

COURSE: CLOUD AND NETWORK SECURITY

NAME: DENISE SOPHY ONDISO MUTAYI

STUDENT NO: CS-CN09-25047

AZURE MONITOR, MICROSOFT DEFENDER FOR CLOUD,
ENABLE JUST-IN TIME ACCESS IN VMS, MICROSOFT
SENTINEL

Table of Contents.

AZURE MONITOR, MICROSOFT DEFENDER FOR CLOUD, ENABLE JUST-IN TIME ACCESS IN VMS, MICROSOFT SENTINEL	1
Introduction	3
Lab 08: Create a Log Analytics Workspace, Azure Storage Account, and Data Collection Rule (DCR)	4
Exercise 1: Deploy an Azure virtual machine	4
Exercise 2: Create an Log Analytics workspace	6
Task 1: Create a Log Analytics workspace	6
Exercise 3: Create an Azure storage account	7
Task 1: Create an Azure storage account	7
Exercise 4: Create a Data Collection Rule	8
Task 1: Create a Data Collection Rule.	8
Lab 09: Configuring Microsoft Defender for Cloud Enhanced Security Features for Servers	10
Configure Microsoft Defender for Cloud Enhanced Security Features for Serve	10
Lab 10: Enable just-in-time access on VMs	10
Exercise 1: Enable JIT on your VMs from Azure virtual machines	10
Exercise 2: Request access to a JIT-enabled VM from the Azure virtual machine's connect page.	11
Lab 11: Microsoft Sentinel	11
Exercise 1: Implement Microsoft Sentinel	11
Task 1: On-board Microsoft Sentinel	11
Task 2: Configure Microsoft Sentinel to use the Azure Activity data connector.	12
Task 3: Create a rule that uses the Azure Activity data connector.	14
Task 4: Create a playbook	14
Task 5: Create a custom alert and configure a playbook as an automated response	16
Task 6: Invoke an incident and review the associated actions.	17

Introduction

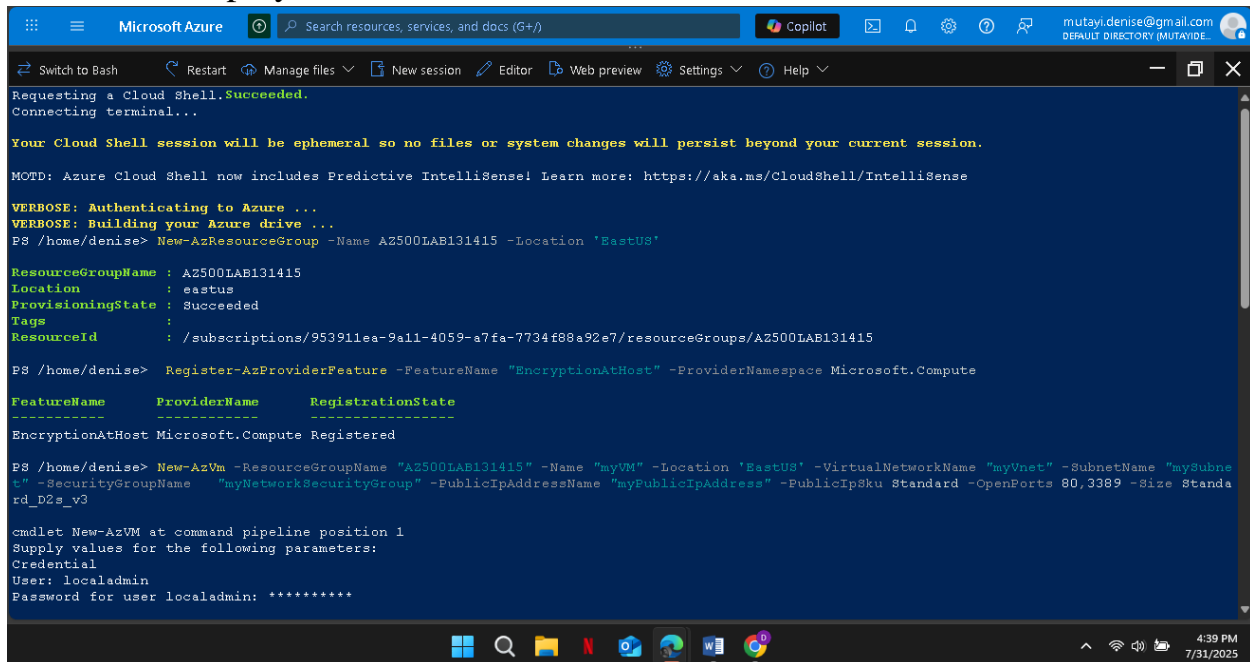
In this lab series, I configured and implemented several security features using Microsoft Defender for Cloud and Microsoft Sentinel on Azure. I began by deploying an Azure virtual machine in the East US region, followed by the creation of a Log Analytics workspace, an Azure storage account, and a data collection rule (DCR) to collect performance counters and event logs. These components were essential in establishing a central point for monitoring and telemetry collection.

Next, I enabled Microsoft Defender for Servers Plan 2 under Cloud Workload Protection (CWP), which provided enhanced security features, including vulnerability assessment, endpoint detection and response (EDR), and just-in-time (JIT) access for virtual machines. I then configured JIT VM access on the deployed virtual machine to minimize exposure to threats by restricting open ports and access duration.

Finally, I onboarded Microsoft Sentinel by connecting it to the previously created Log Analytics workspace. I configured data connectors to collect logs from Azure Activity and Defender for Cloud, created built-in and custom analytics rules to detect suspicious activity, and built a playbook using a Logic App to automate incident response. I also simulated an incident by deleting a JIT access policy to verify that Microsoft Sentinel correctly triggered the alert and executed the playbook.

