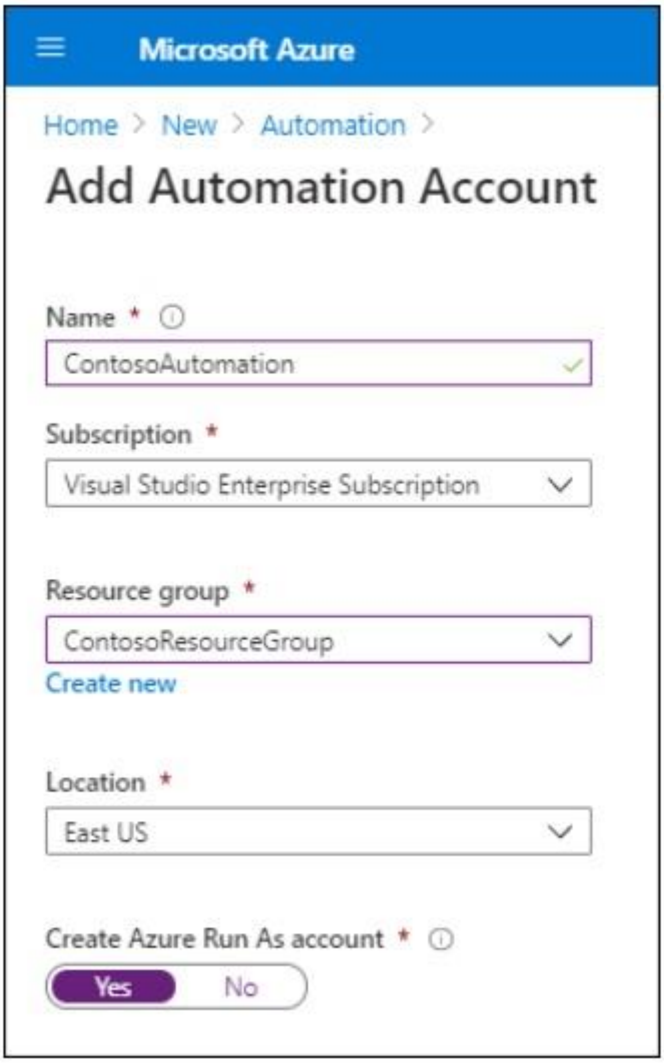


Issue	Details
No support	There is no support for Windows registry tracking recursion support, network file systems, or Windows executable (*.exe) files.
Limitations	The Max File Size column and values are unused in the current implementation; if you collect more than 2,500 files in a 30-minute collection cycle, Change Tracking and Inventory performance might be degraded. When network traffic is high, change records can take up to six hours to display. If you modify a configuration while a computer is shut down, the computer might post changes belonging to the previous configuration.

Requirements for Change Tracking and Inventory

Automation account

Change Tracking and Inventory relies on Azure Automation. When you start Azure Automation for the first time, you must create an Automation account. The Automation account enables you to isolate your Automation resources and related items from the resources relating to other accounts. An Azure Automation account is different from both your Microsoft account and any accounts you create in your Azure subscription. you create an Azure Automation account in the Azure portal, **Azure Automation account** blade.



Add Automation Account

Name * ContosoAutomation

Subscription * Visual Studio Enterprise Subscription

Resource group * ContosoResourceGroup

Location * East US

Create Azure Run As account * [✓ Yes] No

To learn how to create an Automation account, visit Create an Azure Automation account.

