

Week 10 Assignment 1: Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel

Introduction

1. Azure Monitor

Azure Monitor is a comprehensive monitoring solution for collecting, analyzing, and responding to monitoring data from your cloud and on-premises environments. You can use Azure Monitor to maximize the availability and performance of your applications and services. It helps you understand how your applications are performing and allows you to manually and programmatically respond to system events. Azure Monitor collects and aggregates the data from every layer and component of your system across multiple Azure and non-Azure subscriptions and tenants. It stores it in a common data platform for consumption by a common set of tools that can correlate, analyze, visualize, and/or respond to the data. You can also integrate other Microsoft and non-Microsoft tools.

Azure Monitor gives full visibility into your environment. It's your eyes and ears for performance, security, and troubleshooting.

What it does:

- Collects logs and metrics from all Azure resources
- Provides dashboards, alerts, and visualizations
- Helps diagnose performance issues
- Tracks application availability & health

2. Microsoft Defender for Cloud

Microsoft Defender for Cloud is a Cloud Native Application Protection Platform (CNAPP), which is a unified solution that combines multiple cloud security tools to protect applications across their entire lifecycle. The solution provides a comprehensive view of your security posture across your cloud and on-premises

resources. It also helps you secure multicloud and hybrid environments and integrates security into DevOps workflows.

It has three core components:

1. **Cloud Security Posture Management (CSPM)** checks and improves the security posture of cloud resources.
2. **Development Security Operations (DevSecOps)** manages code-level security across multicloud and multi-pipeline environments.
3. **Cloud Workload Protection Platform (CWPP)** defends workloads such as virtual machines (VMs), containers, storage, databases, and serverless functions from threats.

Defender for Cloud uses its broader Cloud Native Application Protection Platform (CNAPP) capabilities to unify protections into one experience. Defender for Cloud embeds security early in the development lifecycle. It helps DevOps teams find misconfigurations, apply policies, and fix risks early. Defender for Cloud integrates with the Defender XDR portal and the Microsoft Security ecosystem, offering unified posture management and SOC experiences.

In addition to its core CNAPP capabilities, Defender for Cloud delivers AI security and AI threat protection to safeguard generative AI workloads throughout their lifecycle. These features help you discover AI applications, identify vulnerabilities, reduce risks, and detect threats targeting your generative AI workloads.

What it does:

- Continuously evaluates your security posture
- Gives secure score recommendations
- Detects threats across VMs, storage, databases, containers, and networks
- Provides hardening and vulnerability insights
- Integrates with Azure, AWS, and GCP

Why it's important:

It helps identify misconfigurations (like public buckets, open ports, weak passwords) and protects workloads from attacks using real-time threat detection.

3. Just-In-Time (JIT) VM Access

Just-in-Time (JIT) VM Access is a security feature, prominent in Microsoft Defender for Cloud (Azure), that locks down management ports (like SSH/RDP) on virtual machines, only opening them dynamically for a limited time when requested and approved, drastically reducing the attack surface from constant exposure. It works by temporarily modifying Network Security Group (NSG) rules to allow specific IP access, then automatically closing them after the set period, preventing unauthorized breaches and simplifying secure access for legitimate users

Why it's important:

- Prevents brute-force attacks
- Reduces the attack surface significantly
- Ensures access is controlled, logged, and temporary

4. Microsoft Sentinel

Microsoft Sentinel is a cloud-native SIEM solution that delivers scalable, cost-efficient security across multicloud and multiplatform environments. It combines AI, automation, and threat intelligence to support threat detection, investigation, response, and proactive hunting. It centralizes logs, detects threats, and automates responses to reduce attack impact.

Microsoft Sentinel SIEM empowers analysts to anticipate and stop attacks across clouds and platforms, faster and with greater precision.

Microsoft Sentinel inherits the Azure Monitor tamper-proofing and immutability practices. While Azure Monitor is an append-only data platform, it includes provisions to delete data for compliance purposes.

What it does:

- Collects and correlates security logs from Azure, AWS, GCP, and on-prem
- Detects threats using built-in analytics and machine learning
- Enables incident investigation and hunting
- Automates responses through playbooks
- Provides dashboards for security events

Lab 08: Create a Log Analytics Workspace, Azure Storage Account, and Data Collection Rule (DCR)

A **Log Analytics workspace** is a data store into which you can collect any type of log data from all of your Azure and non-Azure resources and applications. Workspace configuration options let you manage all of your log data in one workspace to meet the operations, analysis, and auditing needs of different personas in your organization through:

- Azure Monitor features, such as built-in insights experiences, alerts, and automatic actions
- Other Azure services, such as Microsoft Sentinel, Microsoft Defender for Cloud, and Logic Apps
- Microsoft tools, such as Power BI and Excel
- Integration with custom and third-party applications

Data collection rules (DCRs) are part of an Extract, transform, and load (ETL)-like data collection process that improves on legacy data collection methods for Azure Monitor. This process uses a common data ingestion strategy for all data sources

and a standard method of configuration that's more manageable and scalable than previous collection methods.

Specific advantages of DCR-based data collection include:

- Consistent method for configuration of different data sources.
- Ability to apply a transformation to filter or modify incoming data before it's sent to a destination.
- Scalable configuration options supporting infrastructure as code and DevOps processes.
- Option of Azure Monitor pipeline in your own environment to provide high-end scalability, layered network configurations, and periodic connectivity.

Lab scenario

As an Azure Security Engineer for a financial technology company, you are tasked with enhancing monitoring and security visibility across all Azure virtual machines (VMs) used for processing financial transactions and managing sensitive customer data. The security team requires detailed logs and performance metrics from these VMs to detect potential threats and optimize system performance. The Chief Information Security Officer (CISO) has asked you to implement a solution that collects security events, system logs, and performance counters. You have been assigned to configure the Azure Monitor Agent (AMA) along with Data Collection Rules (DCRs) to centralize log collection and performance monitoring.

Lab objectives

In this lab, you will complete the following exercises:

- Exercise 1: Deploy an Azure virtual machine
- Exercise 2: Create a Log Analytics workspace
- Exercise 3: Create an Azure storage account

-
- Exercise 4: Create a data collection rule

Instructions

Exercise 1: Deploy an Azure virtual machine

In this exercise, I completed the following tasks:

Task 1: Deploy an Azure virtual machine

1. Sign-in to the Azure portal <https://portal.azure.com/>.
Sign in to the Azure portal using an account that has the Owner or Contributor role in the Azure subscription you are using for this lab.
In this Cloudslice lab, this account is
LabUser-57445941@LODSPRODMCA.onmicrosoft.com with TAP
9-A*LpfA.
2. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select PowerShell.
3. Ensure PowerShell is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.
4. In the Getting started window, leave the default setting as is: Select a subscription to get started. You can optionally mount a storage account to persist files between sessions. No storage account required.
5. From the Subscription drop-down menu, select your lodsubscription.
6. Leave Use an existing private virtual network unchecked, then click Apply.
7. In the PowerShell session within the Cloud Shell pane, run the following to create a resource group that will be used in this lab:

powershellTypeCopy

```
New-AzResourceGroup -Name AZ500LAB131415 -Location 'EastUS'
```

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome

labclient.labondemand.com/LabClient/b9290af4-c0a5-4d4e-9da9-7f2cef858db0

Favorite

Type Last Viewed

Getting started

Select a subscription to get started. You can optionally mount a storage account to persist files between sessions. [Learn more](#)

☒ No storage account required ☐ Mount storage account

Subscription *

MOC Subscription-lod51809825

☐ Use an existing private virtual network [Learn more](#)

Apply Previous

Instructions Resources

down menu in the upper-left corner of the Cloud Shell pane.

4. In the **Getting started** window, leave the default setting as is: **Select a subscription to get started**. You can optionally mount a storage account to persist files between sessions. No storage account required.

5. From the **Subscription** drop-down menu, select your **lodsubscription**.

6. Leave **Use an existing private virtual network** unchecked, then click **Apply**.

7. In the PowerShell session within the Cloud Shell pane, run the following to create a resource group that will be used in this lab:

powershell Type Copy

Previous Next

5 Hr 44 Min Remaining

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome

labclient.labondemand.com/LabClient/b9290af4-c0a5-4d4e-9da9-7f2cef858db0

Resources

Recent Favorite

Name Type Last Viewed

Switch to Bash Restart Manage files New session Editor Web preview Settings Help

There will be breaking changes from 14.6.0 to 15.1.0. Open <https://go.microsoft.com/fwlink/?linkid=2241373> for details.

VERBOSE: Building your Azure drive ...

```
PS /home/labuser-57473160> Install-Module Az.Compute -RequiredVersion 4.23.0 -Force
PS /home/labuser-57473160> New-AzResourceGroup -Name AZ500LAB131415 -Location 'EastUS'
```

ResourceGroupName : AZ500LAB131415
Location : eastus
ProvisioningState : Succeeded
Tags :
ResourceId : /subscriptions/b115b74e-a0c7-4c09-8308-7500e502c117/resourceGroups/AZ500LAB131415

PS /home/labuser-57473160>

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel

Instructions Resources

Select your **lodsubscription**.

6. Leave **Use an existing private virtual network** unchecked, then click **Apply**.

7. In the PowerShell session within the Cloud Shell pane, run the following to create a resource group that will be used in this lab:

powershell Type Copy

```
PS /home/labuser-57473160> New-AzResourceGroup -Name AZ500LAB131415 -Location 'EastUS'
```

This resource group will be used for labs 8, 9, and 10.

8. In the PowerShell session within the Cloud Shell pane, run the following to enable session at host (FAH):

Previous Next

5 Hr 42 Min Remaining

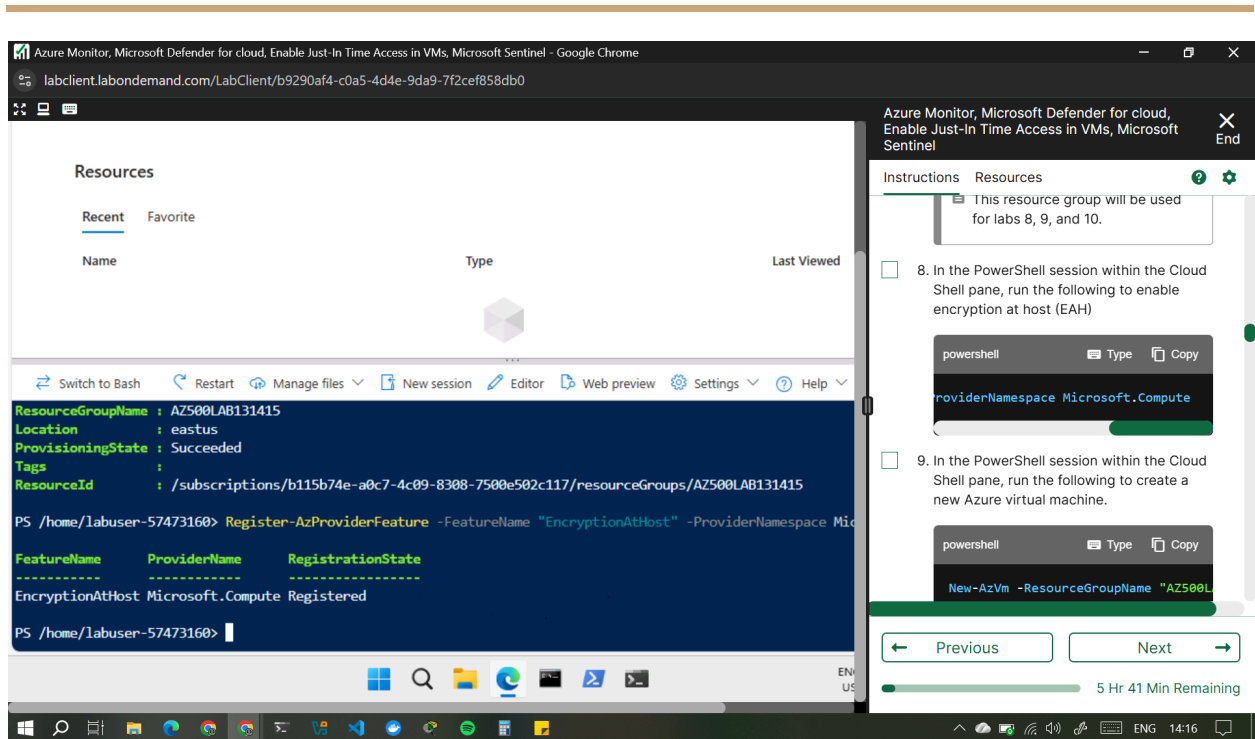
8. This resource group will be used for labs 8, 9, and 10.

-
9. In the PowerShell session within the Cloud Shell pane, run the following to enable encryption at host (EAH)

Encryption at host (or host-based encryption) is a security feature, prominent in cloud platforms like Azure, that encrypts data directly on the virtual machine's host server, providing end-to-end encryption for VM data (OS/data disks, temporary disks, caches) as it moves to and rests in storage, without impacting VM performance. It enhances default encryption by securing data at rest and in transit between the host and storage, ensuring data remains encrypted from the moment it's generated on the host until it's persisted.

```
powershellTypeCopy
```

```
Register-AzProviderFeature -FeatureName "EncryptionAtHost"  
-ProviderNamespace Microsoft.Compute
```



10. In the PowerShell session within the Cloud Shell pane, run the following to create a new Azure virtual machine.

```

powershellTypeCopy
New-AzVm -ResourceGroupName "AZ500LAB131415" -Name "myVM"
-Location 'EastUS' -VirtualNetworkName "myVnet" -SubnetName
"mySubnet" -SecurityGroupName "myNetworkSecurityGroup"
-PublicIpAddressName "myPublicIpAddress" -PublicIpSku Standard
-OpenPorts 80,3389 -Size Standard_D2s_v3

```

11. When prompted for credentials:

Setting	Value
---------	-------

User localadmin

Password Please use your personal password created in
Lab 02 > Exercise 2 > Task 1 > Step 3.

12. Wait for the deployment to complete.

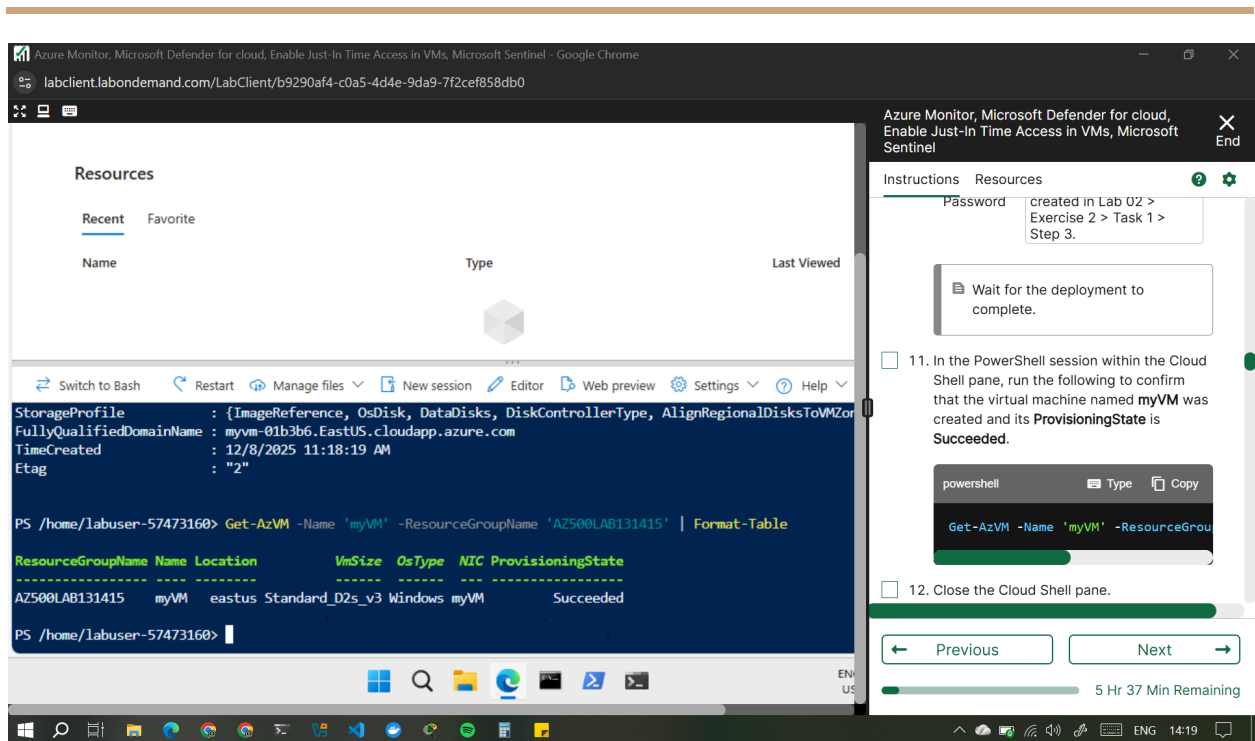
13. In the PowerShell session within the Cloud Shell pane, run the following to confirm that the virtual machine named myVM was created and its ProvisioningState is Succeeded.

14. powershellTypeCopy

15. `Get-AzVM -Name 'myVM' -ResourceGroupName 'AZ500LAB131415' | Format-Table`

The screenshot displays the Azure Cloud Shell environment. On the left, a PowerShell terminal window shows the execution of the `New-AzVM` command to create a virtual machine named 'myVM' in the resource group 'AZ500LAB131415'. The command includes parameters for location ('EastUS'), virtual network ('myVnet'), subnet ('mySubnet'), security group ('myNetworkSecurityGroup'), and public IP address ('myPublicIp'). The terminal output shows the command being executed and the user being prompted for credentials.

On the right, a pane titled 'Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel' displays the deployment progress. It includes a 'Resources' section with a table showing the deployment of a new Azure virtual machine. The table has columns for 'Setting' and 'Value'. The 'User' is set to 'localadmin'. The 'Password' field is populated with the instruction: 'Please use your personal password created in Lab 02 > Exercise 2 > Task 1 > Step 3.' Below the table, there is a 'Wait for the deployment to complete' message and a progress bar indicating '5 Hr 40 Min Remaining'.



Exercise 2: Create a Log Analytics workspace

In this exercise, I completed the following tasks:

Task 1: Create a Log Analytics workspace

In this task, you will create a Log Analytics workspace.

1. In the Azure portal, in the Search resources, services, and docs text box at the top of the Azure portal page, type Log Analytics workspaces and press the Enter key.
2. On the Log Analytics workspaces blade, click + Create.
3. On the Basics tab of the Create Log Analytics workspace blade, specify the following settings (leave others with their default values):

Setting	Value
---------	-------

Subscription the name of the Azure subscription you are using in this lab

Resource AZ500LAB131415
group

Name LAW57445941

Region East US

4. Select Review + create.
5. On the Review + create tab of the Create Log Analytics workspace blade, select Create.

The screenshot shows the 'Create Log Analytics workspace' blade in the Azure portal, specifically the 'Review + Create' tab. The blade is titled 'Log Analytics workspace by Microsoft'. It displays a 'Validation passed' message at the top. The 'Basics' section shows the following details:

Setting	Value
Subscription	MOC Subscription-lod51809825
Resource group	AZ500LAB131415
Name	LAW57473160
Region	East US

The 'Pricing' section shows the 'Pricing tier' as 'Pay-as-you-go (Per GB 2018)'. Below this, a note states: 'The cost of your workspace depends on the volume of data ingested and how long it is retained. Regional pricing details are available on the [Azure Monitor pricing page](#). You can change to a different pricing tier after the workspace is created.'

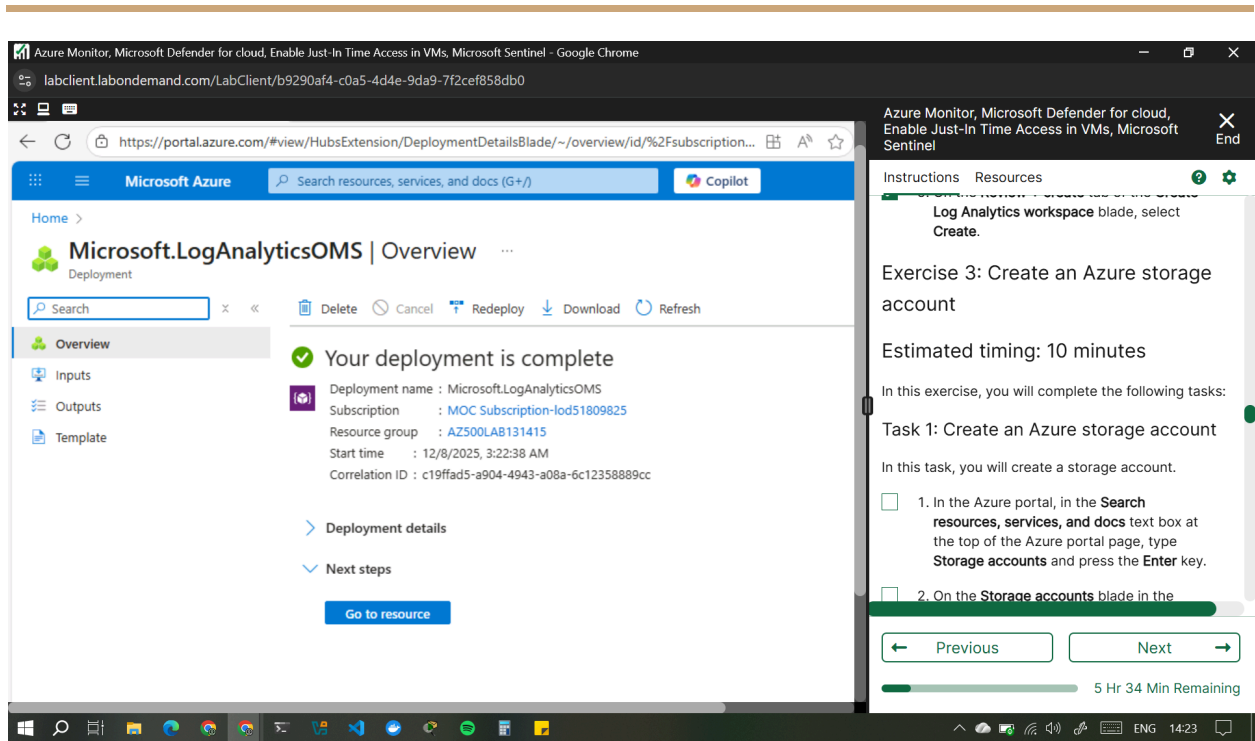
At the bottom of the blade, there are three buttons: 'Create', '< Previous', and 'Download a template for automation'. To the right of the blade, a sidebar contains 'Instructions' and 'Resources'. The 'Instructions' section lists the following settings (leave others with their default values):

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	AZ500LAB131415
Name	LAW57473160
Region	East US

Below the instructions, there are two checkboxes with corresponding text:

- ☐ 4. Select **Review + create**.
- ☐ 5. On the **Review + create** tab of the **Create Log Analytics workspace** blade, select **Create**.