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

Exercise 1: Deploy an Azure virtual machine



The screenshot shows the Microsoft Azure Cloud Shell interface. The terminal window displays the following commands and output:

```
Requesting a Cloud Shell. Succeeded.
Connecting terminal...

Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.

MOTD: Azure Cloud Shell now includes Predictive IntelliSense! Learn more: https://aka.ms/CloudShell/IntelliSense

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/denise> New-AzResourceGroup -Name AZ500LAB131415 -Location 'EastUS'

ResourceGroupName : AZ500LAB131415
Location           : eastus
ProvisioningState   : Succeeded
Tags               :
ResourceId          : /subscriptions/953911ea-9a11-4059-a7fa-7734f88a92e7/resourceGroups/AZ500LAB131415

PS /home/denise> Register-AzProviderFeature -FeatureName "EncryptionAtHost" -ProviderNamespace Microsoft.Compute

FeatureName      ProviderName      RegistrationState
-----
EncryptionAtHost Microsoft.Compute Registered

PS /home/denise> 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

cmdlet New-AzVM at command pipeline position 1
Supply values for the following parameters:
Credential
User: localadmin
Password for user localadmin: *****
```

The terminal window is titled "Microsoft Azure" and includes a search bar and various icons. The bottom status bar shows the time as 4:39 PM on 7/31/2025.

```
Microsoft Azure Search resources, services, and docs (G+) Copilot mutayi.denise@gmail.com
DEFAULT DIRECTORY (MUTAYIDE)

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

- This change will take effect on '11/1/2025'
- The change is expected to take effect in Az version : '15.0.0'
- The change is expected to take effect in Az.Compute version : '11.0.0'
Note : Go to https://aka.ms/azps-changewarnings for steps to suppress this breaking change warning, and other information on breaking changes i
n Azure PowerShell.

ResourceGroupName : AZ500LAB131415
Id                : /subscriptions/953911ea-9a11-4059-a7fa-7734f88a92e7/resourceGroups/AZ500LAB131415/providers/Microsoft.Compute/virtualMachines/myVM
VmId              : 36c3fc79-b524-495e-b5dd-0462cf96ebae
Name              : myVM
Type              : Microsoft.Compute/virtualMachines
Location          : eastus
Tags              : {}
HardwareProfile   : {VmSize}
NetworkProfile    : {NetworkInterfaces}
SecurityProfile   : {UefiSettings, SecurityType}
OSProfile         : {ComputerName, AdminUsername, WindowsConfiguration, Secrets, AllowExtensionOperations, RequireGuestProvisionSignal}
ProvisioningState : Succeeded
StorageProfile    : {ImageReference, OsDisk, DataDisks, DiskControllerType, AlignRegionalDisksToVMZone}
FullyQualifiedDomainName : myvm-13cd8a.EastUS.cloudapp.azure.com
TimeCreated       : 7/31/2025 1:33:38 PM
Etag              : "2"

PS /home/denise>

Microsoft Azure Search resources, services, and docs (G+) Copilot mutayi.denise@gmail.com
DEFAULT DIRECTORY (MUTAYIDE)

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

Location : eastus
Tags     : {}
HardwareProfile : {VmSize}
NetworkProfile : {NetworkInterfaces}
SecurityProfile : {UefiSettings, SecurityType}
OSProfile     : {ComputerName, AdminUsername, WindowsConfiguration, Secrets, AllowExtensionOperations, RequireGuestProvisionSignal}
ProvisioningState : Succeeded
StorageProfile   : {ImageReference, OsDisk, DataDisks, DiskControllerType, AlignRegionalDisksToVMZone}
FullyQualifiedDomainName : myvm-13cd8a.EastUS.cloudapp.azure.com
TimeCreated      : 7/31/2025 1:33:38 PM
Etag             : "2"

PS /home/denise> Get-AzVM -Name 'myVM' -ResourceGroupName 'AZ500LAB131415' | Format-Table

ResourceGroupName Name Location VmSize OsType NIC ProvisioningState
-----
AZ500LAB131415 myVM eastus Standard_D2s_v3 Windows myVM Succeeded

PS /home/denise>
```

Created a new resource group and deploy a Windows-based virtual machine using PowerShell in Azure Cloud Shell.

Exercise 2: Create an Log Analytics workspace

Task 1: Create a Log Analytics workspace

Home > Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot mutayi.denise@gmail.com DEFAULT DIRECTORY (MUTAYIDE...)

Home > Microsoft.LogAnalyticsOMS | Overview Deployment

Search x « Delete Cancel Redeploy Download Refresh

Overview Inputs Outputs Template

✓ Your deployment is complete

Deployment name : Microsoft.LogAnalyticsOMS Start time : 7/31/2025, 4:51:45 PM
Subscription : Azure subscription 1 Correlation ID : 2edeb7e2-12d3-426b-aa48-6af34...
Resource group : AZ500LAB131415

> Deployment details

✓ Next steps

Go to resource

Give feedback
Tell us about your experience with deployment

Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >

Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >

Free Microsoft tutorials
Start learning today >

Work with an expert
Azure experts are service provider partners who can help manage your

Add or remove favorites by pressing Ctrl+Shift+F

4:52 PM 7/31/2025

Home > Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot mutayi.denise@gmail.com DEFAULT DIRECTORY (MUTAYIDE...)