Supported operating systems

Change Tracking and Inventory supports all Windows OSs that meet the Log Analytics agent requirements. These operating systems are:

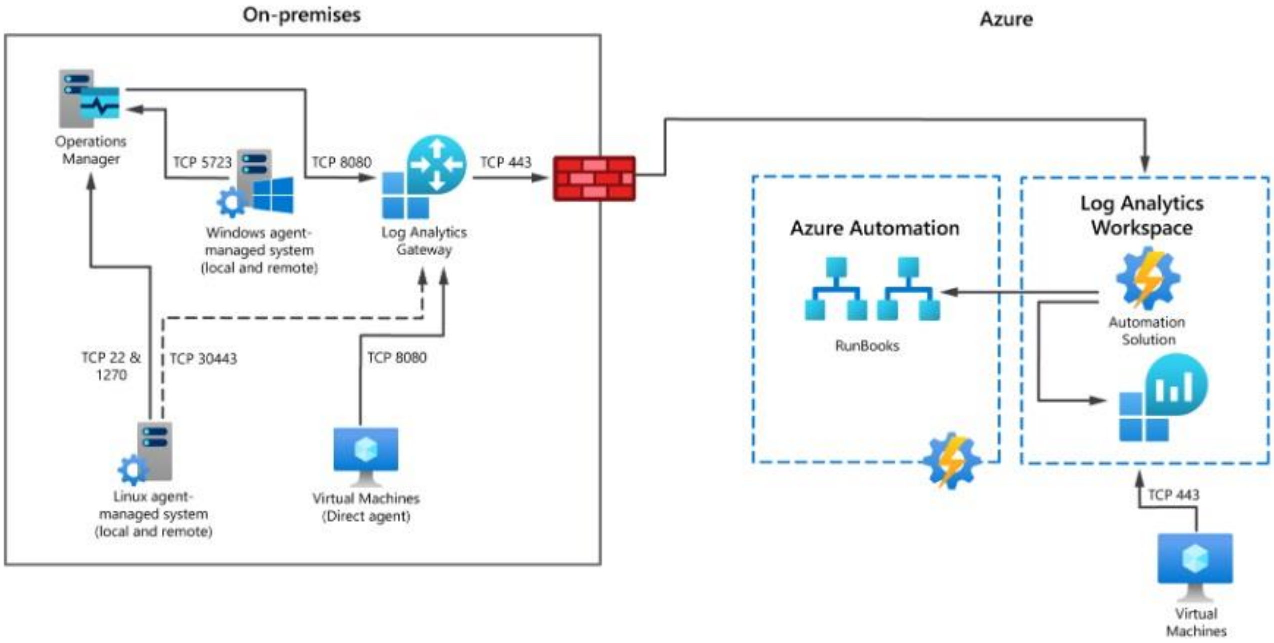
- Windows Server 2019
- Windows Server 2016, version 1709 and 1803
- Windows Server 2012 and Windows Server 2012 R2
- Windows 10 Enterprise (including multi-session) and Windows 10 Pro
- Windows 8.1 Enterprise and Windows 8.1 Pro

Note:

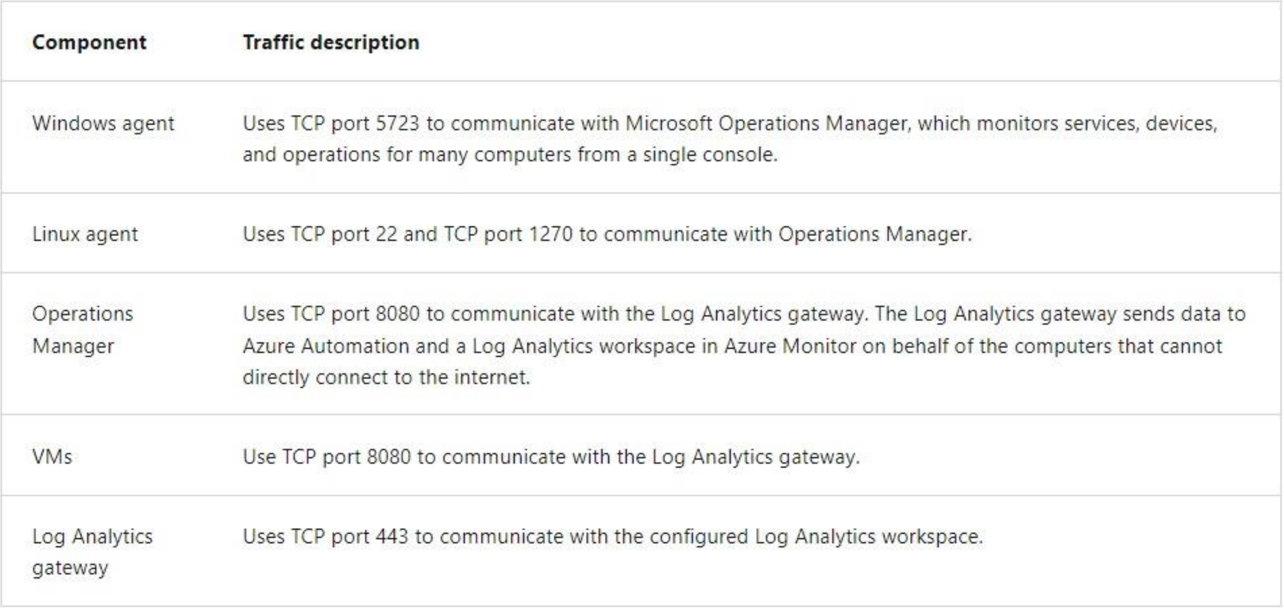
Change Tracking and Inventory is also supported on a number of Linux operating systems.