At the bottom of the sidebar, there is a section titled 'Exercise 3: Create an Azure storage' with 'Previous' and 'Next' buttons. A progress bar at the bottom right indicates '5 Hr 35 Min Remaining'.



Exercise 3: Create an Azure storage account

In this exercise, you will complete the following tasks:

Task 1: Create an Azure storage account

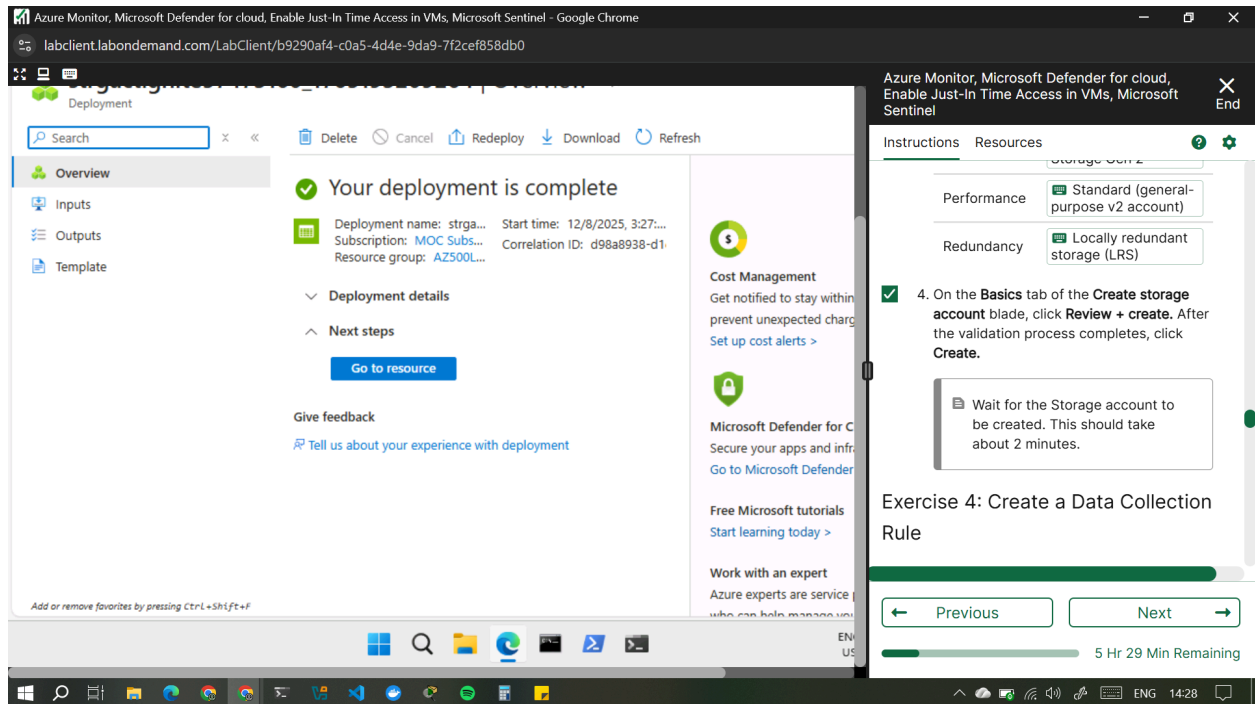
In this task, you will create a storage account.

1. In the Azure portal, in the Search resources, services, and docs text box at the top of the Azure portal page, type Storage accounts and press the Enter key.
2. On the Storage accounts blade in the Azure portal, click the + Create button to create a new storage account.
3. On the Basics tab of the Create storage account blade, specify the following settings (leave others with their default values):

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	AZ500LAB131415
Instance details	
Storage account name	strgactignite57445941
Region	(US) EastUS
Primary service	Azure Blob Storage or Azure Data Lake Storage Gen 2
Performance	Standard (general-purpose v2 account)
Redundancy	Locally redundant storage (LRS)

***NB: Locally Redundant Storage (LRS) is a cost-effective data protection strategy, primarily in cloud platforms like Azure, that keeps three identical copies of your data within a single data center, protecting against local hardware (drive/rack) failures but not against large-scale disasters like floods or fires that could wipe out the entire facility. It's the cheapest option but offers the least resilience compared to Zone-Redundant Storage (ZRS) or Geo-Redundant Storage (GRS).**

4. On the Basics tab of the Create storage account blade, click Review + create. After the validation process completes, click Create.
Wait for the Storage account to be created. This should take about 2 minutes.



Exercise 4: Create a Data Collection Rule

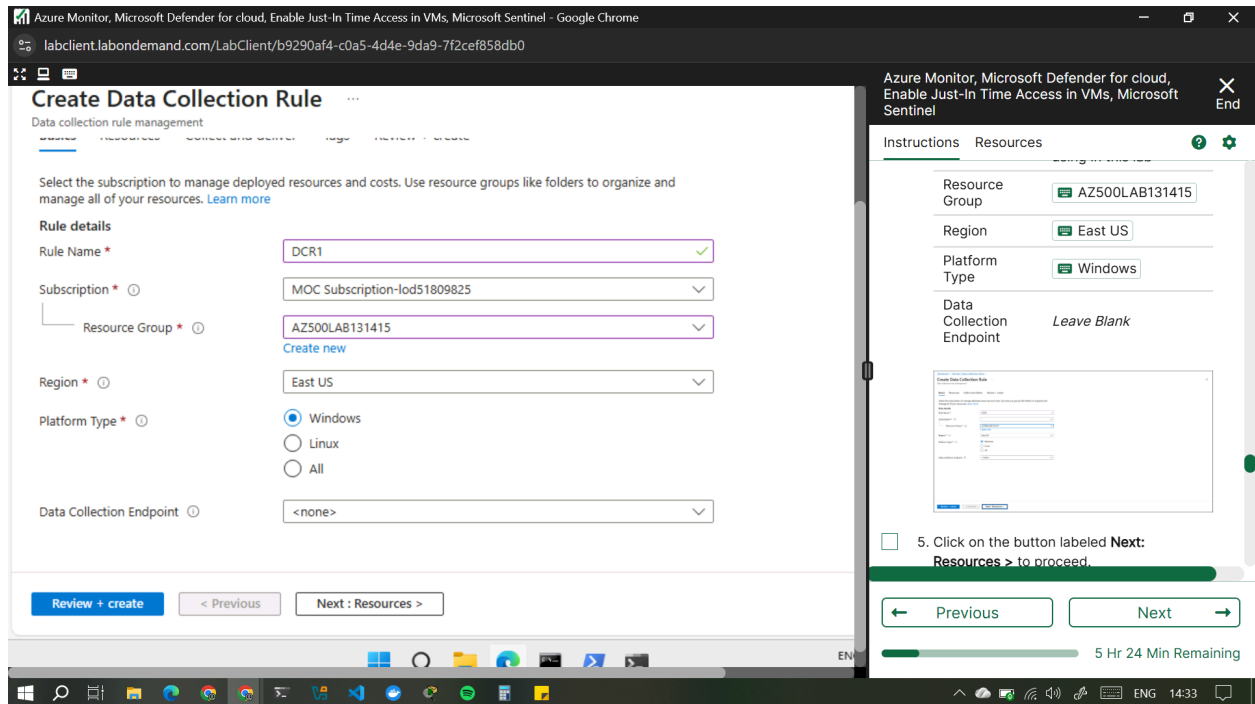
Task 1: Create a Data Collection Rule.

In this task, you will create a data collection rule.

1. In the Azure portal, in the Search resources, services, and docs text box at the top of the Azure portal page, type Monitor and press the Enter key.
2. On the Monitor Settings blade, click Data Collection Rules.
3. Click the + Create button to create a new data collection rule.

-
4. On the Basics tab of the Create Data Collection Rule blade, specify the following settings:

Setting	Value
Rule details	
Rule Name	DCR1
Subscription	the name of the Azure subscription you are using in this lab
Resource Group	AZ500LAB131415
Region	East US
Platform Type	Windows
Data Collection Endpoint	<i>Leave Blank</i>



5. Click on the button labeled Next: Resources > to proceed.
6. On the Resources page, select + Add resources.
7. In the Select a scope template, check the Subscription box in the Scope.
8. At the bottom of the Select a scope template, click Apply.
9. At the bottom of the Resources page, select Next: Collect and deliver >.
10. Click + Add data source, then on the Add data source page, change the Data source type drop-down menu to display Performance Counters. Leave the following default settings:

Setting	Value
+++Performance counter**	**Sample rate (seconds)+++

CPU 60

Memory 60

Disk 60

Network 60

The screenshot shows the Azure Monitor console in Google Chrome. The main area displays the 'Resources' page with filters for 'All resource groups', 'All resource types', and 'All locations'. A table lists the following resources:

Scope	Resource type	Location
☒ MOC Subscription-lod51809825	Subscription	-
☐ > AZ500LAB131415	Resource group	-

At the bottom of the table are buttons for 'Apply', 'Cancel', and 'Clear all selections'.

On the right, a sidebar titled 'Instructions' contains a list of steps:

- 5. Click on the button labeled **Next: Resources >** to proceed.
- 6. On the **Resources** page, select **+ Add resources**.
- 7. In the **Select a scope** template, check the **Subscription** box in the **Scope**.
- 8. At the bottom of the **Select a scope** template, click **Apply**.
- 9. At the bottom of the **Resources** page, select **Next: Collect and deliver >**.
- 10. Click **+ Add data source**, then on the **Add data source** page, change the **Data source type** drop-down menu to display

At the bottom of the sidebar are 'Previous' and 'Next' buttons, and a progress bar indicating '5 Hr 23 Min Remaining'.

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome

labclient.labondemand.com/LabClient/b9290af4-c0a5-4d4e-9da9-7f2cef858db0

Create Data Collection Rule

Data collection rule management

Basics **Resources** Collect and deliver Tags Review + create

Pick a set of resources to collect data from. The Azure Monitor Agent will be automatically installed on virtual machines, scale sets, and servers. For AKS clusters, managed Prometheus will automatically be enabled. For Windows 10 and 11 devices, [download the client installer](#) and follow the [guidance](#).

Info This will also enable System Assigned Managed Identity on these resources, in addition to existing User Assigned Identities (if any).

+ Add resources + Create endpoint

Enable Data Collection Endpoints ☐

Info Only resources in the same region can be assigned to the same endpoint. [Learn more](#)

Name	Type	Location	Resource group	Subscription
myVM	Virtual machine	East US	AZ500LAB131415	MOC Subscripti

Review + create < Previous Next: Collect and deliver >

Instructions Resources

5. Click on the button labeled **Next: Resources >** to proceed.
6. On the **Resources** page, select + **Add resources**.
7. In the **Select a scope** template, check the **Subscription** box in the **Scope**.
8. At the bottom of the **Select a scope** template, click **Apply**.
9. At the bottom of the **Resources** page, select **Next: Collect and deliver >**.
10. Click + **Add data source**, then on the **Add data source** page, change the **Data source type** drop-down menu to display

Previous **Next**

5 Hr 22 Min Remaining

Dashboard > Monitor | Data Collection Rules >

Create Data Collection Rule

Data collection rule management

Basics Resources **Collect and deliver** Review + create

Configure which data sources to collect, and where to send the data to.

+ Add data source

Data source Destination(s)

No standard data sources or destinations found.

Error This data collection rule doesn't have any data sources or destinations selected.

Add data source

* Data source Destination

Select which data source type and the data to collect for your resource(s).

Data source type *

Performance Counters

Choose Basic to enable the collection of performance counters. Choose Custom if you want more control over which performance counters are collected.

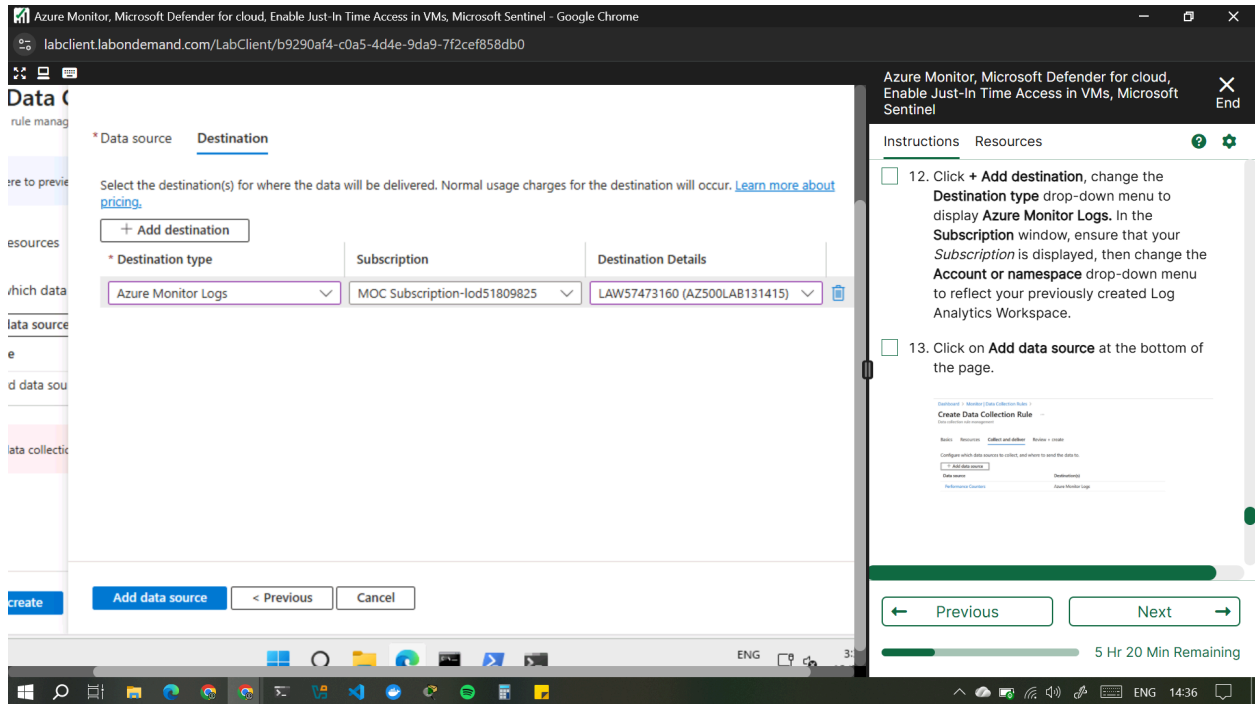
None **Basic** Custom

Performance counter	Sample rate (seconds)
☒ CPU	60
☒ Memory	60
☒ Disk	60
☒ Network	60

Add data source **Next: Destination >** Cancel

11. Click on the button labeled **Next: Destination >** to proceed.
12. Click + **Add destination**, change the **Destination type** drop-down menu to display **Azure Monitor Logs**. In the **Subscription** window, ensure that your *Subscription* is displayed, then change the **Account**

or namespace drop-down menu to reflect your previously created Log Analytics Workspace.



13. Click on Add data source at the bottom of the page.

14. Click Review + create.

[Dashboard](#) > [Monitor](#) | [Data Collection Rules](#) >

Create Data Collection Rule ...

Data collection rule management

✓ Validation passed

Basics Resources Collect and deliver Review + create

Basics

Data rule name	DCR1
Subscription	MCAPS-Hybrid-REQ-48118-2022-serlingdavis
Resource Group	AZ500LAB131415

Selected resources

Resources	Type
myvm	microsoft.compute/virtualmachines

Configurations

Data source	Destination(s)
Performance Counters	Azure Monitor Logs

Platform Type

Platform	Windows
----------	---------

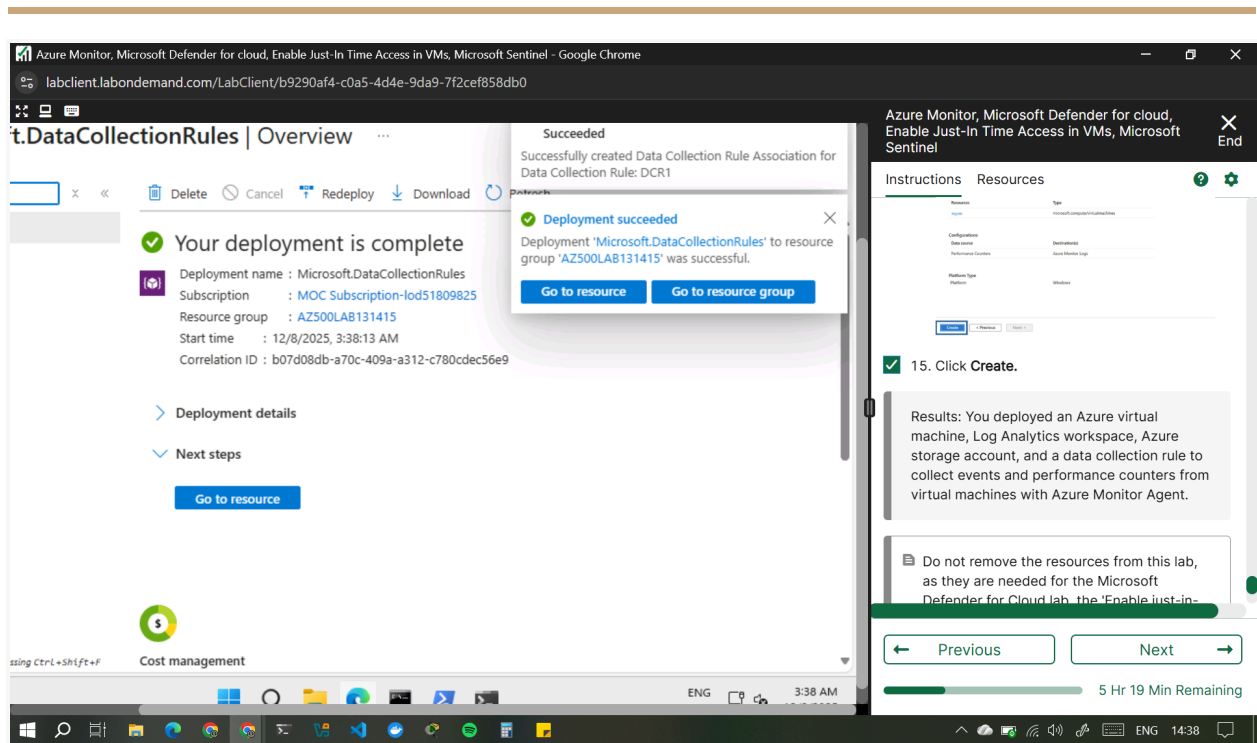
Create

< Previous

Next: >

15. Click Create.

Results: I deployed an Azure virtual machine, Log Analytics workspace, Azure storage account, and a data collection rule to collect events and performance counters from virtual machines with Azure Monitor Agent.



Lab 09: Configuring Microsoft Defender for Cloud Enhanced Security Features for Servers

Lab scenario

As an Azure Security Engineer for a global e-commerce company, you are responsible for securing the company's cloud infrastructure. The organization relies heavily on Azure virtual machines (VMs) and on-premises servers to run critical applications, manage customer data, and process transactions. The Chief Information Security Officer (CISO) has identified the need for enhanced security measures to protect these resources against cyber threats, vulnerabilities, and misconfigurations. You have been tasked with enabling Microsoft Defender for Servers in Microsoft Defender for Cloud to provide advanced threat protection and security monitoring for both Azure VMs and hybrid servers.