Home > Microsoft.DataCollectionRules | Overview Deployment

Search x « Delete Cancel Redeploy Download Refresh

Overview Inputs Outputs Template

✓ Your deployment is complete

Deployment name : Microsoft.DataCollectionRules Start time : 7/31/2025, 5:10:37 PM
Subscription : Azure subscription 1 Correlation ID : b193aa73-795a-4c3d-9313-1ae64...
Resource group : AZ500LAB131415

> Deployment details

✓ Next steps

Go to resource

Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >

Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >

Free Microsoft tutorials
Start learning today >

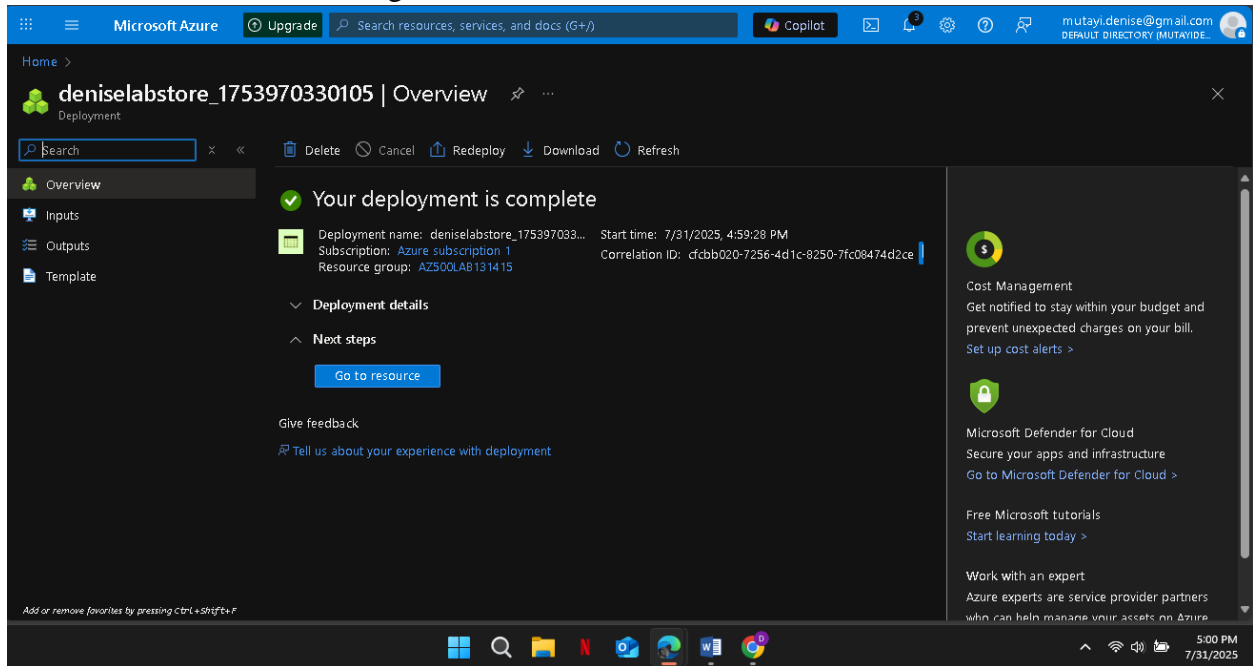
Work with an expert
Azure experts are service provider partners who can help manage your

Add or remove favorites by pressing Ctrl+Shift+F

5:12 PM 7/31/2025

Exercise 3: Create an Azure storage account

Task 1: Create an Azure storage account



Created an Azure storage account

Exercise 4: Create a Data Collection Rule

Task 1: Create a Data Collection Rule.

The screenshot displays the 'Create Data Collection Rule' wizard in the Microsoft Azure portal. The interface is in a dark theme. The top navigation bar includes the Microsoft Azure logo, an 'Upgrade' button, a search bar, and a Copilot button. The user's profile 'mutayi.denise@gmail.com' is visible in the top right.

The wizard is titled 'Create Data Collection Rule' with a subtitle 'Data collection rule management'. A green banner at the top indicates 'Validation passed'. A tip box suggests clicking a link to create a rule that collects platform metrics.

The 'Basics' tab is selected, showing the following details:

- Data rule name: DCR1
- Subscription: Azure subscription 1
- Resource Group: AZ500LAB131415

The 'Selected resources' section is currently empty. At the bottom of the 'Basics' tab, there is a 'Create' button and navigation links for '< Previous' and 'Next: >'. The system clock shows 5:09 PM on 7/31/2025.

The 'Collect and deliver' tab is the next step in the wizard. It contains the instruction: 'Configure which data sources to collect and where to send the data to.' Below this is a '+ Add data source' button. A table lists the configured data sources and destinations:

Data source	Destination(s)
Performance Counters	Azure Monitor Logs

At the bottom of the 'Collect and deliver' tab, there is a 'Review + create' button and navigation links for '< Previous' and 'Next: Tags >'. The system clock shows 5:08 PM.

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

Home > Monitor | Data Collection Rules >

Create Data Collection Rule

Data collection rule management

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

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 ☐

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	Azure subscription 1

Showing 1 - 1 of 1 results.