Network requirements

Change Tracking and Inventory also has a number of network requirements based on the requirements of both the underlying Log Analytics workspace and Linux and Windows agents. The agent communicates with the Azure Monitor service using TCP port 443. If the monitored server connects through a firewall or proxy server, you must ensure that your configuration matches that displayed in the following diagram.



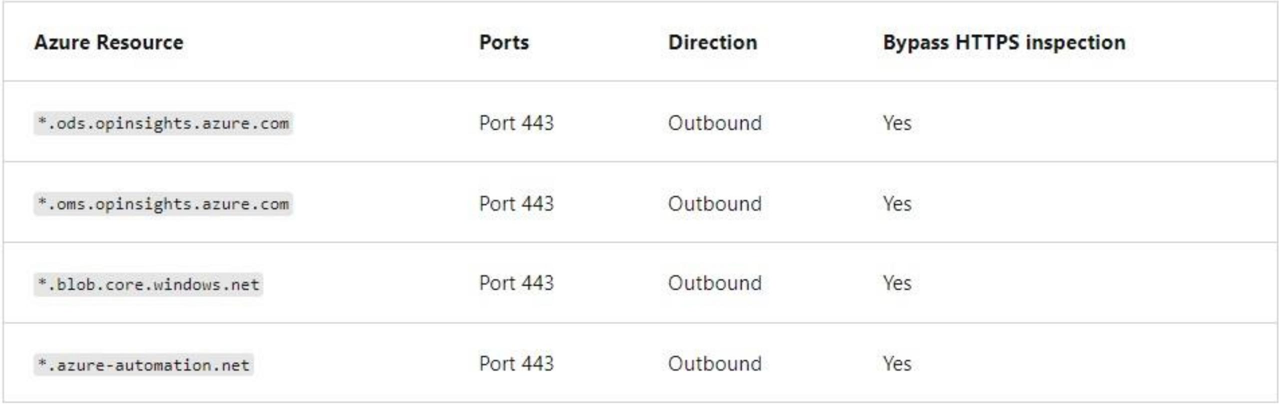
Typical settings for on-premises servers being monitored are described in the following table.



Component	Traffic description
Windows agent	Uses TCP port 5723 to communicate with Microsoft Operations Manager, which monitors services, devices, and operations for many computers from a single console.
Linux agent	Uses TCP port 22 and TCP port 1270 to communicate with Operations Manager.
Operations Manager	Uses TCP port 8080 to communicate with the Log Analytics gateway. The Log Analytics gateway sends data to Azure Automation and a Log Analytics workspace in Azure Monitor on behalf of the computers that cannot directly connect to the internet.
VMs	Use TCP port 8080 to communicate with the Log Analytics gateway.
Log Analytics gateway	Uses TCP port 443 to communicate with the configured Log Analytics workspace.