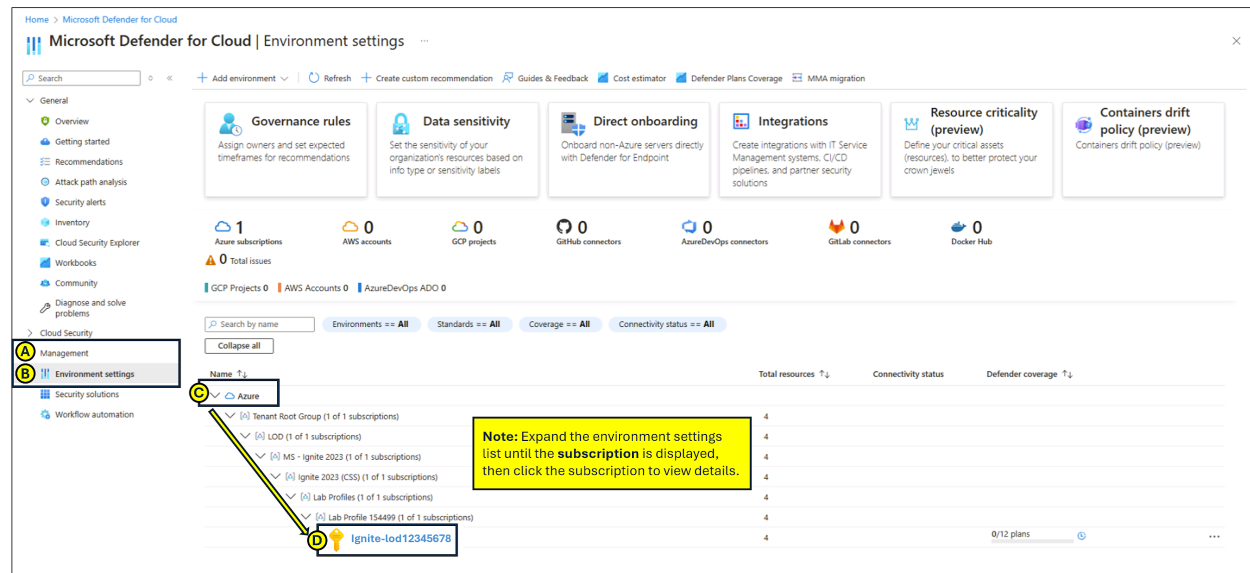
Lab objectives

- Configure Microsoft Defender for Cloud Enhanced Security Features for Servers
- Review the enhanced security features for Microsoft Defender for Servers Plan 2

Exercise instructions

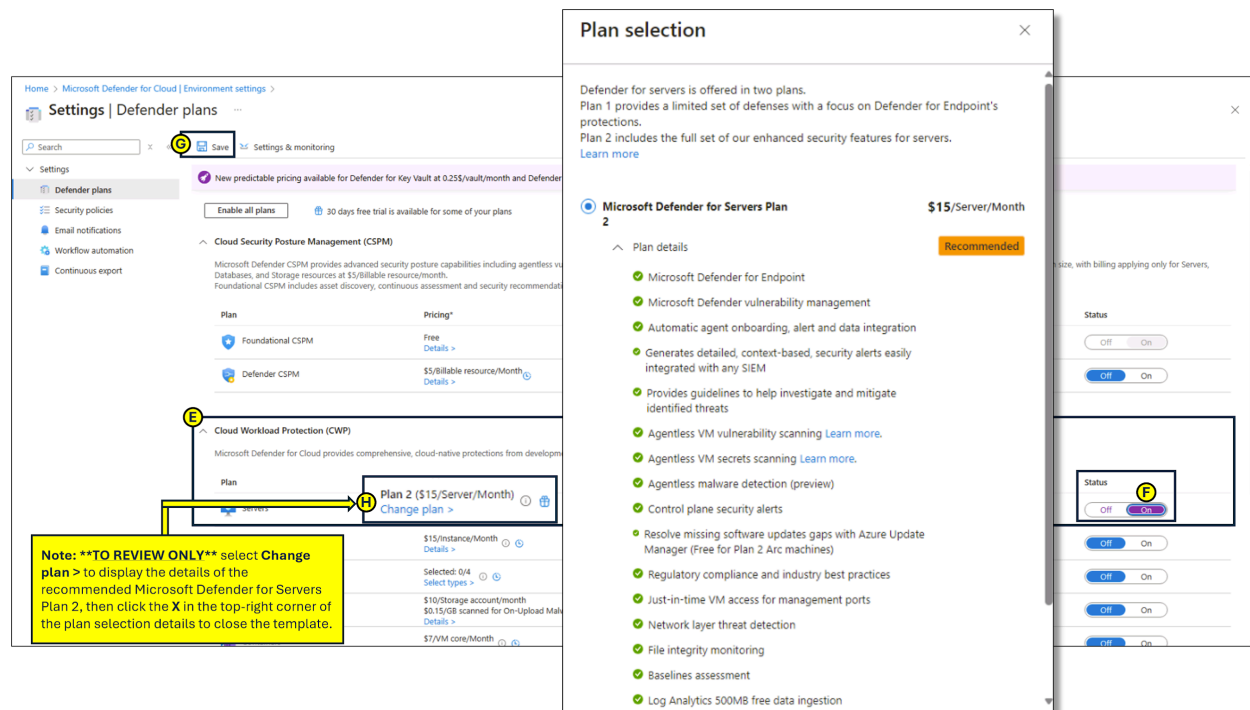
Configure Microsoft Defender for Cloud Enhanced Security Features for Servers

1. In the Azure portal, in the Search resources, services, and docs text box at the top of the Azure portal page, type Microsoft Defender for Cloud and press the Enter key.
2. On the Microsoft Defender for Cloud, Management blade, go to the Environment settings. Expand the environment settings folders until the subscription section is displayed, then click the subscription to view details.



3. In the Settings blade, under Defender plans, expand Cloud Workload Protection (CWP).

4. From the Cloud Workload Protection (CWP) Plan list, select Servers. On the right side of the page, change the Status from Off to On, then click Save.
 5. To review the details of Microsoft Defender for Servers Plan 2, select Change plan >.
- Note: Enabling the Cloud Workload Protection (CWP) Servers plan from Off to On enables Microsoft Defender for Servers Plan 2.



Results: I enabled Microsoft Defender for Servers Plan 2 on my subscription.

Lab 10: Enable just-in-time access on VMs

Lab scenario

As an Azure Security Engineer at a financial services company, you're responsible for securing Azure resources, including virtual machines (VMs) that host critical applications. The security team has identified that continuous open access to VMs

increases the risk of brute-force attacks and unauthorized access. To mitigate this, the Chief Information Security Officer (CISO) has requested that you enable Just-in-Time (JIT) VM access on a specific Azure VM used for processing financial transactions.

Lab objectives

In this lab, you will complete the following exercises:

- Exercise 1: Enable JIT on your VMs from the Azure portal.
- Exercise 2: Request access to a VM that has JIT enabled from the Azure portal.

Exercise instructions

Exercise 1: Enable JIT on your VMs from Azure virtual machines

You can enable JIT on a VM from the Azure virtual machines pages of the Azure portal.

1. In the search box at the top of the portal, enter virtual machines. Select Virtual machines in the search results.
2. Select myVM.
3. Select Configuration from the Settings section of myVM.
4. Under Just-in-time VM access, select Enable just-in-time.
5. Under Just-in-time VM access, click on the link that reads Open Microsoft Defender for Cloud.

Instructions Resources

2. Select **myVM**.
3. Select **Configuration** from the **Settings** section of **myVM**.
4. Under **Just-in-time VM access**, select **Enable just-in-time**.
5. Under **Just-in-time VM access**, click on the link that reads **Open Microsoft Defender for Cloud**.
6. By default, just-in-time access for the VM uses these settings:
 - Windows machines
 - RDP port: 3389
 - Maximum allowed access: Three hours
 - Allowed source IP addresses: Any

← Previous Next →

4 Hr 39 Min Remaining

Instructions Resources

Results: You have explored various methods on how to enable JIT on your VMs and how to request access to VMs that have JIT enabled in Microsoft Defender for Cloud.

Congratulations!

You have successfully completed this Lab. Click **Next** to advance to the next Lab.

← Previous Next →

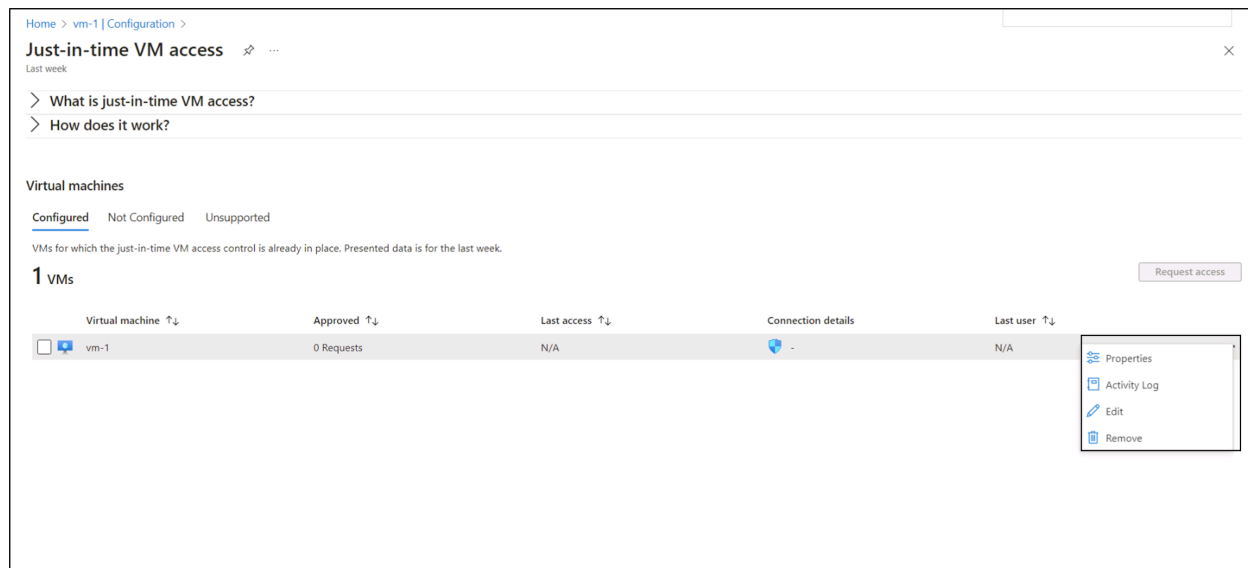
4 Hr 33 Min Remaining

6. By default, just-in-time access for the VM uses these settings:

- Windows machines
 - RDP port: 3389
 - Maximum allowed access: Three hours
 - Allowed source IP addresses: Any
- Linux machines
 - SSH port: 22
 - Maximum allowed access: Three hours
 - Allowed source IP addresses: Any

7. By default, just-in-time access for the VM uses these settings:

- From the Configured tab, right-click on the VM to which you want to add a port, and select edit.



8.

- Under JIT VM access configuration, you can either edit the existing settings of an already protected port or add a new custom port.
- When you've finished editing the ports, select Save.

Exercise 2: Request access to a JIT-enabled VM from the Azure virtual machine's connect page.

When a VM has a JIT enabled, you have to request access to connect to it. You can request access in any of the supported ways, regardless of how you enabled JIT.

1. In the Azure portal, open the virtual machines pages.
2. Select the VM to which you want to connect, and open the Connect page.
 - Azure checks to see if JIT is enabled on that VM.
 - If JIT isn't enabled for the VM, you're prompted to enable it.
 - If JIT is enabled, select Request access to pass an access request with the requesting IP, time range, and ports that were configured for that VM.

The screenshot shows the Azure portal interface for requesting access to a virtual machine. The main content area displays a table with one request. The sidebar on the right contains instructions and a results section.

Request access

ne VM access?

ured Unsupported

ne VM access control is already in place. Presented data is for the last week.

Request access

Approved	Last access	Connection details	Last user
1 Requests	N/A		N/A

Instructions Resources

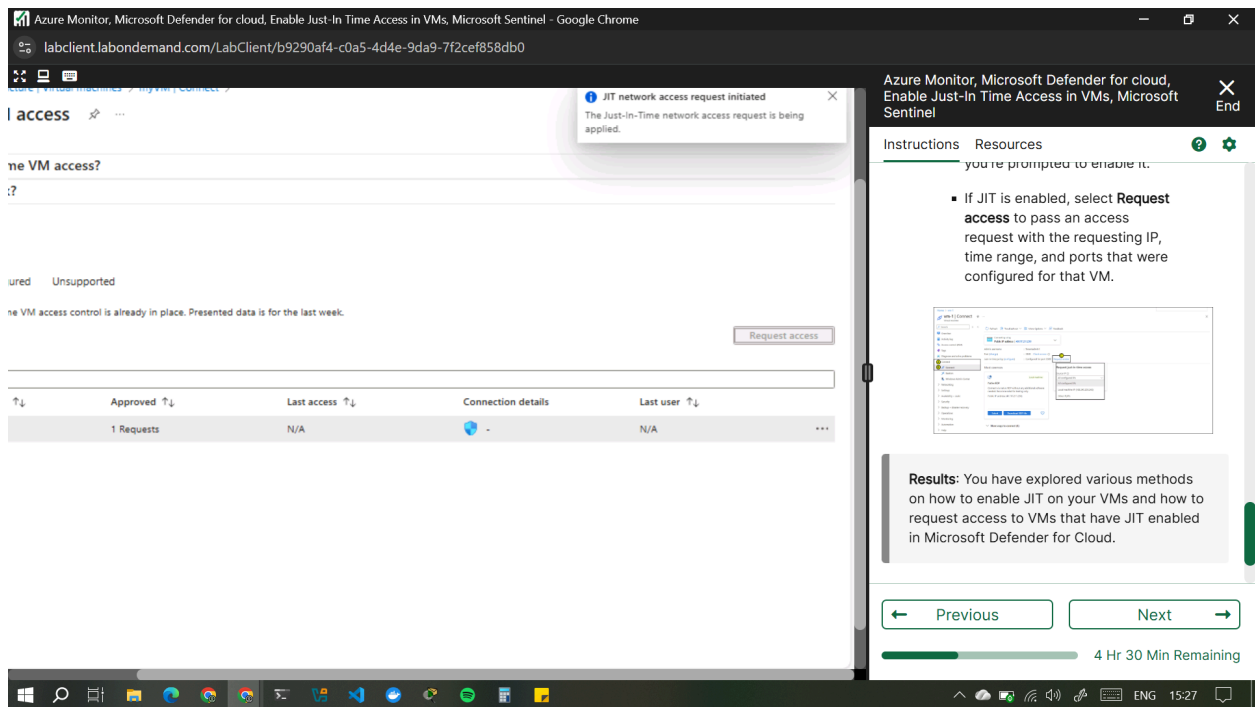
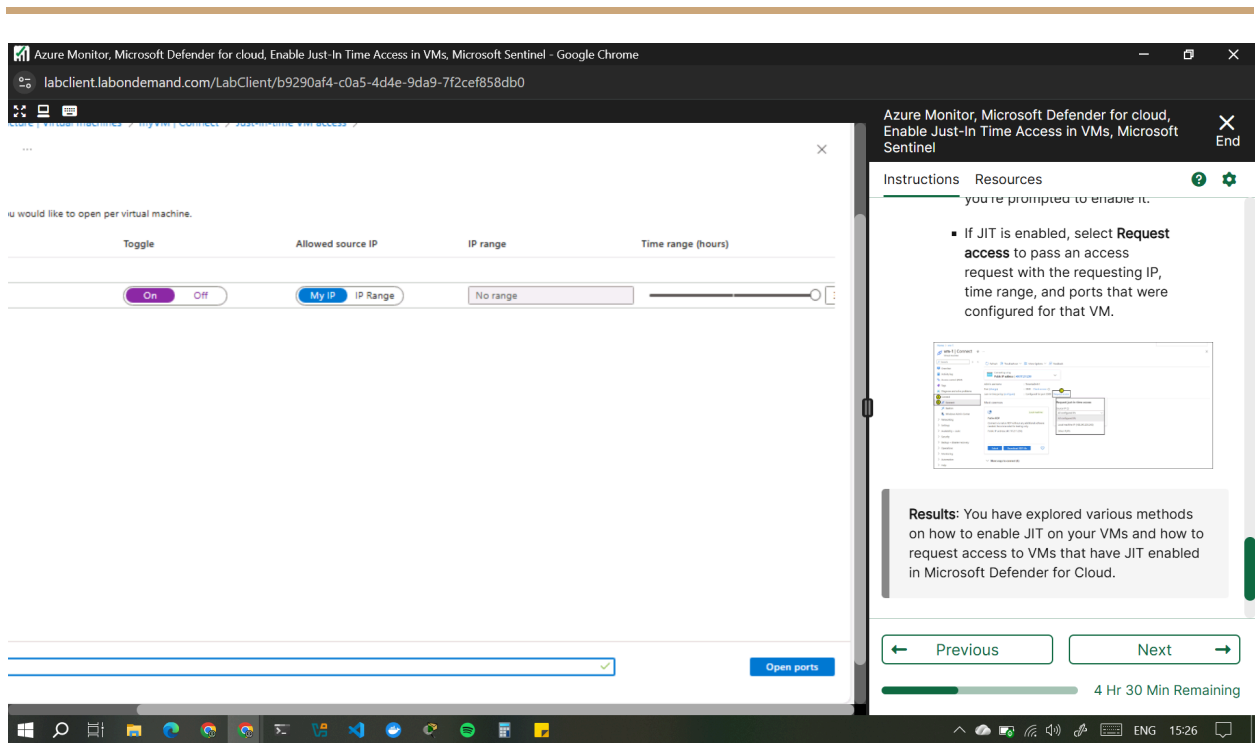
you're prompted to enable it.

- If JIT is enabled, select **Request access** to pass an access request with the requesting IP, time range, and ports that were configured for that VM.

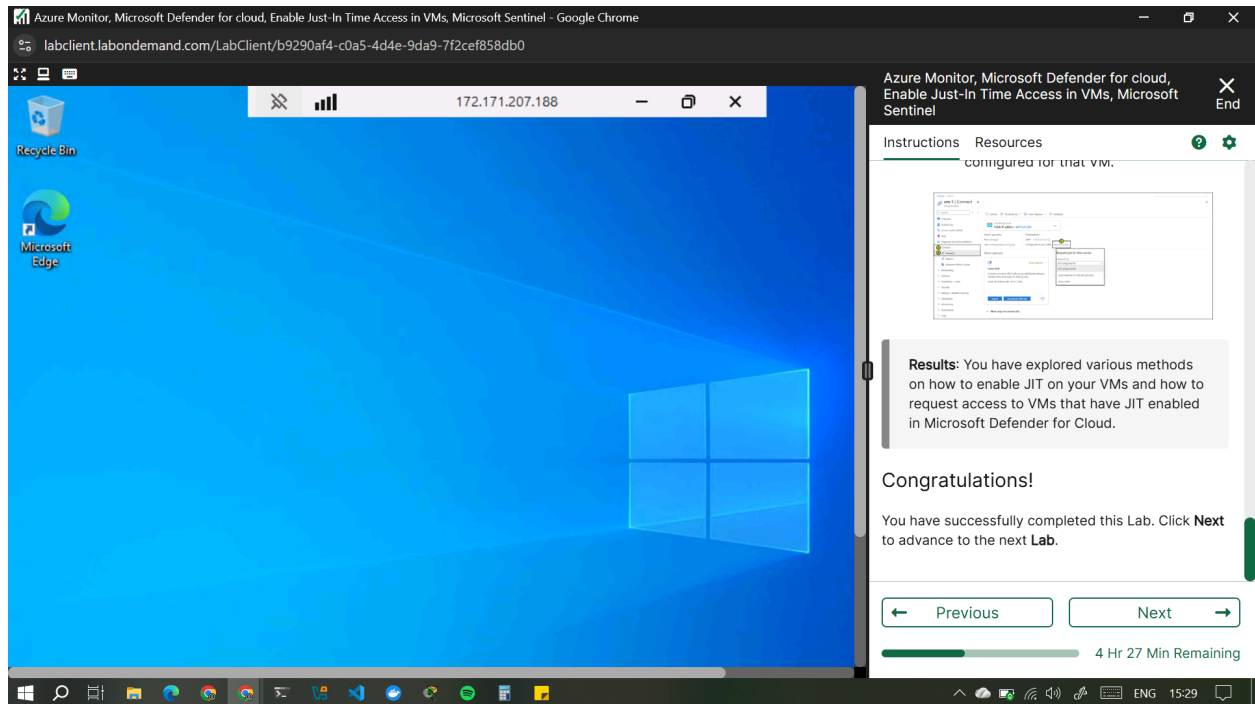
Results: You have explored various methods on how to enable JIT on your VMs and how to request access to VMs that have JIT enabled in Microsoft Defender for Cloud.

Previous **Next**

4 Hr 31 Min Remaining



- After requesting access to the configured VM, I was able to connect to it using RDP



Results: I have explored various methods on how to enable JIT on VMs and how to request access to VMs that have JIT enabled in Microsoft Defender for Cloud.

Lab 11: Microsoft Sentinel

Lab scenario

Note: Azure Sentinel is renamed to Microsoft Sentinel

You have been asked to create a proof of concept of Microsoft Sentinel-based threat detection and response. Specifically, you want to:

- Start collecting data from Azure Activity and Microsoft Defender for Cloud.
- Add built in and custom alerts
- Review how Playbooks can be used to automate a response to an incident.