[Review + create](#) < Previous Next : Collect and deliver >

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

Home > Monitor | Data Collection Rules >

Create Data Collection Rule

Data collection rule management

[Basics](#) [Resources](#) [Collect and deliver](#) [Tags](#) [Review + create](#)

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources. [Learn more](#)

Rule details

Rule Name * DCR1 ✓

Subscription * Azure subscription 1 ✓

Resource Group * AZ500LAB131415 ✓
[Create new](#)

Region * East US ✓

Platform Type * ☒ Windows
☐ Linux
☐ All

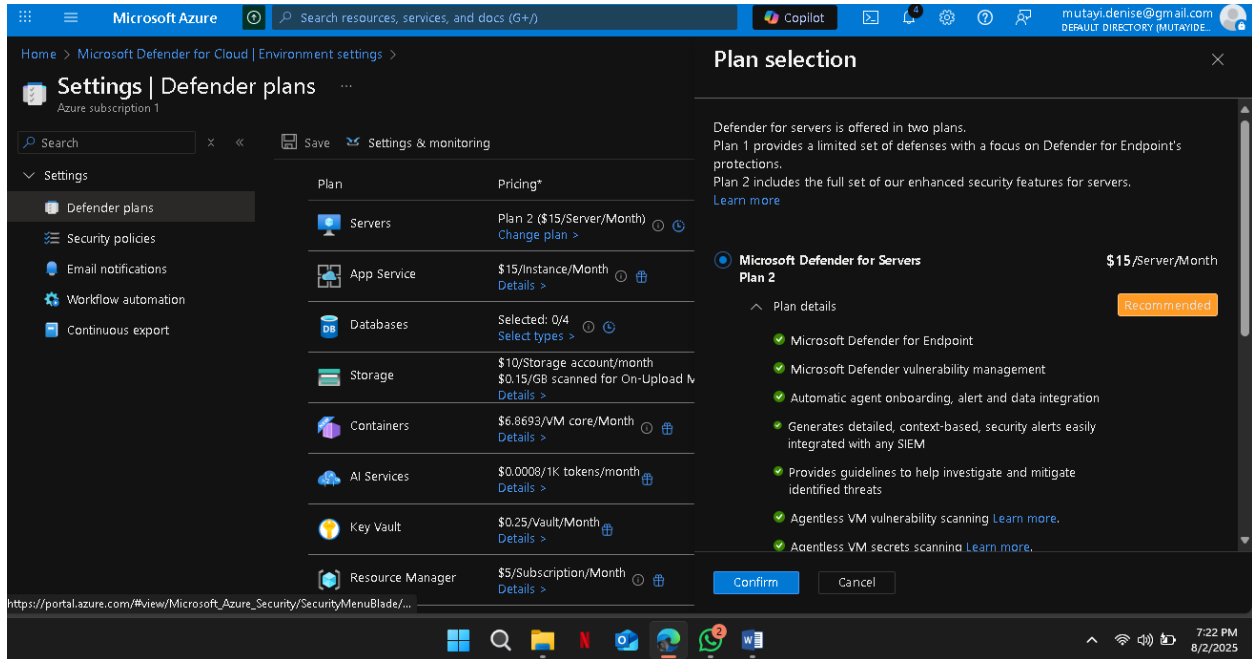
Data Collection Endpoint <none> ✓

[Review + create](#) < Previous Next : Resources >

Created a data collection rule

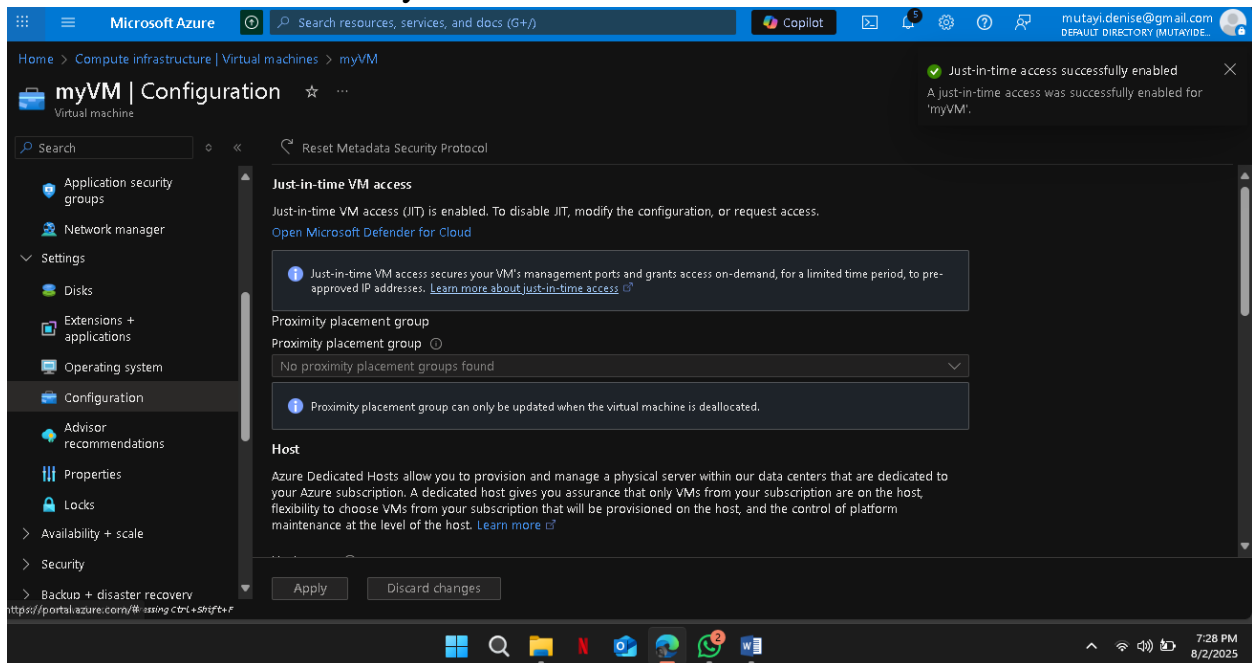
Lab 09: Configuring Microsoft Defender for Cloud Enhanced Security Features for Servers