Firewall requirements

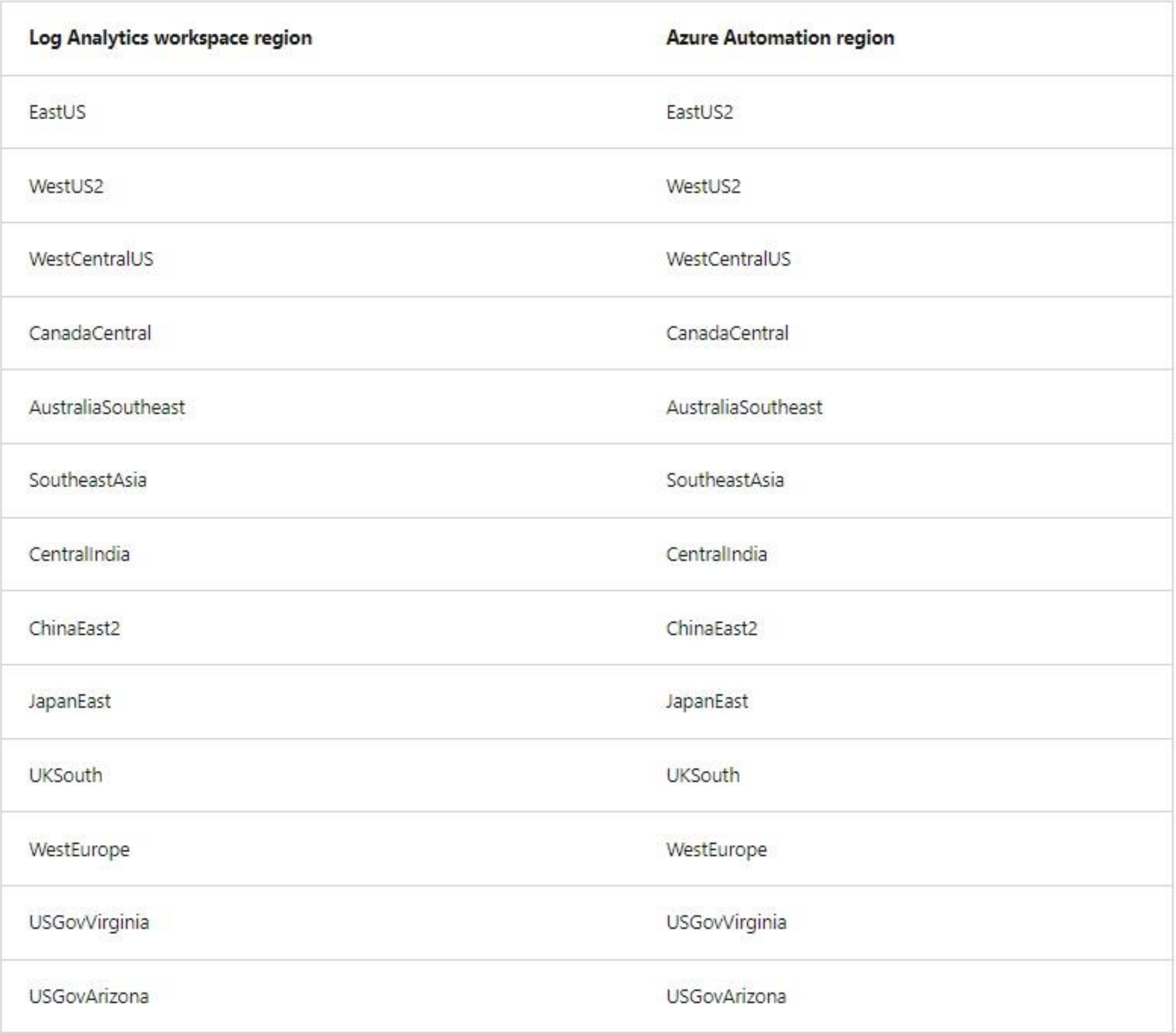
Change Tracking and Inventory requires access through your firewall to certain resources as outlined in the following table.