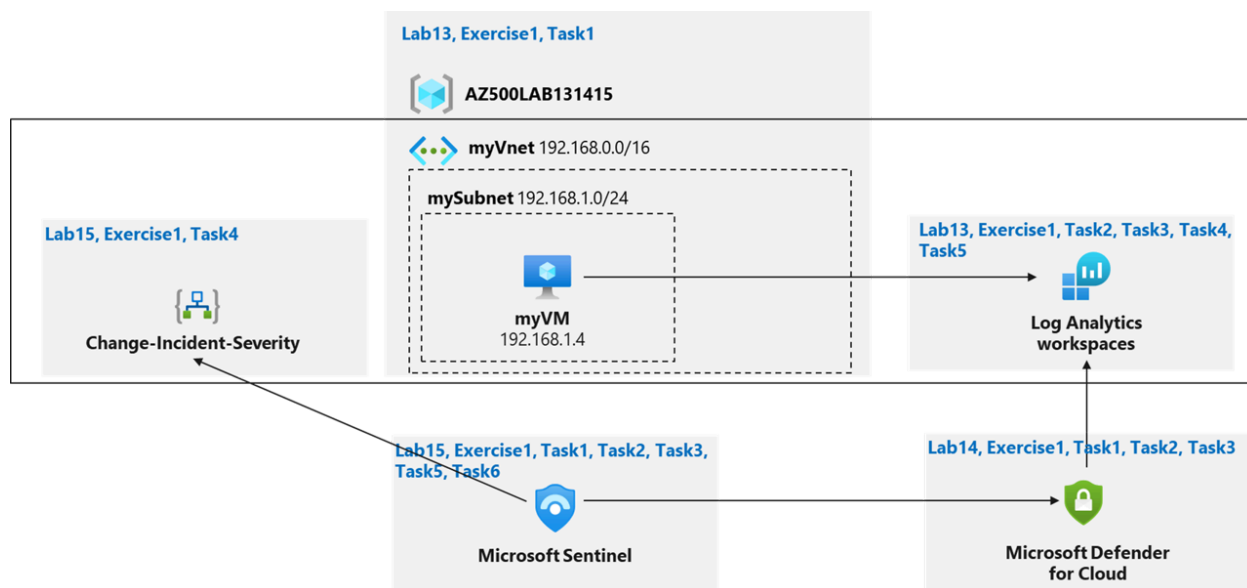
-
- In Microsoft Sentinel, a **playbook** is an automated workflow, built on **Azure Logic Apps** (a cloud-based platform for building automated workflows (Logic Apps) that integrate apps, data, services, and systems, enabling businesses to automate processes and orchestrate data across cloud/on-premise environments using visual designers and extensive connectors), that orchestrates response actions to security incidents or alerts, reducing manual effort by performing tasks like isolating a machine, blocking an account, or sending notifications, either automatically via an automation rule or manually on-demand. Playbooks use connectors to interact with Sentinel and other systems, offering powerful, customizable automation for Security Operations Centers (SOCs) to handle threats consistently and quickly.

Lab objectives

In this lab, you will complete the following exercise:

- Exercise 1: Implement Microsoft Sentinel

Microsoft Sentinel diagram



Instructions

Lab files:

- \\Allfiles\Labs\15\changeincidentseverity.json

Exercise 1: Implement Microsoft Sentinel

In this exercise, you will complete the following tasks:

- Task 1: On-board Microsoft Sentinel
- Task 2: Connect Azure Activity to Sentinel
- Task 3: Create a rule that uses the Azure Activity data connector.
- Task 4: Create a playbook
- Task 5: Create a custom alert and configure the playbook as an automated response.
- Task 6: Invoke an incident and review the associated actions.

Task 1: On-board Microsoft Sentinel

In this task, you will on-board Microsoft Sentinel and connect the Log Analytics workspace.

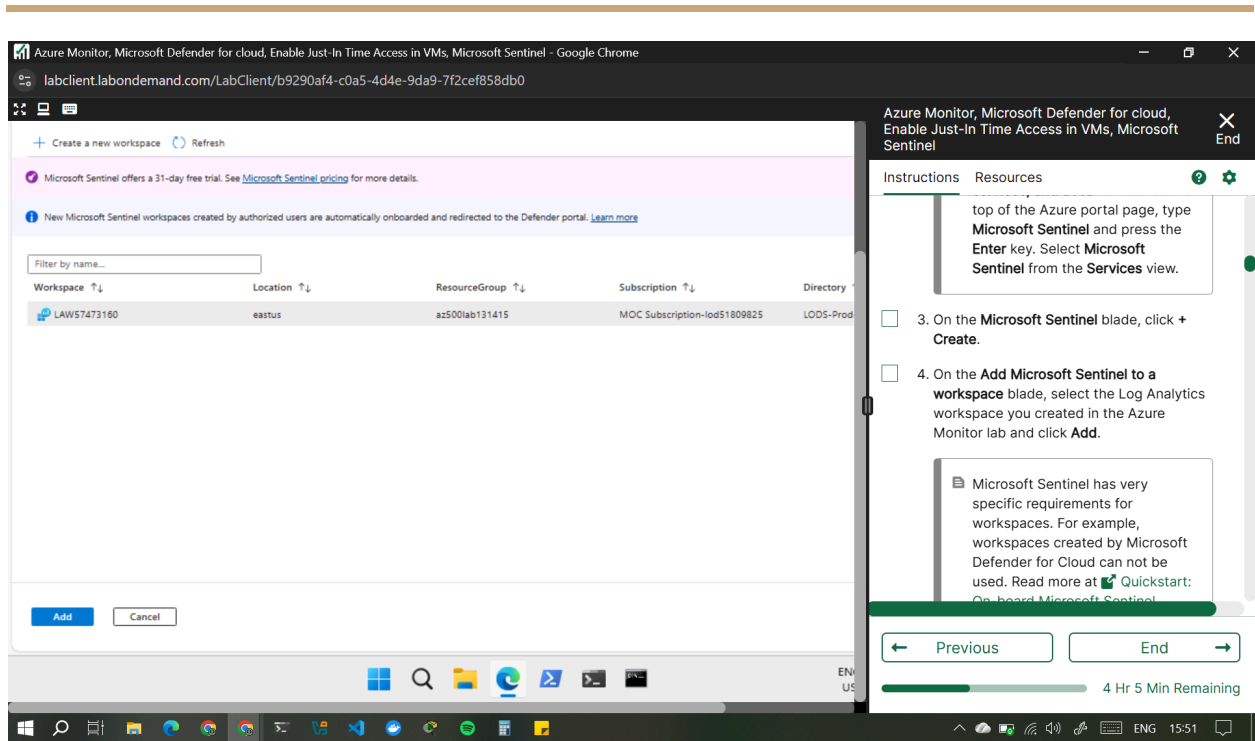
1. Sign-in to the Azure portal <https://portal.azure.com/>.
Sign in to the Azure portal using an account that has the Owner or Contributor role in the Azure subscription you are using for this lab. In this Cloudslice lab, this account is LabUser-57445941@LODSPRODMCA.onmicrosoft.com with TAP 9-A*LpfA.

2. In the Azure portal, in the Search resources, services, and docs text box at the top of the Azure portal page, type Microsoft Sentinel and press the Enter key.

If this is your first attempt to action Microsoft Sentinel in the Azure dashboard complete the following step(s): In the Azure portal, in the Search resources, services, and docs text box at the top of the Azure portal page, type Microsoft Sentinel and press the Enter key. Select Microsoft Sentinel from the Services view.

3. On the Microsoft Sentinel blade, click + Create.
4. On the Add Microsoft Sentinel to a workspace blade, select the Log Analytics workspace you created in the Azure Monitor lab and click Add.

Microsoft Sentinel has very specific requirements for workspaces. For example, workspaces created by Microsoft Defender for Cloud can not be used. Read more at [Quickstart: On-board Microsoft Sentinel](#)



Task 2: Configure Microsoft Sentinel to use the Azure Activity data connector.

In this task, you will configure Sentinel to use the Azure Activity data connector.

1. In the Azure portal, on the Microsoft Sentinel | Overview blade, in the Content management section, click Content hub.
2. On the Microsoft Sentinel | Content hub blade, review the list of available content.
3. Type Azure into the search bar and select the entry representing Azure Activity. Review its description at the far right, and then click Install.
4. Wait for the Install Success notification. In the left navigation panel, in the Configuration section, click Data connectors.

NB: Data connectors are software tools that act as bridges to automatically move, integrate, and synchronize data between different systems, applications, databases, or cloud services, enabling seamless data flow for unified analysis, reporting, and informed decision-making, eliminating manual effort and errors.

They extract data from sources (like CRMs, social media, files) and deliver it to a central destination (like a data warehouse or lake) for analysis.

The screenshot displays the Microsoft Sentinel Content hub interface. At the top, a navigation bar shows 'Add Microsoft Sentinel to a workspace' and 'Microsoft Sentinel'. Below this, a summary section displays statistics: 449 Solutions, 324 Standalone contents, 1 Installed, and 0 Updates. A search bar contains the text 'azure'. Below the search bar, a table lists search results for 'azure'.

Content title	Status	Content source	Provider	Support
Azure Cognitive Search	Not installed	Solution	Microsoft	Microsoft
Azure DDoS Protection	Not installed	Solution	Microsoft	Microsoft
Azure DDoS Protection Workbook	Not installed	Solution	Microsoft	Microsoft
DDoS Attack IP Addresses - Percent Thresh...	Not installed	Solution	Microsoft	Microsoft
DDoS Attack IP Addresses - PPS Threshold	Not installed	Solution	Microsoft	Microsoft

An 'Install Success' notification is visible in the top right corner, stating '1 item successfully installed.'.

On the right side, a sidebar titled 'Instructions' provides a list of steps:

2. On the **Microsoft Sentinel | Content hub** blade, review the list of available content.
3. Type **Azure** into the search bar and select the entry representing **Azure Activity**. Review its description at the far right, and then click **Install**.
4. Wait for the **Install Success** notification. In the left navigation panel, in the **Configuration** section, click **Data connectors**.

At the bottom of the sidebar, there are 'Previous' and 'End' buttons, and a progress bar indicating '4 Hours Remaining'.

The screenshot displays the Microsoft Sentinel 'Data connectors' blade. The left navigation pane includes sections like General, Threat management, Content management, and Configuration. The main area shows a list of connectors, with 'Azure Activity' (Microsoft) listed as 'Not connected (1)'. A sidebar on the right provides instructions for the next steps in the setup process.

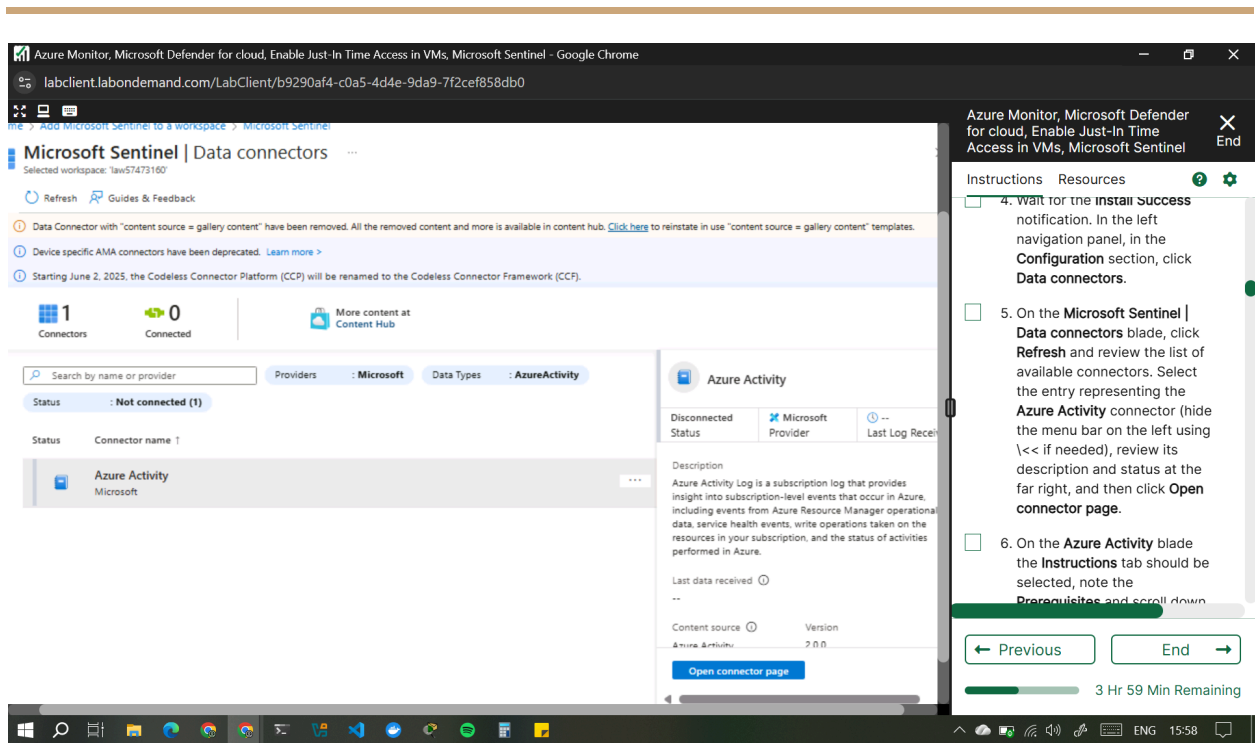
Instructions Resources

- 4. Wait for the **install Success** notification. In the left navigation panel, in the **Configuration** section, click **Data connectors**.
- 5. On the **Microsoft Sentinel | Data connectors** blade, click **Refresh** and review the list of available connectors. Select the entry representing the **Azure Activity** connector (hide the menu bar on the left using \<< if needed), review its description and status at the far right, and then click **Open connector page**.
- 6. On the **Azure Activity** blade the **Instructions** tab should be selected, note the **Prerequisites** and scroll down

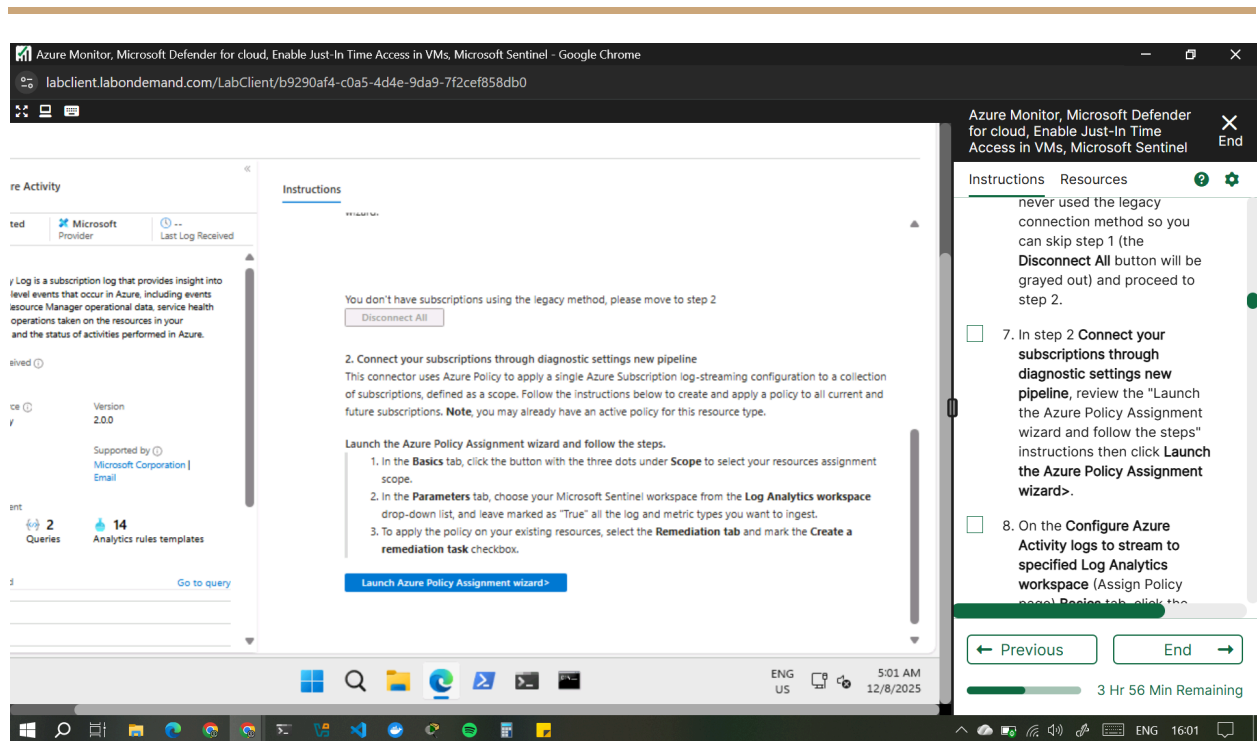
← Previous End →

4 Hours Remaining

5. On the Microsoft Sentinel | Data connectors blade, click Refresh and review the list of available connectors. Select the entry representing the Azure Activity connector (hide the menu bar on the left using \<< if needed), review its description and status at the far right, and then click Open connector page.

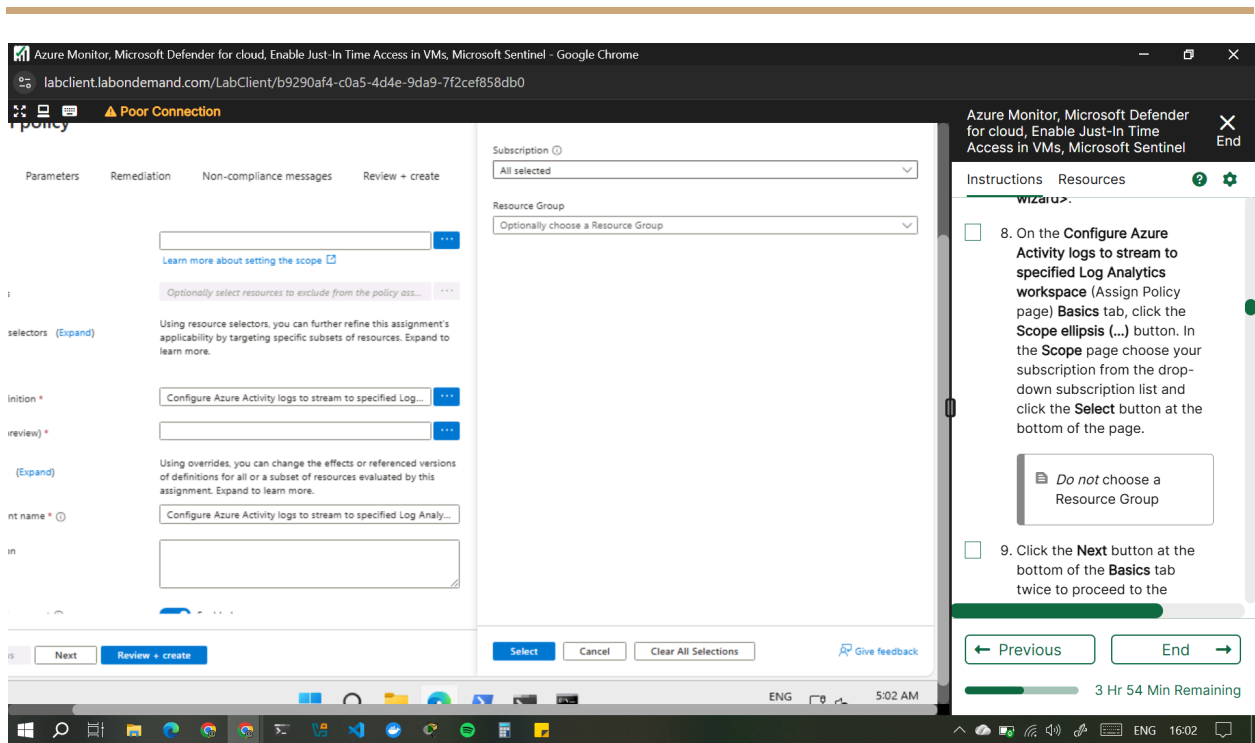


6. On the Azure Activity blade the Instructions tab should be selected, note the Prerequisites and scroll down to the Configuration. Take note of the information describing the connector update. Your subscription never used the legacy connection method so you can skip step 1 (the Disconnect All button will be grayed out) and proceed to step 2.
7. In step 2 Connect your subscriptions through diagnostic settings new pipeline, review the "Launch the Azure Policy Assignment wizard and follow the steps" instructions then click Launch the Azure Policy Assignment wizard>.

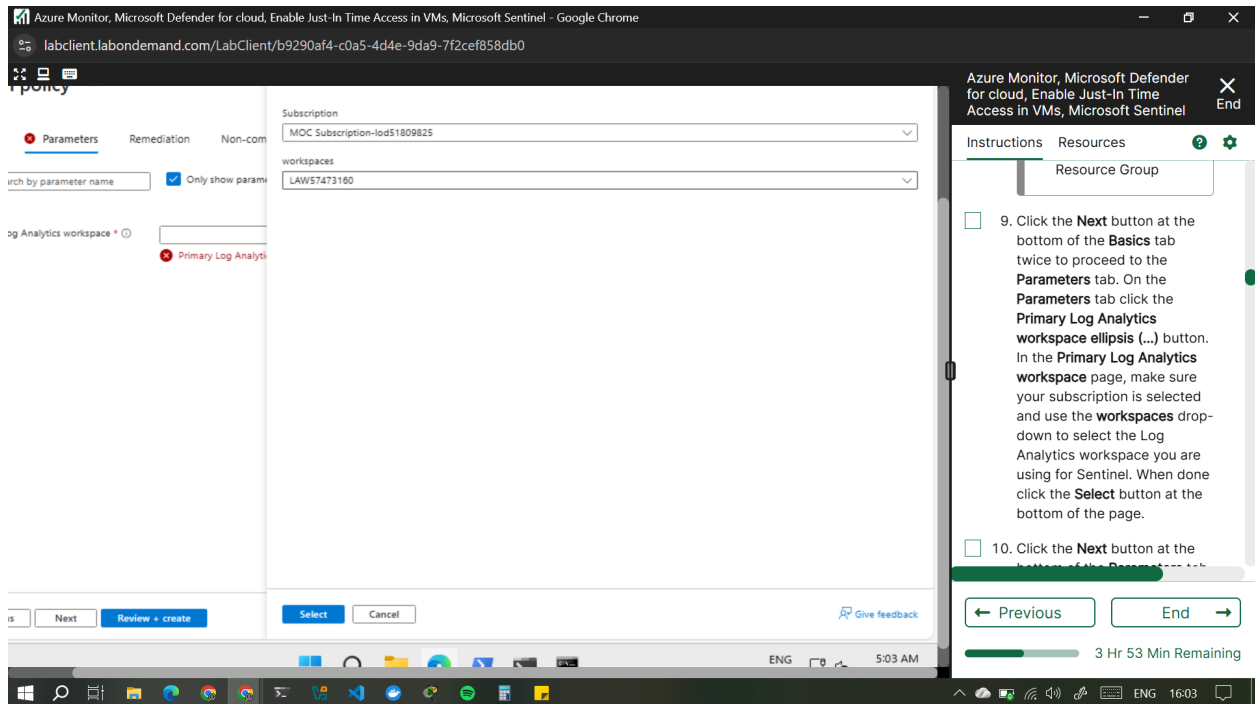


8. On the Configure Azure Activity logs to stream to specified Log Analytics workspace (Assign Policy page) Basics tab, click the Scope ellipsis (...) button. In the Scope page choose your subscription from the drop-down subscription list and click the Select button at the bottom of the page.