Configure Microsoft Defender for Cloud Enhanced Security Features for Servers

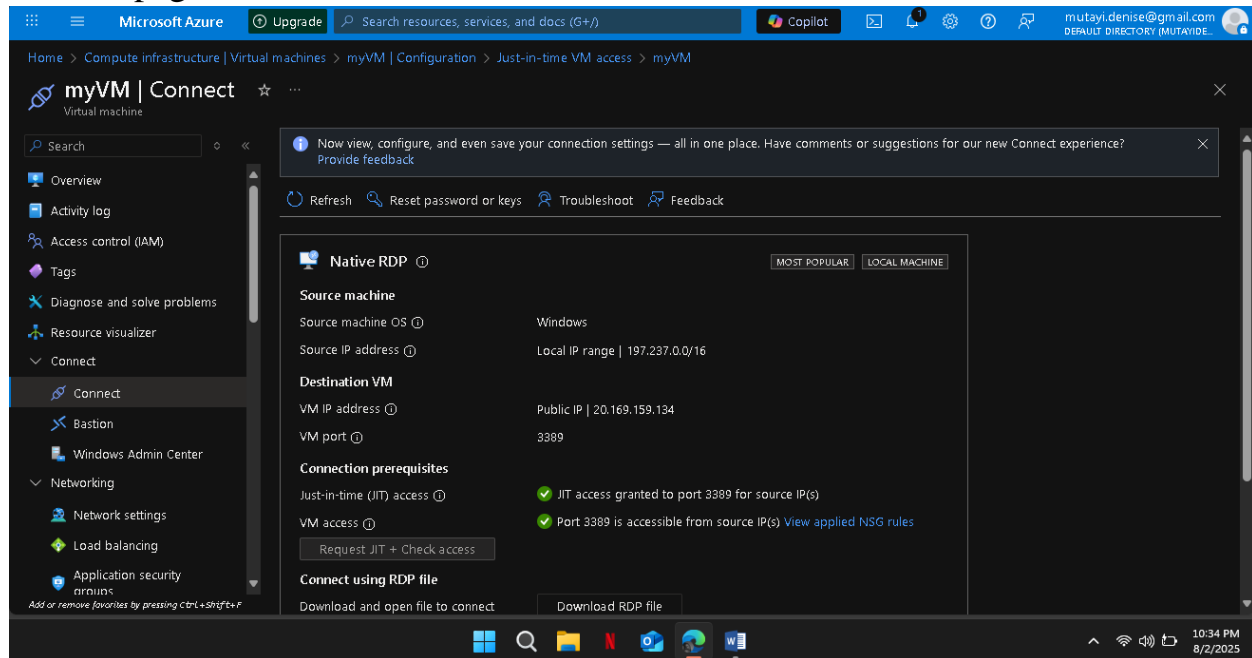


Lab 10: Enable just-in-time access on VMs

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



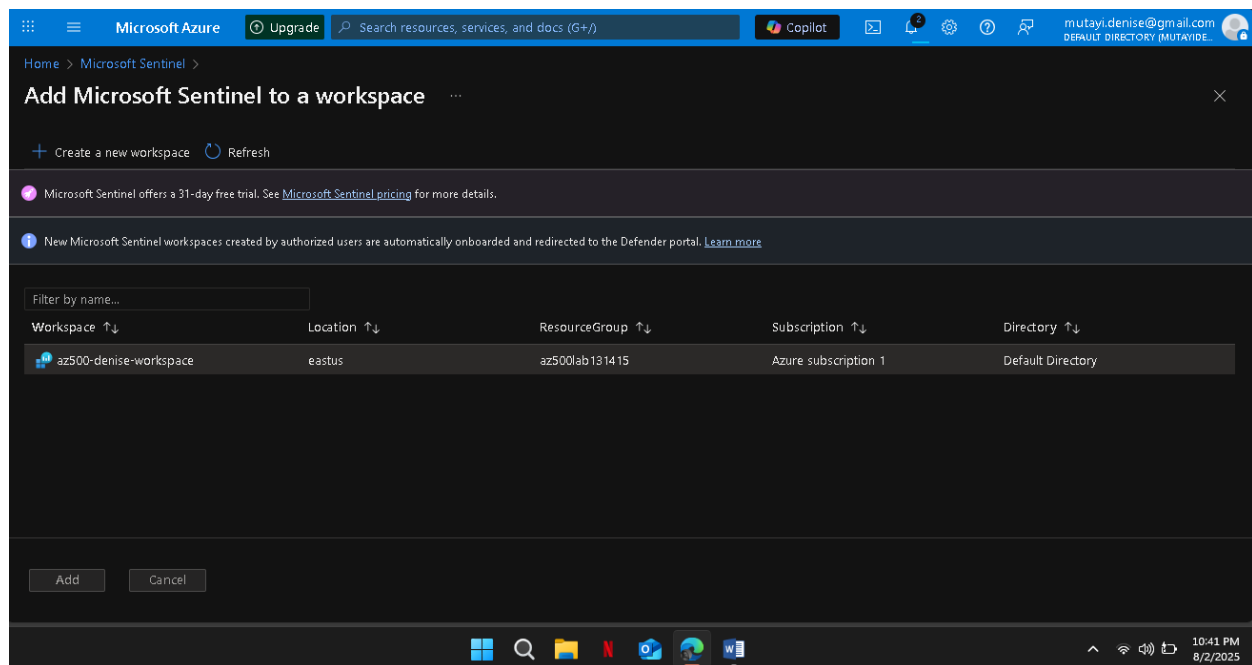
Exercise 2: Request access to a JIT-enabled VM from the Azure virtual machine's connect page.