Azure Resource	Ports	Direction	Bypass HTTPS inspection
`*.ods.opinsights.azure.com`	Port 443	Outbound	Yes
`*.oms.opinsights.azure.com`	Port 443	Outbound	Yes
`*.blob.core.windows.net`	Port 443	Outbound	Yes
`*.azure-automation.net`	Port 443	Outbound	Yes

Azure region requirements

You must link Change Tracking and Inventory to a Log Analytics workspace and an Automation account in your Azure subscription. However, only certain regions are supported for these links, as described in the following table.



Log Analytics workspace region	Azure Automation region
EastUS	EastUS2
WestUS2	WestUS2
WestCentralUS	WestCentralUS
CanadaCentral	CanadaCentral
AustraliaSoutheast	AustraliaSoutheast
SoutheastAsia	SoutheastAsia
CentralIndia	CentralIndia
ChinaEast2	ChinaEast2
JapanEast	JapanEast
UKSouth	UKSouth
WestEurope	WestEurope
USGovVirginia	USGovVirginia
USGovArizona	USGovArizona

Tip:

Your Log Analytics workspace and Automation account must be in the same subscription as one another.

Enable Change Tracking and Inventory

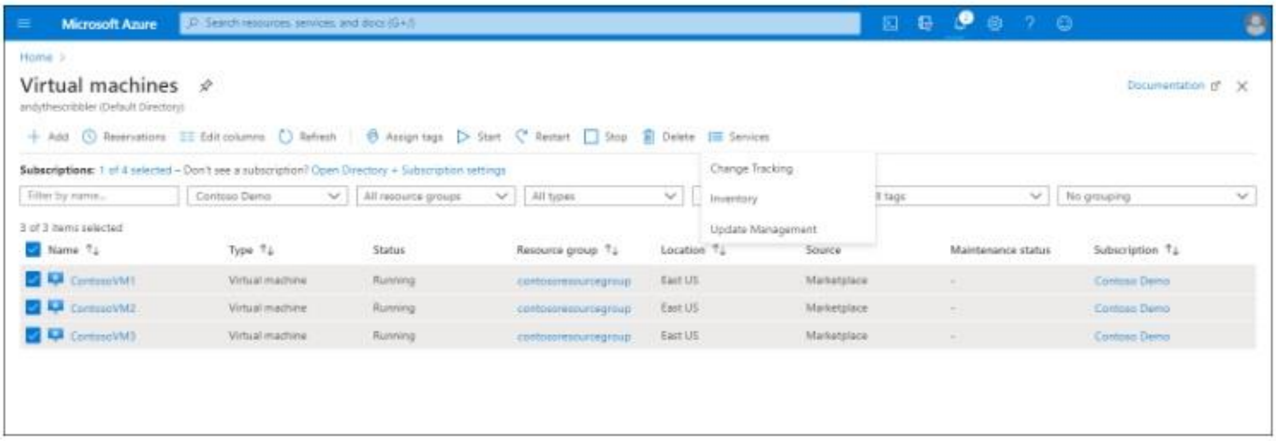
You can enable Change Tracking and Inventory in a number of ways:

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

Enable Change Tracking and Inventory from the Azure portal

Use the following high-level procedure to enable Change Tracking and Inventory using the Azure portal:

1. In the Azure portal, navigate to **Virtual machines**.
2. Use the checkboxes to choose the virtual machines to add to Change Tracking and Inventory.
3. Select **Services**, and then select **Change Tracking** or **Inventory**.