Do not choose a Resource Group



9. Click the Next button at the bottom of the Basics tab twice to proceed to the Parameters tab. On the Parameters tab click the Primary Log Analytics workspace ellipsis (...) button. In the Primary Log Analytics workspace page, make sure your subscription is selected and use the workspaces drop-down to select the Log Analytics workspace you are using for Sentinel. When done click the Select button at the bottom of the page.



10. Click the Next button at the bottom of the Parameters tab to proceed to the Remediation tab. On the Remediation tab select the Create a remediation task checkbox. This will enable the "Configure Azure Activity logs to stream to specified Log Analytics workspace" in the Policy to remediate drop-down. In the System assigned identity location drop-down, select the region (East US for example) you selected earlier for your Log Analytics workspace.
- **Azure Policy remediation** is the process of automatically fixing existing, non-compliant resources to meet defined policy standards, using effects like *Modify* or *DeployIfNotExists* to bring them into compliance, acting as an "auto-fix" for governance rules by applying changes to resources that don't match standards after assignment. It can be triggered manually or automatically when a policy is assigned and is essential for enforcing corporate governance at scale.

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome

labclient.labondemand.com/LabClient/b9290af4-c0a5-4d4e-9da9-7f2cef858db0

Assign policy

Basics Parameters **Remediation** Non-compliance messages Review + create

By default, this assignment will only take effect on newly created resources. Existing resources can be updated via a remediation task after the policy is assigned. For deploy/IfNotExists policies, the remediation task will deploy the specified template. For modify policies, the remediation task will edit tags on the existing resources.

☒ Create a remediation task

Policy to remediate Configure Azure Activity logs to stream to specified Log Analytics workspace

Managed Identity
Policies with the deploy/IfNotExists and modify effect types need the ability to deploy resources and edit tags on existing resources respectively. To do this, choose between an existing user assigned managed identity or creating a system assigned managed identity. [Learn more about Managed Identity.](#)

Create a Managed Identity ☒

Type of Managed Identity ☒ System assigned managed identity ☐ User assigned managed identity

System assigned identity location (US) East US

Permissions

Previous Next **Review + create**

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel

Instructions Resources

In the **Primary Log Analytics workspace** page, make sure your subscription is selected and use the **workspaces** drop-down to select the Log Analytics workspace you are using for Sentinel. When done click the **Select** button at the bottom of the page.

10. Click the **Next** button at the bottom of the **Parameters** tab to proceed to the **Remediation** tab. On the **Remediation** tab select the **Create a remediation task** checkbox. This will enable the "Configure Azure Activity logs to stream to specified Log Analytics workspace" in the **Policy to remediate** drop-down. In the **System assigned identity location** drop-down, select the region (East US for example) you selected earlier for your Log Analytics workspace.

Previous End

3 Hr 52 Min Remaining

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome

labclient.labondemand.com/LabClient/b9290af4-c0a5-4d4e-9da9-7f2cef858db0

Assign policy

Basics Parameters **Remediation** Non-compliance messages Review + create

☒ Create a remediation task

Policy to remediate Configure Azure Activity logs to stream to specified Log Analytics workspace

Managed Identity
Policies with the deploy/IfNotExists and modify effect types need the ability to deploy resources and edit tags on existing resources respectively. To do this, choose between an existing user assigned managed identity or creating a system assigned managed identity. [Learn more about Managed Identity.](#)

Create a Managed Identity ☒

Type of Managed Identity ☒ System assigned managed identity ☐ User assigned managed identity

System assigned identity location (US) East US

Permissions

This identity will also be given the following permissions: Monitoring Contributor, Log Analytics Contributor

Role assignments (permissions) are created based on the role definitions specified in the policies.

Previous Next **Review + create**

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel

Instructions Resources

This will enable the "Configure Azure Activity logs to stream to specified Log Analytics workspace" in the **Policy to remediate** drop-down. In the **System assigned identity location** drop-down, select the region (East US for example) you selected earlier for your Log Analytics workspace.

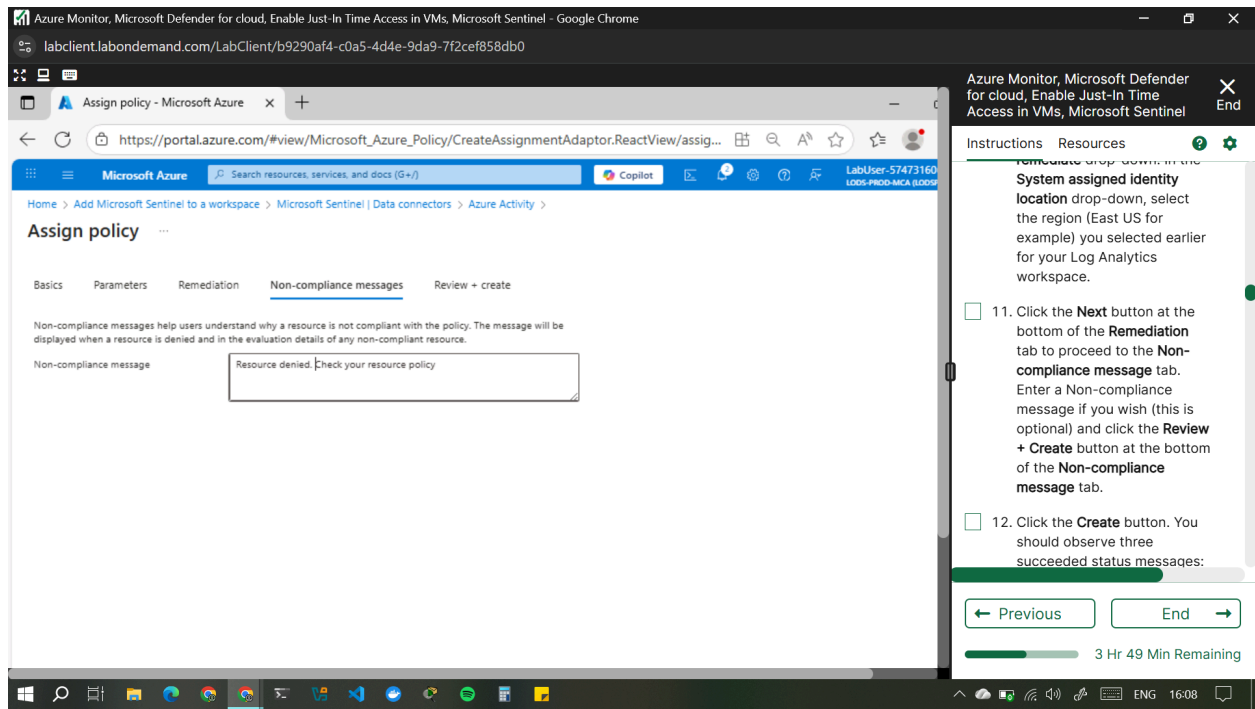
11. Click the **Next** button at the bottom of the **Remediation** tab to proceed to the **Non-compliance message** tab. Enter a Non-compliance message if you wish (this is optional) and click the **Review + Create** button at the bottom of the **Non-compliance** tab.

Previous End

3 Hr 51 Min Remaining

11. Click the Next button at the bottom of the Remediation tab to proceed to the Non-compliance message tab. Enter a Non-compliance message if you wish (this is optional) and click the

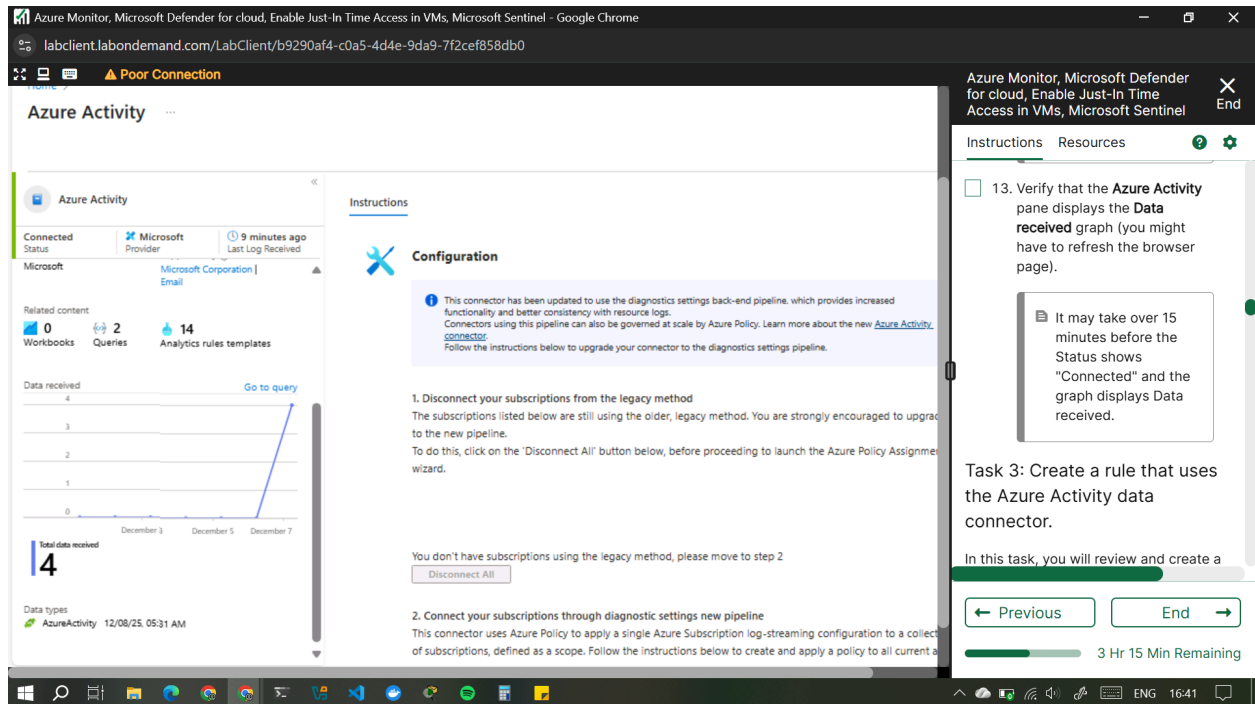
Review + Create button at the bottom of the Non-compliance message tab.



12. Click the Create button. You should observe three succeeded status messages: Creating policy assignment succeeded, Role Assignments creation succeeded, and Remediation task creation succeeded. You can check the Notifications, bell icon to verify the three successful tasks.

The screenshot displays the Azure Portal interface for Microsoft Sentinel. The main content area shows the 'Data Connectors' blade with instructions for connecting subscriptions. The 'Activity' pane on the left provides step-by-step guidance. The 'Notifications' pane in the center shows four successful events: 'Remediation task creation succeeded', 'Role Assignments creation succeeded', 'Creating policy assignment succeeded', and 'Install Success'. The 'Instructions' pane on the right shows step 12, which involves clicking the 'Create' button and observing three successful status messages. A progress bar at the bottom indicates '3 Hr 42 Min Remaining'.

13. Verify that the Azure Activity pane displays the Data received graph (you might have to refresh the browser page).
It may take over 15 minutes before the Status shows "Connected" and the graph displays Data received.



Task 3: Create a rule that uses the Azure Activity data connector.

In this task, you will review and create a rule that uses the Azure Activity data connector.

1. On the Microsoft Sentinel | Configuration blade, click Analytics.
2. On the Microsoft Sentinel | Analytics blade, click the Rule templates tab.

Review the types of rules you can create. Each rule is associated with a specific Data Source.

3. In the listing of rule templates, type Suspicious into the search bar form and click the Suspicious number of resource creation or deployment entry associated with the Azure Activity data source. And then, in the pane displaying the rule template properties, click Create rule (scroll to the right of the page if needed).

This rule has the **medium** severity.

Microsoft Sentinel | Analytics

Rules by severity: High (1) Medium (0) Low (0) Informational (0)

Active rules Rule templates Anomalies

Search: suspicious Add filter

Severity	Name	Rule type	Data sources	Tactics	Techniques	Sub techniques	Source name
Low	Suspicious Res...	Scheduled	Azure Activity	Impact	T1496		Azure Activity
Medium	Microsoft Entra...	Scheduled	Azure Activity	Cx +1	T1528 +1		Azure Activity
Medium	Suspicious num...	Scheduled	Azure Activity	Impact	T1496		Azure Activity
Medium	Suspicious gran...	Scheduled	Azure A... +1	Pq +1	T1098 +1		Azure Activity

Instructions: rules you can create. Each rule is associated with a specific Data Source.

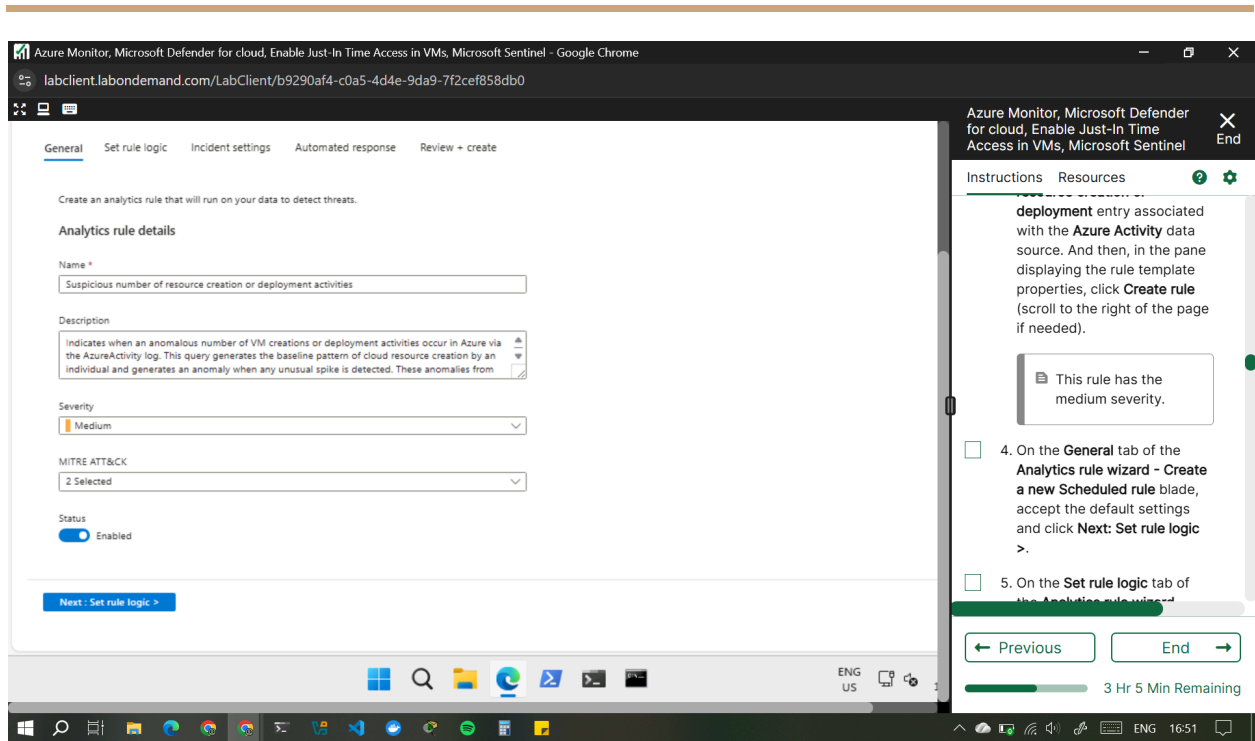
3. In the listing of rule templates, type **Suspicious** into the search bar form and click the **Suspicious number of resource creation or deployment** entry associated with the **Azure Activity** data source. And then, in the pane displaying the rule template properties, click **Create rule** (scroll to the right of the page if needed).

This rule has the medium severity.

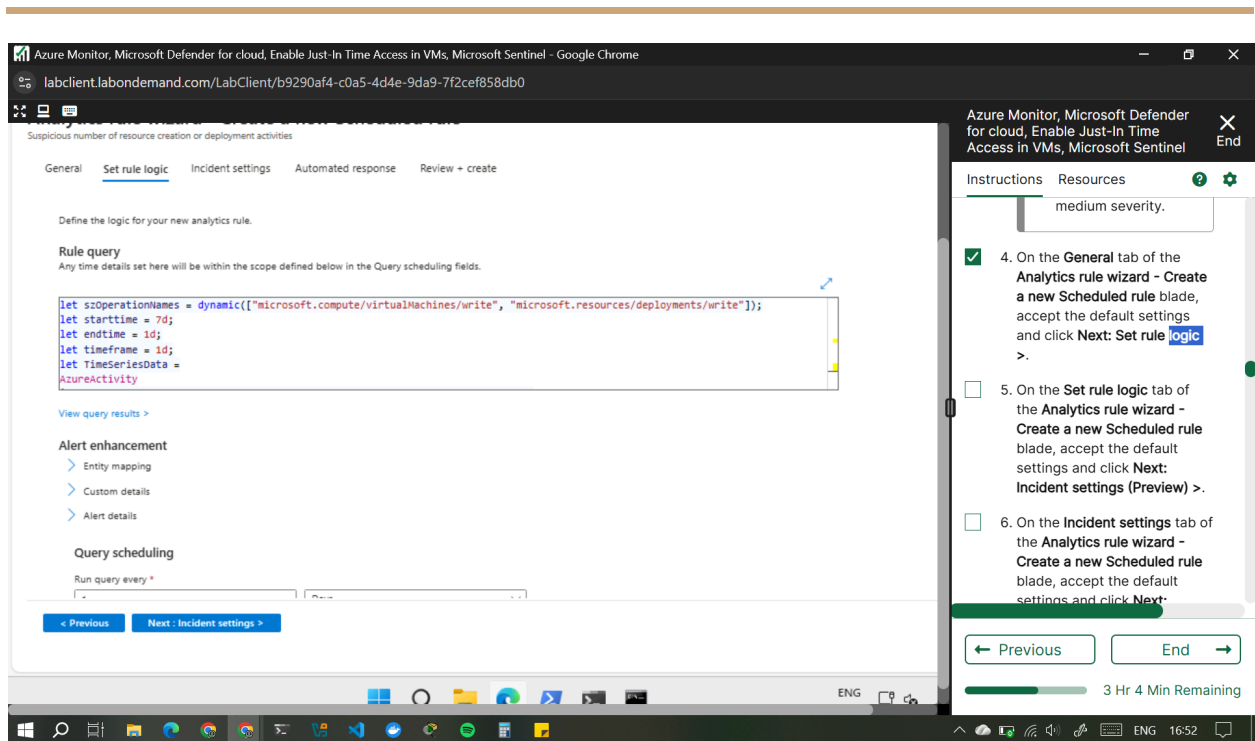
Previous End

3 Hr 6 Min Remaining

- On the General tab of the Analytics rule wizard - Create a new Scheduled rule blade, accept the default settings and click Next: Set rule logic >.

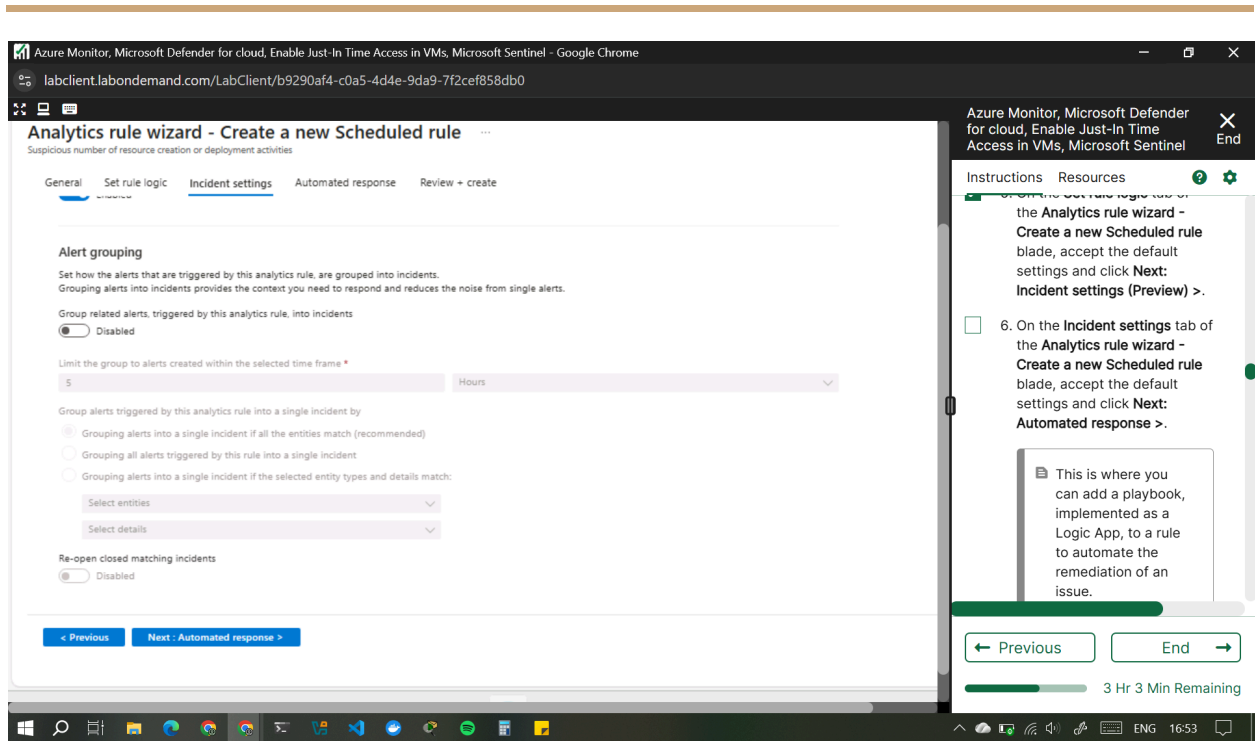


5. On the Set rule logic tab of the Analytics rule wizard - Create a new Scheduled rule blade, accept the default settings and click Next: Incident settings (Preview) >.