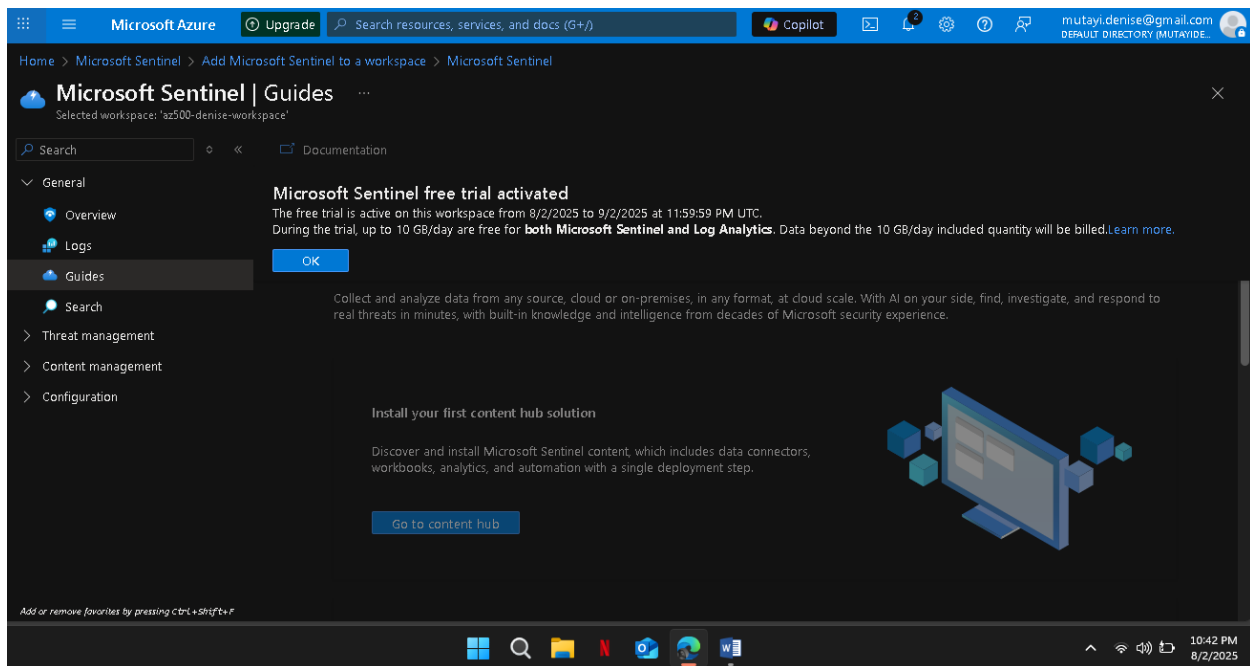


Lab 11: Microsoft Sentinel

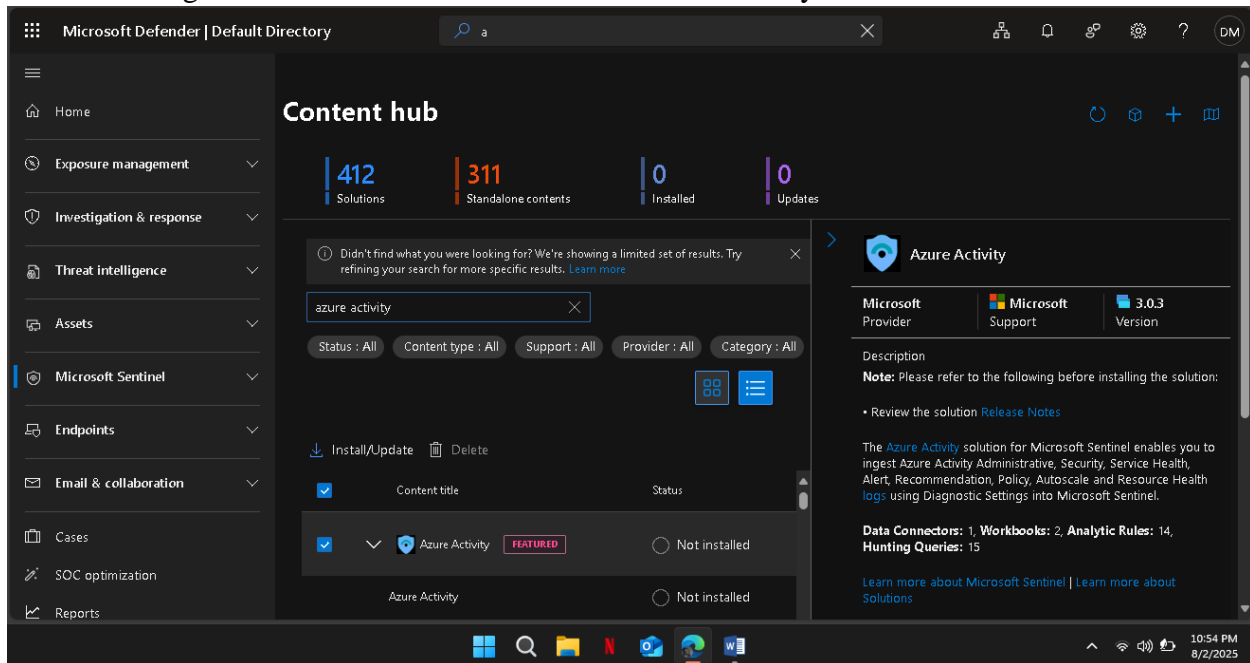
Exercise 1: Implement Microsoft Sentinel