Subscriptions: 1 of 4 selected – Don't see a subscription? Open Directory + Subscription settings

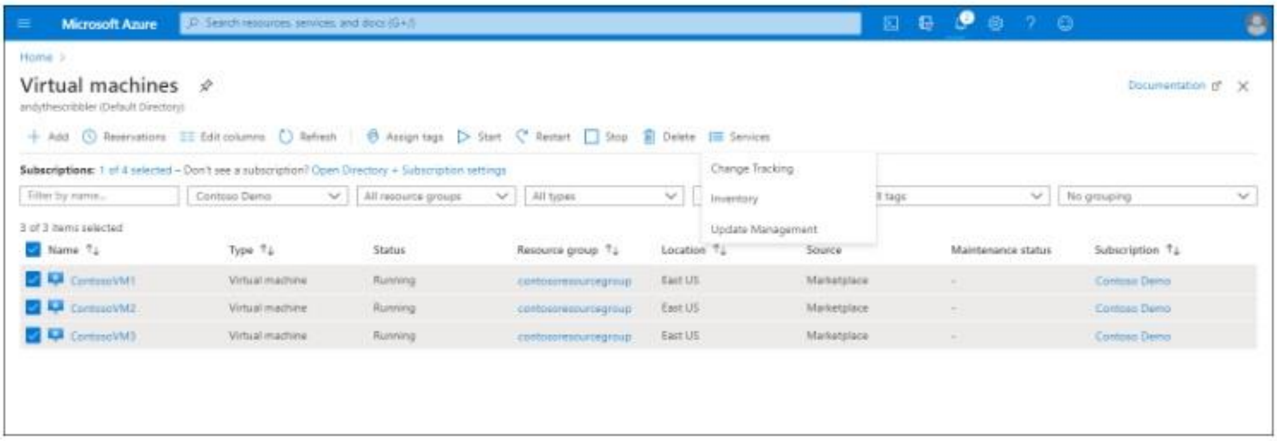
3 of 3 items selected

☑ Name	Type	Status	Resource group	Location	Source	Maintenance status	Subscription
☑ ContosoVM1	Virtual machine	Running	contosoresourcegroup	East US	Marketplace	-	Contoso Demo
☑ ContosoVM2	Virtual machine	Running	contosoresourcegroup	East US	Marketplace	-	Contoso Demo
☑ ContosoVM3	Virtual machine	Running	contosoresourcegroup	East US	Marketplace	-	Contoso Demo

1. Azure filters the list of VMs to list only the VMs that are in the same subscription and location. You can change this behavior.
2. Azure selects an existing Log Analytics workspace and Automation account (if available). If you want to use a different Log Analytics workspace and Automation account, select **CUSTOM** to select them from the Custom Configuration page.
3. Select **Enable** to enable the feature you've selected.

Note:

The setup can take up to 15 minutes to complete.



Subscriptions: 1 of 4 selected – Don't see a subscription? Open Directory + Subscription settings

3 of 3 items selected

☑ Name	Type	Status	Resource group	Location	Source	Maintenance status	Subscription
☑ ContosoVM1	Virtual machine	Running	contosoresourcegroup	East US	Marketplace	-	Contoso Demo
☑ ContosoVM2	Virtual machine	Running	contosoresourcegroup	East US	Marketplace	-	Contoso Demo
☑ ContosoVM3	Virtual machine	Running	contosoresourcegroup	East US	Marketplace	-	Contoso Demo

ASSESSMENT NO. 1

Name:__________________________ Year, Course and Section: ______________

Subject: _________________________

Check your knowledge

1. What is Windows Server?
2. How to install Windows Server Interview Questions?
3. What is the main purpose of Windows Server?
4. Why is Windows Server important?
5. What do you know about the active directory in the system administration?
6. What is group policy?
7. Can you tell us about your experience with hardware Components?
8. Why backing up an active directory is important, and how can you back up an active directory?
9. What is a domain controller?
10. What do you know about proxy servers?

1.3 References

Learn.microsoft.com

1.4 Acknowledgement

All the figures and information presented in this module were taken from the references enumerated above.