6. On the Incident settings tab of the Analytics rule wizard - Create a new Scheduled rule blade, accept the default settings and click Next: Automated response >.

NB: This is where you can add a playbook, implemented as a Logic App, to a rule to automate the remediation of an issue.



7. On the Automated response tab of the Analytics rule wizard - Create a new Scheduled rule blade, accept the default settings and click Next: Review and create >.
8. On the Review and create tab of the Analytics rule wizard - Create a new Scheduled rule blade, click Save.

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome

labclient.labondemand.com/LabClient/b9290af4-c0a5-4d4e-9da9-7f2cef858db0

Analytics rule wizard - Create a new Scheduled rule

Suspicious number of resource creation or deployment activities

Validation passed.

General Set rule logic Incident settings Automated response **Review + create**

Analytics rule details

Name: Suspicious number of resource creation or deployment activities

Description: Indicates when an anomalous number of VM creations or deployment activities occur in Azure via the AzureActivity log. This query generates the baseline pattern of cloud resource creation by an individual and generates an anomaly when any unusual spike is detected. These anomalies from unusual or privileged users could be an indication of a cloud infrastructure takeover by an adversary.

MITRE ATT&CK: > Impact (I)

Severity: Medium

Status: Enabled

Analytics rule settings

Rule query: let szOperationNames = dynamic(["microsoft.compute/virtualmachines/write", "microsoft.resources/deployments/write"]); let starttime = 7d; let endtime = 1d; let timeframe = 1d; let TimeSeriesData = AzureActivity | where TimeGenerated between (startofday(agot(starttime)) .. startofday(now())) | where OperationNameValue in~ (szOperationNames) | project TimeGenerated, Caller | make-series Total = count() on TimeGenerated from startofday(agot(starttime)) to startofday(now()) step timeframe by Caller: TimeSeriesData | extend (anomalies, score, baseline) = series_decompose_anomalies(Total, 3, -1, "linefit") | mv-expand Total to typeof(double), TimeGenerated to typeof(datetime), anomalies to typeof(double), score to typeof(double), baseline to typeof(long) | where TimeGenerated >= startofday(agot(endtime)) | where anomalies > 0 and baseline > 0 | project Caller, TimeGenerated, Total, baseline, anomalies, score | join (AzureActivity | where TimeGenerated > startofday(agot(endtime)) | where OperationNameValue in~ (szOperationNames) | summarize make_set(OperationNameValue, 100), make_set(ResourceId, 100)) make_set(CallerIpAddress, 100) by bin(TimeGenerated, timeframe), Caller | mv-expand CallerIpAddress=set_CallerIpAddress | project-away Caller1 | extend Name = if(Caller has '@' tostring(split(Caller, '@')[0]), "") | extend UPNSuffix = if(Caller has '@' tostring(split(Caller, '@')[1][0]), "") | extend AadUserId = if(Caller has '@' tostring(split(Caller, '@')[1][0]), "") | extend AadUserId = if(Caller has '@' tostring(split(Caller, '@')[1][0]), "")

Rule frequency: Run query every 1 day

< Previous Save

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel

Instructions Resources

WIZARD - Create a new Scheduled rule blade, accept the default settings and click Next: Review and create >.

8. On the **Review and create** tab of the **Analytics rule wizard - Create a new Scheduled rule** blade, click **Save**.

You now have an active rule.

Task 4: Create a playbook

In this task, you will create a playbook. A security playbook is a collection of tasks that can be invoked by Microsoft Sentinel in response to an alert.

Previous End

3 Hr 2 Min Remaining

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome

labclient.labondemand.com/LabClient/b9290af4-c0a5-4d4e-9da9-7f2cef858db0

Analytics rule wizard - Create a new Scheduled rule

Suspicious number of resource creation or deployment activities

Validation passed.

General Set rule logic Incident settings Automated response **Review + create**

Suppression: Not configured

Entity mapping

Entity 1: Account
Identifier: FullName, Value: Caller
Identifier: UPNSuffix, Value: UPNSuffix

Entity 2: Account
Identifier: AadUserId, Value: AadUserId

Entity 3: IP
Identifier: Address, Value: CallerIpAddress

Custom details: Not configured

Alert details: Not configured

Incident settings

Create incidents from this rule: Enabled

Alert grouping: Disabled

Automated response

Automation rules: Not configured

< Previous Save

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel

Instructions Resources

WIZARD - Create a new Scheduled rule blade, accept the default settings and click Next: Review and create >.

8. On the **Review and create** tab of the **Analytics rule wizard - Create a new Scheduled rule** blade, click **Save**.

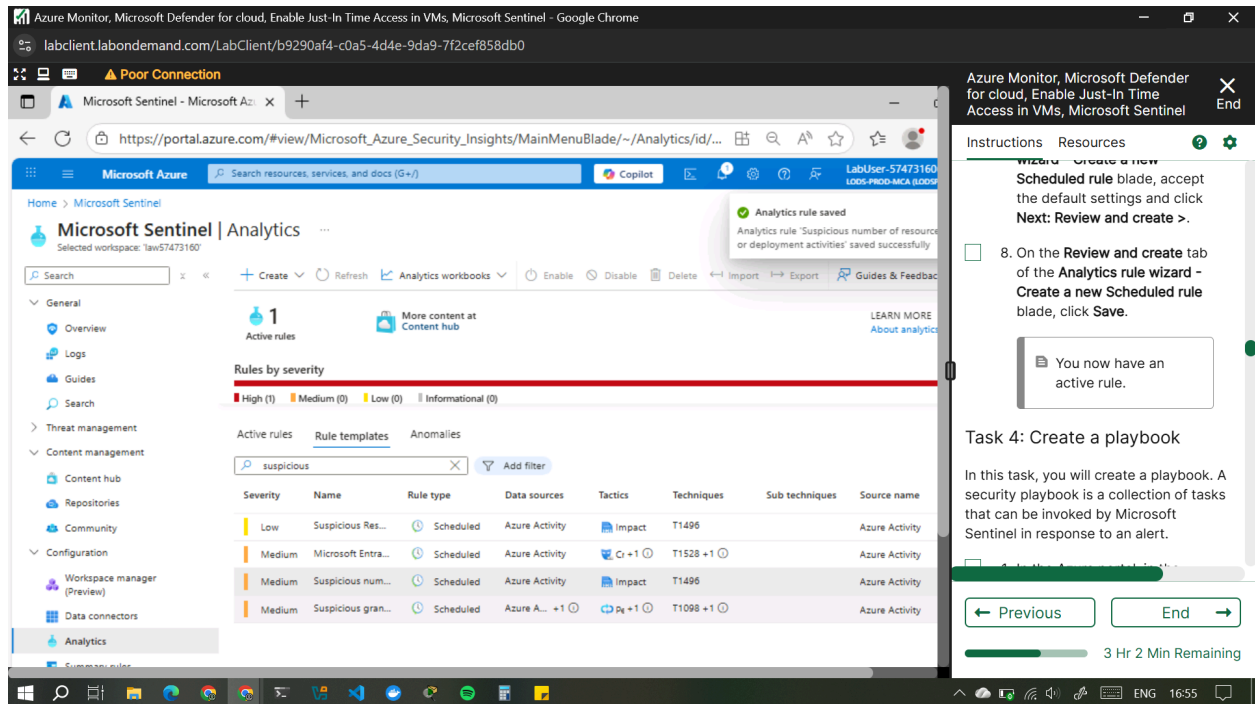
You now have an active rule.

Task 4: Create a playbook

In this task, you will create a playbook. A security playbook is a collection of tasks that can be invoked by Microsoft Sentinel in response to an alert.

Previous End

3 Hr 2 Min Remaining

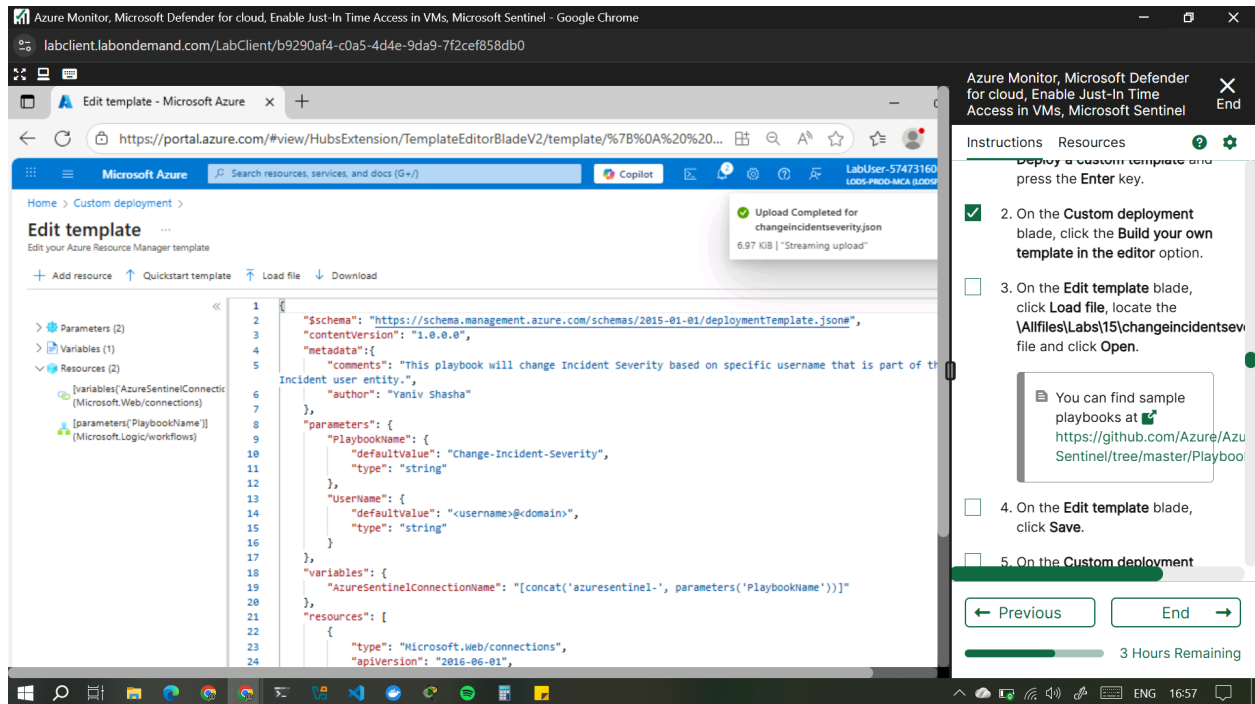


You now have an active rule.

Task 4: Create a playbook

In this task, you will create a playbook. A security playbook is a collection of tasks that can be invoked by Microsoft Sentinel in response to an alert.

1. In the Azure portal, in the Search resources, services, and docs text box at the top of the Azure portal page, type Deploy a custom template and press the Enter key.
2. On the Custom deployment blade, click the Build your own template in the editor option.
3. On the Edit template blade, click Load file, locate the \\Allfiles\\Labs\\15\\changeincidentseverity.json file and click Open.
You can find sample playbooks at <https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks>.



4. On the Edit template blade, click Save.
5. On the Custom deployment blade, ensure that the following settings are configured (leave any others with their default values):

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	AZ500LAB131415
Location	(US) East US
Playbook Name	Change-Incident-Severity

User Name your email address

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome

labclient.labondemand.com/LabClient/b9290af4-c0a5-4d4e-9da9-7f2cef858db0

Custom deployment

Deploy from a custom template

Can I deploy multiple resources within a single ARM template? Generate a Powershell script to deploy a resource +1

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

Select a template Basics Review + create

Template

Customized template of 2 resources

Edit template Edit parameters Visualize

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ MOC Subscription-Iod51809825

Resource group * ⓘ AZ500LAB131415 [Create new](#)

Instance details

Region * ⓘ (US) East US ✓

Playbook Name Change-Incident-Severity ✓

User Name LabUser-S7473160@L0D5PROD/MCA.onmicrosoft.com ✓

Previous Next Review + create

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel

Instructions Resources

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	AZ500LAB131415
Location	(US) East US
Playbook Name	Change-Incident-Severity
User Name	your email address

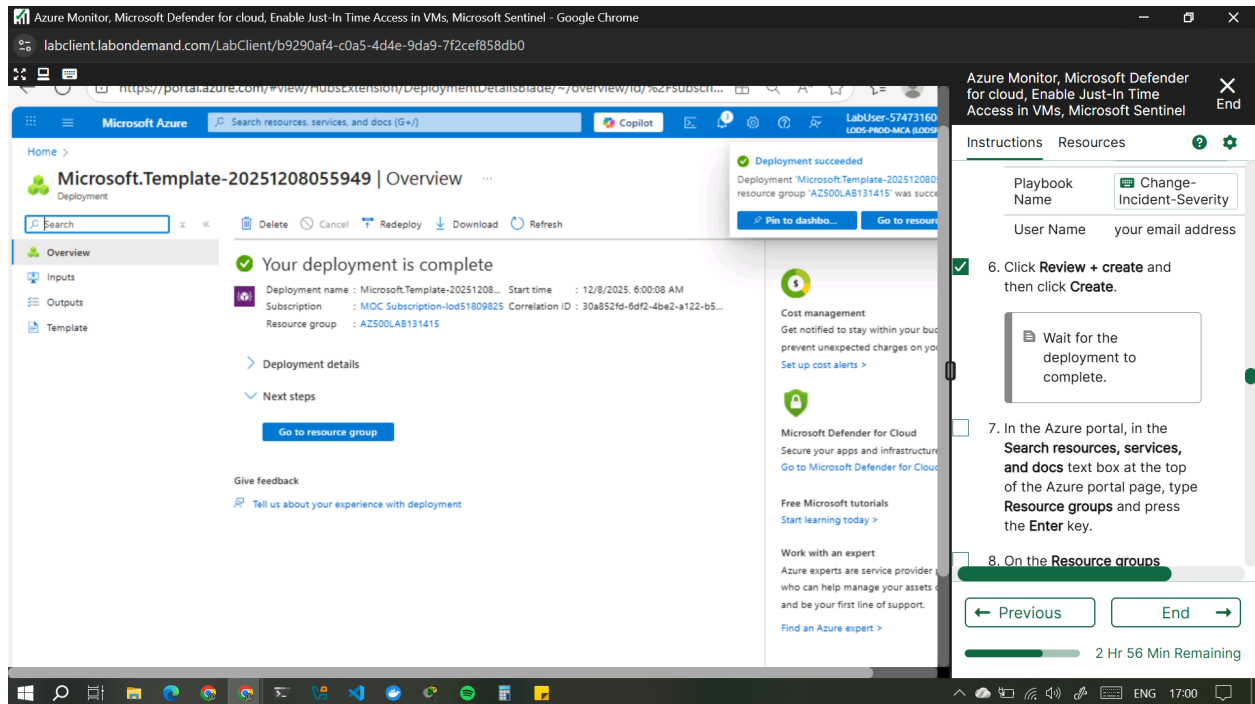
6. Click **Review + create** and then click **Create**.

Wait for the deployment to

← Previous End →

2 Hr 58 Min Remaining

6. Click Review + create and then click Create.
Wait for the deployment to complete.



7. In the Azure portal, in the Search resources, services, and docs text box at the top of the Azure portal page, type Resource groups and press the Enter key.
8. On the Resource groups blade, in the list of resource group, click the AZ500LAB131415 entry.
9. On the AZ500LAB131415 resource group blade, in the list of resources, click the entry representing the newly created Change-Incident-Severity logic app.
10. On the Change-Incident-Severity blade, click Edit.
On the Logic Apps Designer blade, each of the four s displays a warning. This means that each needs to reviewed and configured.
11. On the Logic Apps Designer blade, click the first s step.
12. Click Change connection, then Add new, ensure that the entry in the Tenant drop down list contains your Azure AD tenant name and click Sign-in.
13. When prompted, sign in with the user account that has the Owner or Contributor role in the Azure subscription you are using for this lab.

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome

labclient.labondemand.com/LabClient/b9290af4-c0a5-4d4e-9da9-7f2cef858db0

Microsoft Azure Search resources, services, and docs (G+)

LabUser-57473160@LO... LODS-PROD-MCA (LODSPROD...

Resource Manager | Resource groups > AZ500LAB131415 > Change-Incident-Severity >

je-Incident-Severity

Save Discard Parameters Code view Connections Errors Info

Create connection

When a response to an Azure Sentinel alert is triggered

Create a new connection

Authentication * OAuth

Tenant ID * LODS-Prod-MCA

Sign in to create a connection to Microsoft Sentinel.

Sign in Cancel

Instructions Resources

On the **Logic Apps Designer** blade, each of the four s displays a warning. This means that each needs to reviewed and configured.

11. On the **Logic Apps Designer** blade, click the first s step.
12. Click **Change connection**, then **Add new**, ensure that the entry in the **Tenant** drop down list contains your Azure AD tenant name and click **Sign-in**.
13. When prompted, sign in with the user account that has the Owner or Contributor role in

Previous End

2 Hr 53 Min Remaining

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome

labclient.labondemand.com/LabClient/b9290af4-c0a5-4d4e-9da9-7f2cef858db0

Save Discard Parameters Code view Connections Errors Info

Alert - Get incident

Invalid connection. To load...

Alert - Get accounts

Invalid connection. To load...

Change Incident severity 2

Change incident severity 2

Parameters Settings Code view Testing About

Specify subscription id * Subscription ID x

Specify resource group * Resource group x

Specify workspace id * Workspace ID x

Identifier * Incident

Specify alert / incident * Number x

Specify severity * High

Connected to LabUser-57473160@LODSPROD.MCA.onmicrosoft.com. Change connection

Instructions Resources

needs to reviewed and configured.

11. On the **Logic Apps Designer** blade, click the first s step.
12. Click **Change connection**, then **Add new**, ensure that the entry in the **Tenant** drop down list contains your Azure AD tenant name and click **Sign-in**.
13. When prompted, sign in with the user account that has the Owner or Contributor role in the Azure subscription you are using for this lab.
14. Click the second s step and, in the list of s, select the second entry, representing the you created in the previous step.

Previous End

2 Hr 50 Min Remaining

14. Click the second s step and, in the list of s, select the second entry, representing the you created in the previous step.

15. Repeat the previous step for the remaining two s steps.
- Ensure there are no warnings displayed on any of the steps.
16. On the Logic Apps Designer blade, click Save to save your changes.

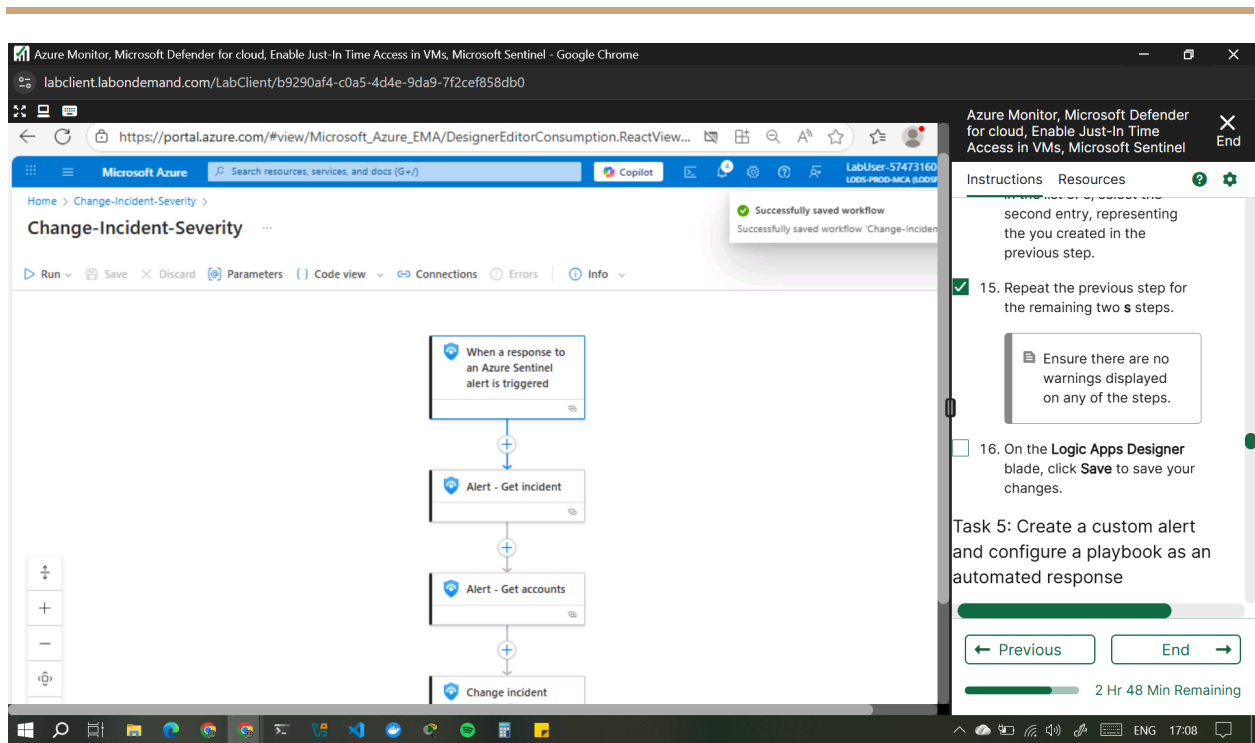
The screenshot displays the Azure Logic Apps Designer interface. The main workspace shows a workflow with the following steps:

- When a response to an Azure Sentinel alert is triggered
- Alert - Get incident
- Alert - Get accounts
- Change incident severity 2

The right-hand pane contains instructions for the workflow steps:

- 12. Click **Change connection**, then **Add new**, ensure that the entry in the **Tenant** drop down list contains your Azure AD tenant name and click **Sign-in**.
- 13. When prompted, sign in with the user account that has the Owner or Contributor role in the Azure subscription you are using for this lab.
- 14. Click the second s step and, in the list of s, select the second entry, representing the you created in the previous step.
- 15. Repeat the previous step for the remaining two s steps

At the bottom of the right-hand pane, there are buttons for **Previous** and **End**, and a progress bar indicating **2 Hr 49 Min Remaining**.