Task 1: On-board Microsoft Sentinel





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



Microsoft Defender | Default Directory

Search

Home

Exposure management

Investigation & response

Threat intelligence

Assets

Microsoft Sentinel

Endpoints

Email & collaboration

Cases

SOC optimization

Reports

Content hub

412 Solutions

311 Standalone contents

20 Installed

0 Updates

Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. [Learn more](#)

azure activity

Status : AllContent type : AllSupport : AllProvider : AllCategory : All

Install/UpdateDelete

<input type="checkbox"/>	Content title	Status
<input type="checkbox"/>	▼ Azure Activity FEATURED	Installed
	Azure Activity	Installed

Azure Activity

Microsoft Provider

Microsoft Support

3.0.3 Version

Description

Note: Please refer to the following before installing the solution:

- Review the solution [Release Notes](#)

The **Azure Activity** solution for Microsoft Sentinel enables you to ingest Azure Activity Administrative, Security, Service Health, Alert, Recommendation, Policy, Autoscale and Resource Health logs using Diagnostic Settings into Microsoft Sentinel.

Data Connectors: 1, **Workbooks:** 2, **Analytic Rules:** 14, **Hunting Queries:** 15

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

10:59 PM8/2/2025

Microsoft Azure

Upgrade

Search resources, services, and docs (G+Y)

Copilot

mutayi.denise@gmail.com

DEFAULT DIRECTORY (MUTAYIDE...)

Hi Denise, see what more you can get from your Azure free account.

You've got 4 days left to use the remaining \$183.11 of your free credit. [See what's included.](#)

Take a free online course on Microsoft Learn

Watch a demo and attend a live Q&A

Start a project with Quickstart Center

Explore support resources

Azure services

Create a resource

Microsoft Sentinel

Virtual machines

Microsoft Defender for...

Monitor

Storage accounts

Notifications

More events in the activity log →Dismiss all ▼

\$183.11 credit remaining

Subscription 'Azure subscription 1' has a remaining credit of \$183.11.

Upgrade to a Pay-As-You-Go subscription.

a few seconds ago

Remediation task creation succeeded

Creating remediation task 'be0c0b0622f546f7bde20625' was successful.

a few seconds ago

Role Assignments creation succeeded

All role assignments were created successfully.

a few seconds ago

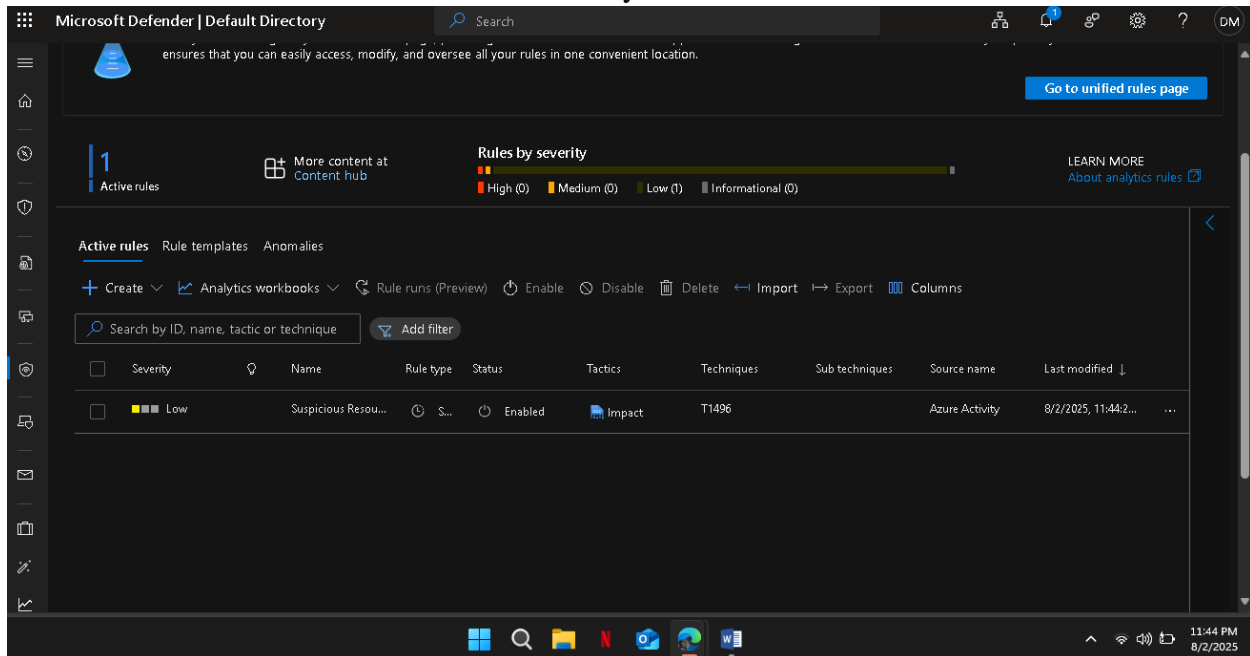
Creating policy assignment succeeded

Creating policy assignment 'Configure Azure Activity logs to stream to specified Log Analytics workspace' in 'Azure subscription 1' was successful. Please note that the assignment takes around 5-15 minutes to take effect.