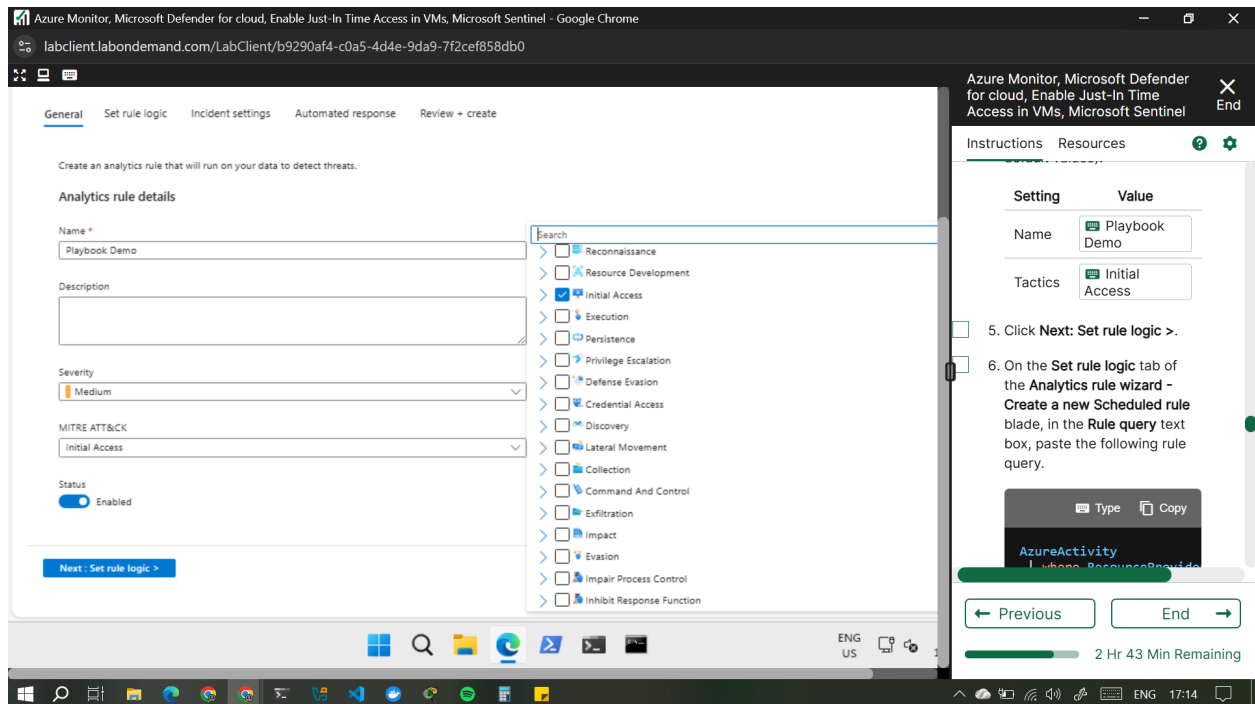


Task 5: Create a custom alert and configure a playbook as an automated response

1. In the Azure portal, navigate back to the Microsoft Sentinel | Overview blade.
2. On the the Microsoft Sentinel | Overview blade, in the Configuration section, click Analytics.
3. On the Microsoft Sentinel | Analytics blade, click + Create and, in the drop-down menu, click Scheduled query rule.
4. On the General tab of the Analytics rule wizard - Create a new Scheduled rule blade, specify the following settings (leave others with their default values):

Setting	Value
Name	Playbook Demo
Tactics	Initial Access

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally accessible knowledge base, framework, and matrix that details cyber adversary behaviors, including their tactics (goals like "Initial Access," "Execution") and specific techniques (methods like "Phishing," "Credential Dumping") used in real-world attacks, providing a common language for defenders to understand, map, detect, and mitigate threats across enterprise, mobile, cloud, and ICS environments



5. Click Next: Set rule logic >.
6. On the Set rule logic tab of the Analytics rule wizard - Create a new Scheduled rule blade, in the Rule query text box, paste the following rule query.

AzureActivity

| where ResourceProviderValue =~ "Microsoft.Security"

| where OperationNameValue =~
"Microsoft.Security/locations/jitNetworkAccessPolicies/delete"

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome

labclient.labondemand.com/LabClient/b9290af4-c0a5-4d4e-9da9-7f2cef858db0

Analytics rule wizard - Create a new Scheduled rule

General Set rule logic Incident settings Automated response Review + create

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
AzureActivity
| where ResourceProviderValue =~ "Microsoft.Security"
| where OperationNameValue =~ "Microsoft.Security/locations/jitNetworkAccessPolicies/delete"
```

View query results >

Alert enhancement

- Entity mapping
- Custom details

Here you can surface particular event parameters and their values in alerts that comprise those events, by adding key-value pairs below. In the Key field, enter a name of your choosing that will appear as the field name in alerts. In the Value field, choose the event parameter you wish to surface in the alerts from the drop-down list. [Learn more >](#)

Instructions Resources

Create a new Scheduled rule blade, in the Query scheduling section, set the Run query every to 5 Minutes.

8. On the Set rule logic tab of the Analytics rule wizard - Create a new Scheduled rule blade, accept the default values of the remaining settings and click Next: Incident settings >.

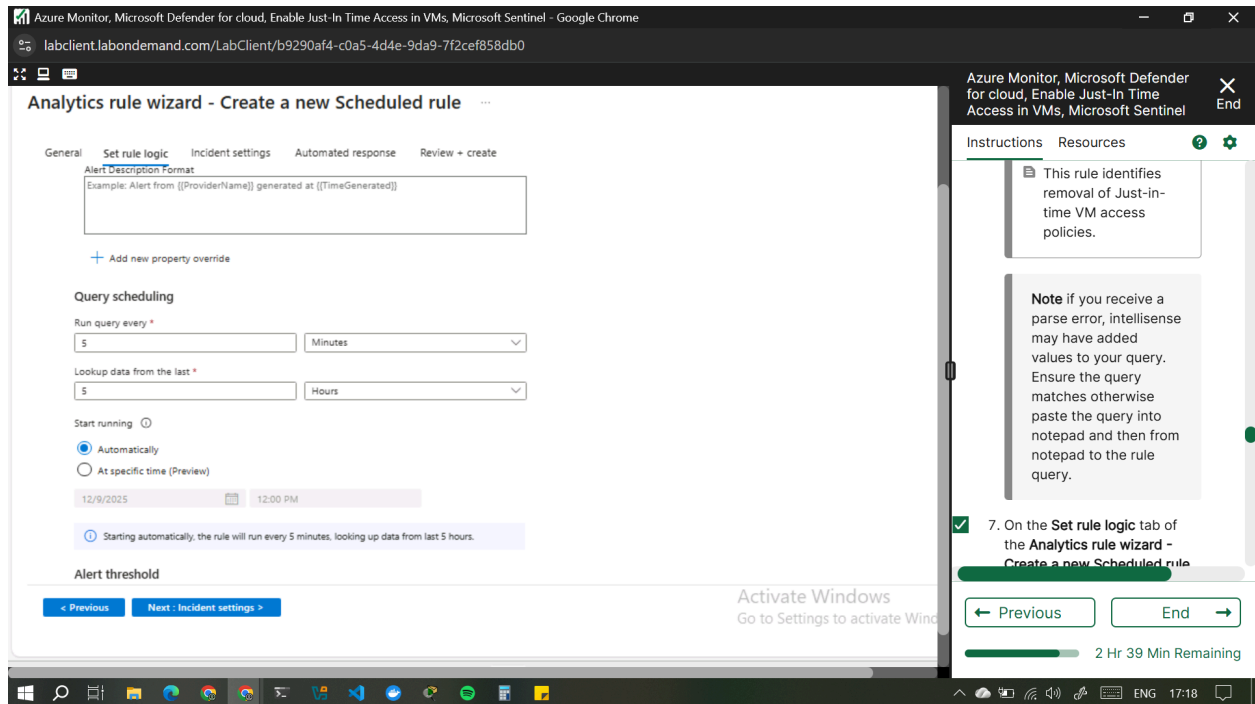
9. On the Incident settings tab of the Analytics rule wizard - Create a new Scheduled rule blade, accept the default settings and click Next: Automated response >.

10. On the Automated response

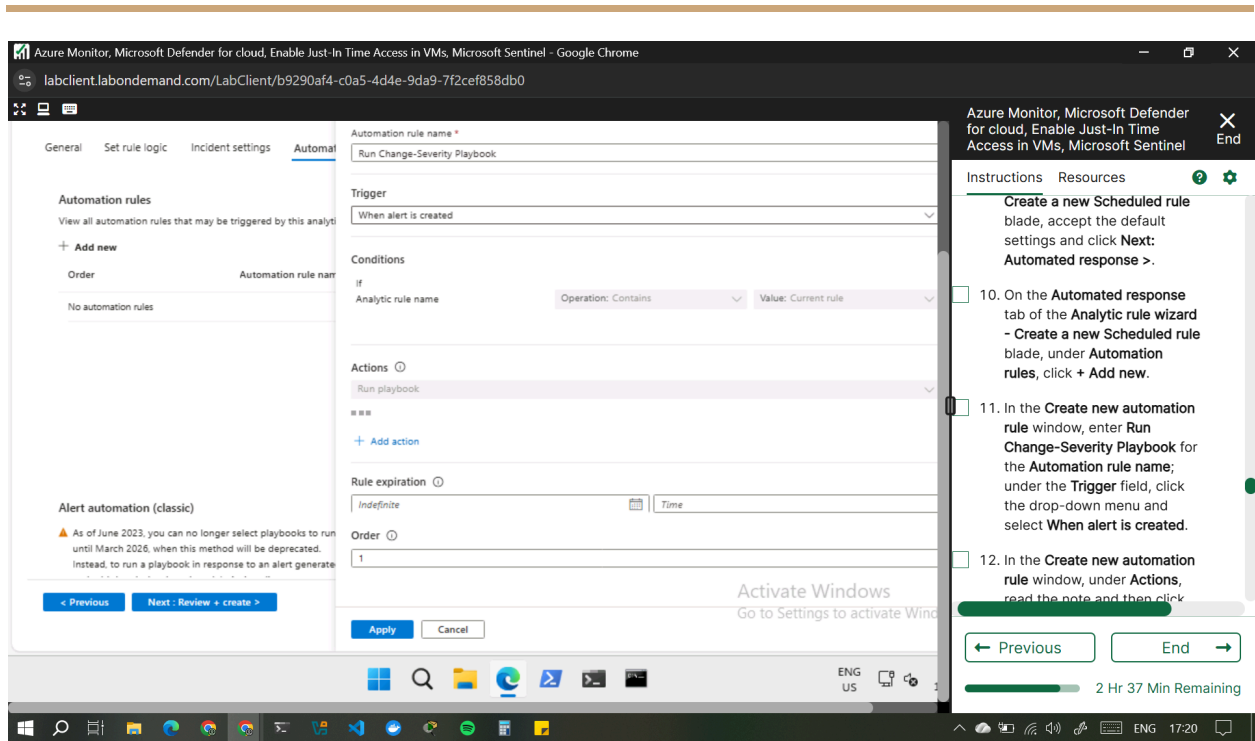
Previous End

2 Hr 40 Min Remaining

7. This rule identifies removal of Just-in-time VM access policies.
Note if you receive a parse error, intellisense may have added values to your query. Ensure the query matches otherwise paste the query into notepad and then from notepad to the rule query.
8. On the Set rule logic tab of the Analytics rule wizard - Create a new Scheduled rule blade, in the Query scheduling section, set the Run query every to 5 Minutes.



9. On the Set rule logic tab of the Analytics rule wizard - Create a new Scheduled rule blade, accept the default values of the remaining settings and click Next: Incident settings >.
10. On the Incident settings tab of the Analytics rule wizard - Create a new Scheduled rule blade, accept the default settings and click Next: Automated response >.
11. On the Automated response tab of the Analytic rule wizard - Create a new Scheduled rule blade, under Automation rules, click + Add new.
12. In the Create new automation rule window, enter Run Change-Severity Playbook for the Automation rule name; under the Trigger field, click the drop-down menu and select When alert is created.



13. In the Create new automation rule window, under Actions, read the note and then click Manage playbook permissions. On the Manage permissions window, select the checkbox next to the previously created Resource group AZ500LAB1314151 and then click Apply.

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome

labclient.labondemand.com/LabClient/b9290af4-c0a5-4d4e-9da9-7f2cef858db0

https://portal.azure.com/#view/Microsoft_Azure_Security_Insights/RuleEditor.ReactView/subsc...

Microsoft Azure Search resources, services, and docs (G+/) Copilot LabUser-57473160 LOGS-PROD-MICA (ECON)

Analytics rule wizard - Create a new

General Set rule logic Incident settings Automate

Automation rules

View all automation rules that may be triggered by this analysis

+ Add new

Order Automation rule name

No automation rules

Alert automation (classic)

As of June 2023, you can no longer select playbooks to run until March 2026, when this method will be deprecated. Instead, to run a playbook in response to an alert generate

Manage permissions

Choose the resource groups that contain the playbooks you want to give Microsoft Sentinel permissions to run

Browse Current permissions

Search All subscriptions selected

☐	Name	Subscription	Permissions
☒	AZ500LAB131415	MOC Subscription-lod51809825	
☐	NetworkWatcherRG	MOC Subscription-lod51809825	

Apply Cancel

Instructions

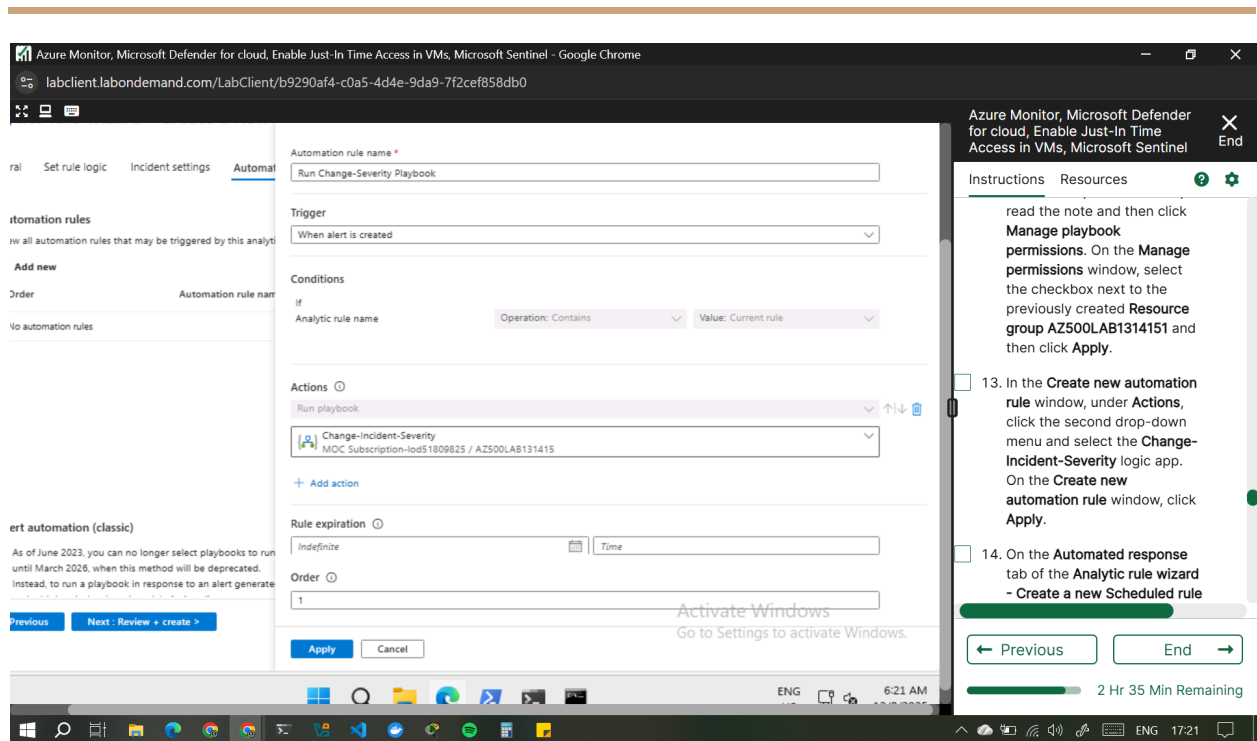
Resources

11. In the **Create new automation rule** window, enter **Run Change-Severity Playbook** for the **Automation rule name**; under the **Trigger** field, click the drop-down menu and select **When alert is created**.
12. In the **Create new automation rule** window, under **Actions**, read the note and then click **Manage playbook permissions**. On the **Manage permissions** window, select the checkbox next to the previously created **Resource group AZ500LAB131415** and then click **Apply**.
13. In the **Create new automation rule** window, under **Actions**.

← Previous End →

2 Hr 36 Min Remaining

14. In the Create new automation rule window, under Actions, click the second drop-down menu and select the Change-Incident-Severity logic app. On the Create new automation rule window, click Apply.



15. On the Automated response tab of the Analytic rule wizard - Create a new Scheduled rule blade, click Next: Review and create > and click Save

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome

labclient.labondemand.com/LabClient/b9290af4-c0a5-4d4e-9da9-7f2cef858db0

Analytics rule wizard - Create a new Scheduled rule

General Set rule logic Incident settings **Automated response** Review + create

Automation rules
View all automation rules that may be triggered by this analytics rule and create new automation rules.

+ Add new

Order	Automation rule name	Trigger	Action	Status
1	Run Change-Severity Playbook	Alert created	Run playbook 'Change-Incident-...	Enabled

Alert automation (classic)
As of June 2023, you can no longer select playbooks to run directly from an analytics rule by adding it to the following list. Playbooks already in the list will continue to run until March 2026, when this method will be deprecated. Instead, to run a playbook in response to an alert generated by this analytics rule, create an Automation rule (see above), choose "When alert is created" as the rule's trigger.

< Previous Next: Review + create >

Activate Windows
Go to Settings to activate Windows

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel

Instructions Resources

- Create a new Scheduled rule blade, click **Next: Review and create >** and click **Save**

You now have a new active rule called **Playbook Demo**. If an event identified by the rule logic occurs, it will result in a medium severity alert, which will generate a corresponding incident.

Task 6: Invoke an incident and review the associated actions.

< Previous End >

2 Hr 35 Min Remaining

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome

labclient.labondemand.com/LabClient/b9290af4-c0a5-4d4e-9da9-7f2cef858db0

Analytics rule wizard - Create a new Scheduled rule

General Set rule logic Incident settings Automated response **Review + create**

Validation passed.

Analytics rule details

Name	Playbook Demo
Description	
MITRE ATT&CK	Initial Access
Severity	Medium
Status	Enabled

Analytics rule settings

Rule query	AzureActivity where ResourceProviderValue == "Microsoft.Security" where OperationNameValue == "Microsoft.Security/locations/JitNetworkAccessPolicies/delete"
Rule frequency	Run query every 5 minutes
Rule period	Last 5 hours data
Rule start time	Automatic
Rule threshold	Trigger alert if query returns more than 0 results
Event grouping	Group all events into a single alert

< Previous Save

Activate Windows
Go to Settings to activate Windows

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel

Instructions Resources

- Create a new Scheduled rule blade, click **Next: Review and create >** and click **Save**

You now have a new active rule called **Playbook Demo**. If an event identified by the rule logic occurs, it will result in a medium severity alert, which will generate a corresponding incident.

Task 6: Invoke an incident and review the associated actions.

< Previous End >

2 Hr 35 Min Remaining

You now have a new active rule called Playbook Demo. If an event identified by

the rule logic occurs, it will result in a medium severity alert, which will generate a corresponding incident.

Microsoft Sentinel | Analytics

Rules by severity

Active rules

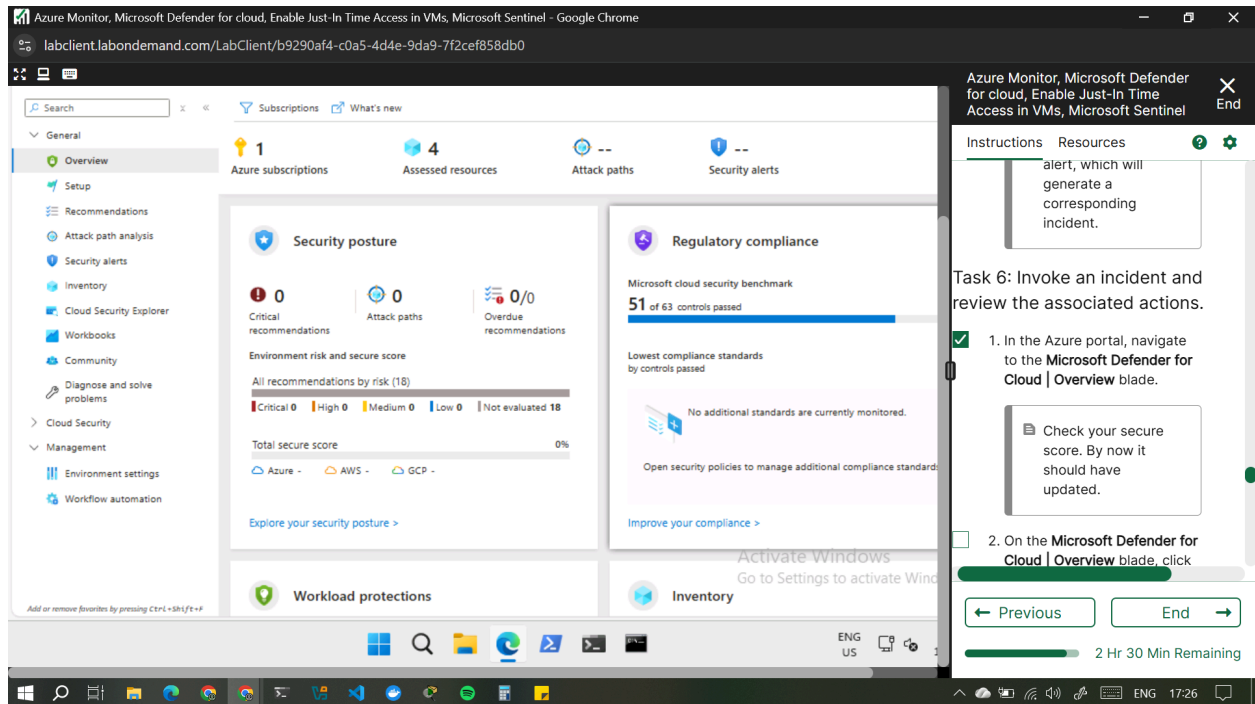
Severity	Name	Rule T...	Status	Tactics	Techniques	Sub techniques	Source
Medium	Playbook Demo	S...	Enabled	Initial Access			
Medium	Suspicious num...	S...	Enabled	Impact	T1496		
High	Advanced Multi...	F...	Enabled	Colle +11			

Task 6: Invoke an incident and review the associated actions.

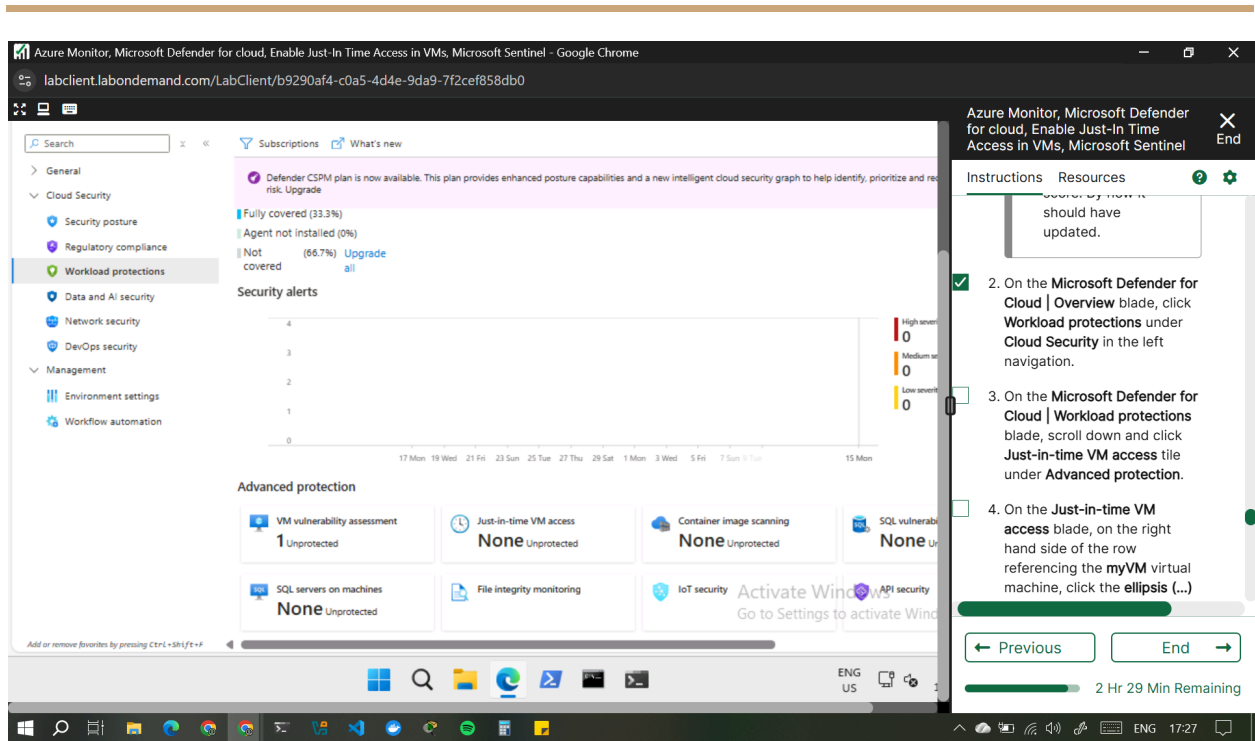
2 Hr 34 Min Remaining

Task 6: Invoke an incident and review the associated actions.

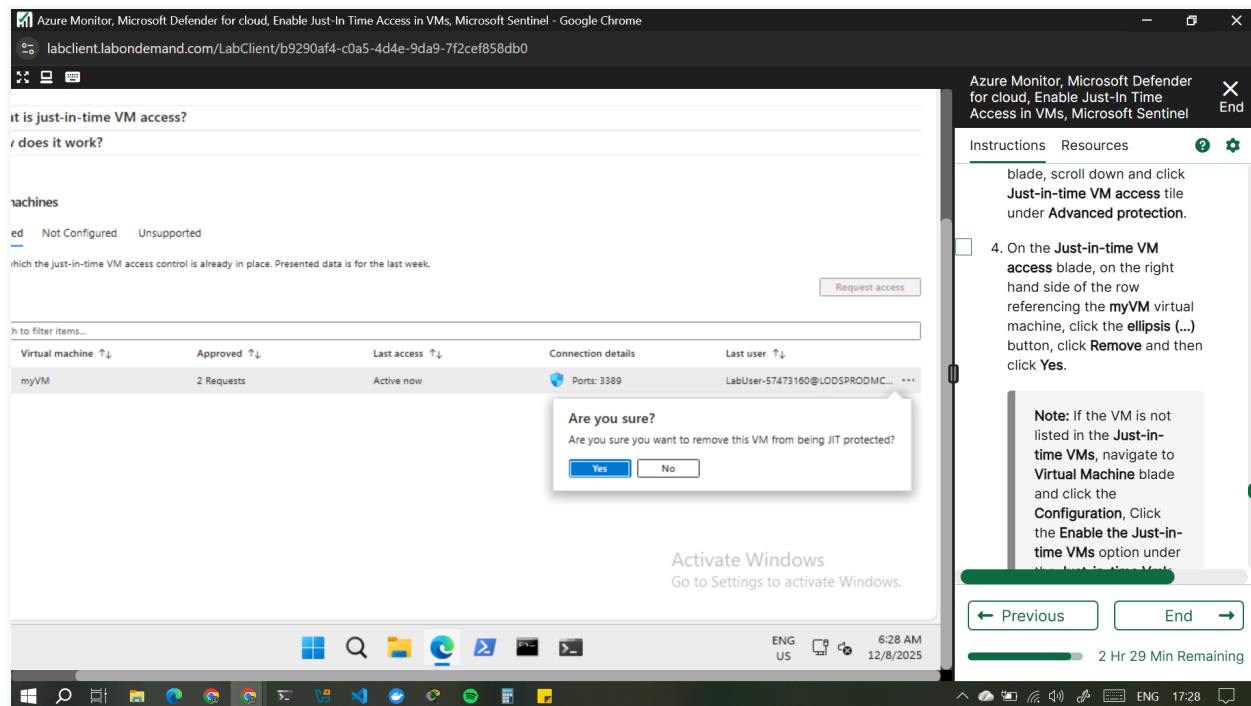
1. In the Azure portal, navigate to the Microsoft Defender for Cloud | Overview blade.
Check your secure score. By now it should have updated.

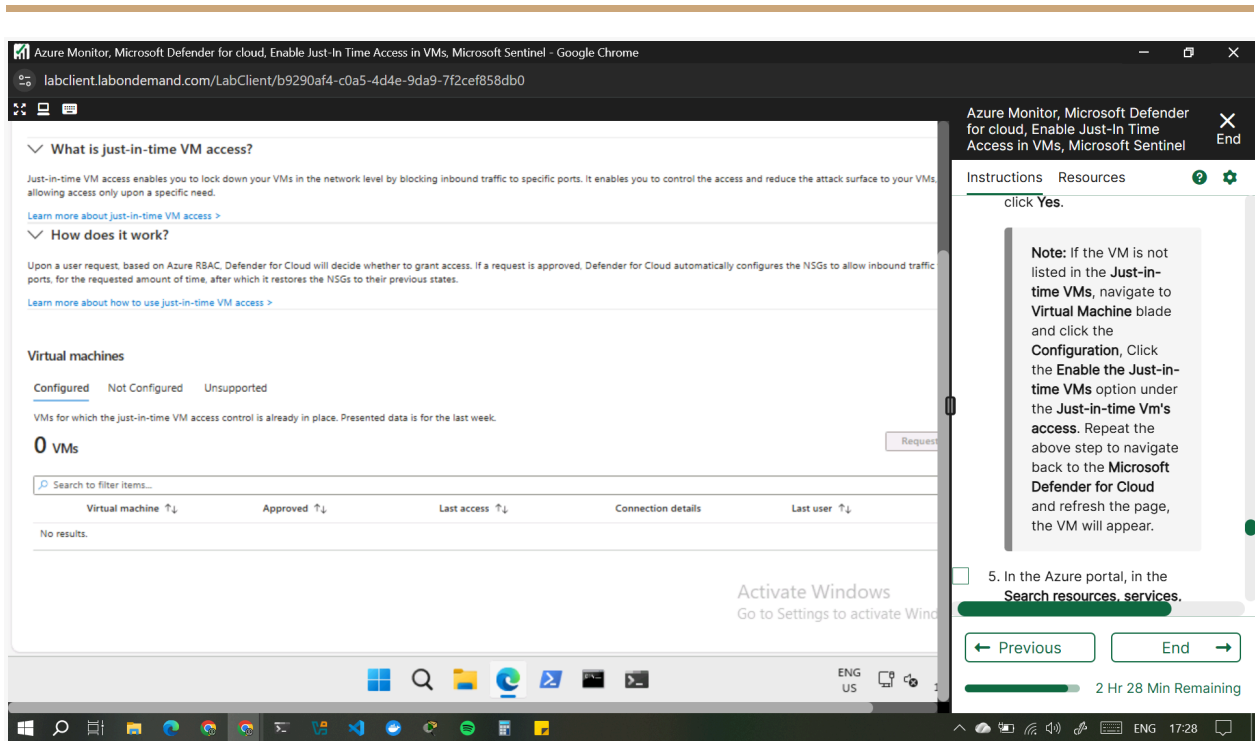


2. On the Microsoft Defender for Cloud | Overview blade, click Workload protections under Cloud Security in the left navigation.
3. On the Microsoft Defender for Cloud | Workload protections blade, scroll down and click Just-in-time VM access tile under Advanced protection.



- On the Just-in-time VM access blade, on the right hand side of the row referencing the myVM virtual machine, click the ellipsis (...) button, click Remove and then click Yes.





5. In the Azure portal, in the Search resources, services, and docs text box at the top of the Azure portal page, type Activity log and press the Enter key.
6. Navigate to the Activity log blade, note an **Delete JIT Network Access Policies** entry.
This may take a few minutes to appear. Refresh the page if it does not appear.

The screenshot shows the Azure Monitor Activity log interface. The left sidebar contains navigation options like Overview, Activity log, Alerts, Issues, Metrics, Logs, Change Analysis, Service health, Workbooks, Dashboards with Grafana, Insights, Managed Services, Settings, Diagnostic settings, Data Collection Rules, and Data Collection Endpoints. The main area displays the Activity log for the subscription 'MOC Subscription-lod51809825'. A search filter 'delete' is applied. The table shows four items, all with a status of 'Succeeded'.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
Delete JIT Network Access Policies	Succeeded	2 minutes a...	Mon Dec 08...	MOC Subscription-lod51809825	LabUser-5747316
Delete Connection	Succeeded	26 minutes ...	Mon Dec 08...	MOC Subscription-lod51809825	LabUser-5747316
Delete Connection	Succeeded	27 minutes ...	Mon Dec 08...	MOC Subscription-lod51809825	LabUser-5747316
Delete server vulnerability assessme	Succeeded	2 hours ago	Mon Dec 08...	MOC Subscription-lod51809825	LabUser-5747316

On the right, an 'Instructions' panel provides step-by-step guidance. Step 6 instructs the user to navigate to the Activity log blade and note a 'Delete JIT Network Access Policies' entry. Step 7 instructs the user to navigate back to the Microsoft Sentinel Overview blade. A progress bar at the bottom indicates '2 Hr 26 Min Remaining'.

7. In the Azure portal, navigate back to the Microsoft Sentinel | Overview blade.
8. On the Microsoft Sentinel | Overview blade, review the dashboard and verify that it displays an incident corresponding to the deletion of the Just-in-time VM access policy.

It can take up to 5 minutes for alerts to appear on the Microsoft Sentinel | Overview blade. If you are not seeing an alert at that point, run the query rule referenced in the previous task to verify that the Just-in-time access policy deletion activity has been propagated to the Log Analytics workspace associated with your Microsoft Sentinel instance. If that is not the case, re-create the Just-in-time VM access policy and delete it again.

7. In the Azure portal, navigate back to the **Microsoft Sentinel | Overview** blade.

8. On the **Microsoft Sentinel | Overview** blade, review the dashboard and verify that it displays an incident corresponding to the deletion of the Just-in-time VM access policy.

It can take up to 5 minutes for alerts to appear on the **Microsoft Sentinel | Overview** blade. If you are not seeing an alert at that point, wait 5 minutes and refresh the page.

← Previous End →

2 Hr 11 Min Remaining

9. On the **Microsoft Sentinel | Overview** blade, in the **Threat Management** section, click **Incidents**.

9. On the **Microsoft Sentinel | Overview** blade, in the **Threat Management** section, click **Incidents**.

10. Verify that the blade displays an incident with either medium or high severity level.

It can take up to 5 minutes for the incident to appear on the **Microsoft Sentinel | Incidents** blade.

Review the Microsoft

← Previous End →

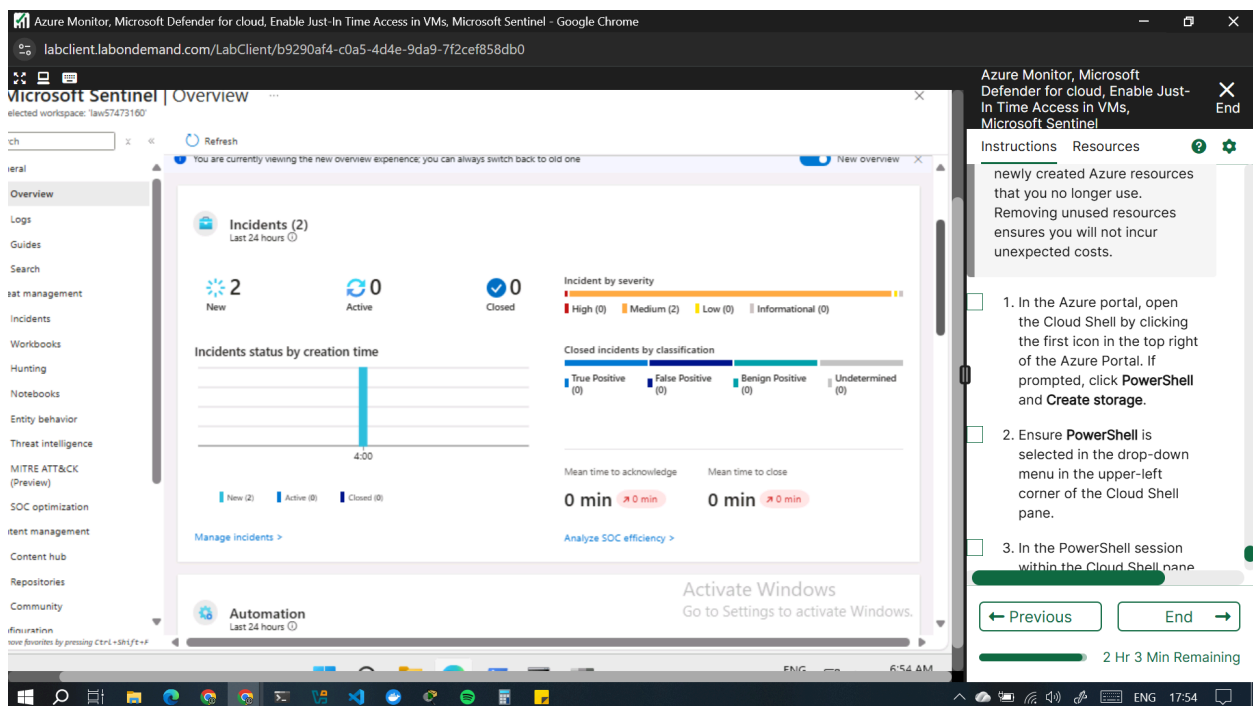
2 Hr 10 Min Remaining

10. Verify that the blade displays an incident with either medium or high severity level.

It can take up to 5 minutes for the incident to appear on the Microsoft Sentinel | Incidents blade.

Review the Microsoft Sentinel | Playbooks blade. You will find there the count of successful and failed runs.

You have the option of assigning a different severity level and status to an incident.

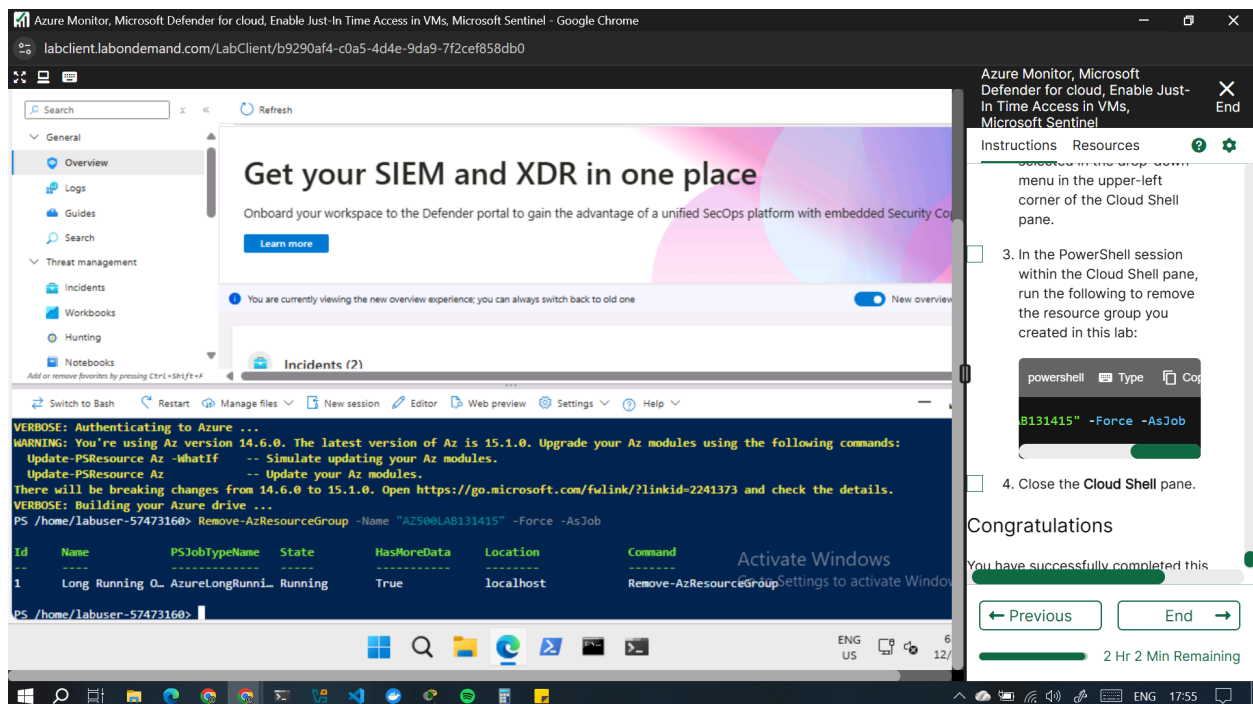


Results: You have created a Microsoft Sentinel workspace, connected it to Azure Activity logs, created a playbook and custom alerts that are triggered in response to the removal of Just-in-time VM access policies, and verified that the configuration is valid.

Clean up resources

Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs.

1. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, click PowerShell and Create storage.
2. Ensure PowerShell is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.
3. In the PowerShell session within the Cloud Shell pane, run the following to remove the resource group you created in this lab:
4. [REDACTED]
5. `Remove-AzResourceGroup -Name "AZ500LAB131415" -Force -AsJob`
6. Close the Cloud Shell pane.



Conclusion

This week's labs demonstrated how Azure's security and monitoring ecosystem works together to protect cloud environments. By implementing Azure Monitor, Defender for Cloud, Just-In-Time VM Access, and Microsoft Sentinel, I gained hands-on experience in collecting and analyzing logs, improving security posture, reducing attack surfaces, and detecting threats in real time. These labs strengthened my understanding of cloud security operations and provided practical skills in monitoring, incident response, and proactive threat prevention.