a few seconds ago

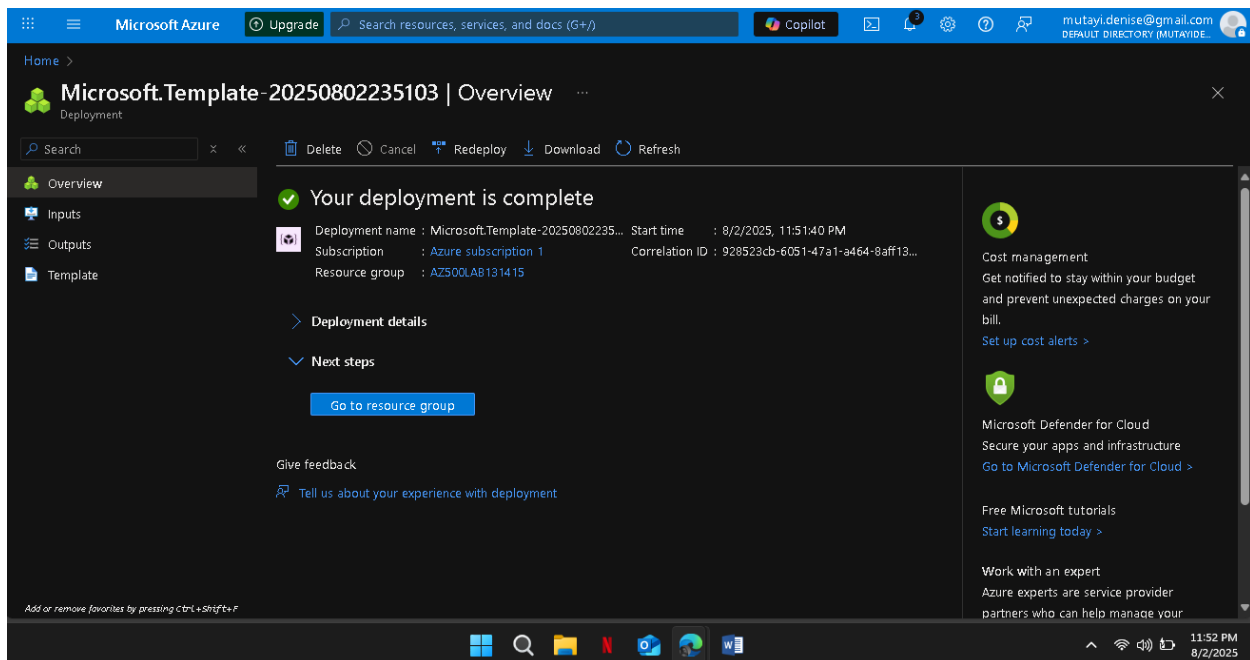
11:25 PM8/2/2025

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



Task 4: Create a playbook

A security playbook is a collection of tasks that can be invoked by Microsoft Sentinel in response to an alert.



Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | Copilot | mutayi.denise@gmail.com | DEFAULT DIRECTORY (MUTAYIDE)

Change Incident Severity

Run | Save | Discard | Parameters | Code view | Connections | Errors | Info

When a response to an Azure Sentinel alert is triggered

Alert - Get incident

Alert - Get accounts

Change incident

Change incident severity 2

Parameters | Settings | Code view | Testing | About

Specify resource group *

Resource group x

Specify Workspace ID *

Workspace ID x

Identifier *

Incident

Specify Alert / Incident *

Number x

Specify Severity *

High

Connected to live.com#mutayi.denise@gmail.com. | Change connection

12:11 AM 8/3/2025

Notifications

More events in the activity log → | Dismiss all ▾

✔ Successfully saved workflow

Successfully saved workflow 'Change-Incident-Severity'

a few seconds ago

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

Microsoft Defender | Default Directory

Analytics > Analytics rule wizard

Validation passed.

Analytics rule wizard - Create a new Scheduled rule

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

Analytics rule details

Name: Playbook Demo

Description: MITRE ATT&CK

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

< Previous Cancel

Microsoft Defender | Default Directory

Manage all your rules in one place

Now you can manage all your rules on one page, providing a centralized and streamlined approach to rule management. This enhancement not only simplifies your workflow but also ensures that you can easily access, modify, and oversee all your rules in one convenient location.

[Go to unified rules page](#)

2 Active rules

More content at Content hub

Rules by severity

High (0) Medium (1) Low (1) Informational (0)

[LEARN MORE About analytics rules](#)

Active rules Rule templates Anomalies

+ Create Analytics workbooks Rule runs (Preview) Enable Disable Delete

Search by ID, name, tactic or technique Add filter

Severity	Name	Rule type	Status	Tactics	Techniques	Sub
Medium	Playbook Demo	S...	Enabled	Initial Access		
Low	Suspicious Resou...	S...	Enabled	Impact	T1496	

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

The screenshot shows the Microsoft Azure Monitor Activity log interface. The left sidebar contains navigation options: Overview, Activity log (selected), Alerts, Metrics, Logs, Change Analysis, Service health, Workbooks, Dashboards with Grafana (preview), Insights, Managed Services, Settings, Diagnostic settings, and Data Collection Rules. The main pane displays the Activity log for 'Azure subscription 1' with filters for 'Management Group: None', 'Event severity: All', and 'Timespan: Last 6 hours'. A table lists the first 53 items, showing operations like 'Create or Update Network Security Group', 'Delete JIT Network Access Policy', 'Update Automation Rules', 'Update Alert Rules', and 'Create role assignment'. The status of these operations is 'Succeeded' or 'Accepted'.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
Create or Update Network Security G	Succeeded	4 minutes a...	Sun Aug 03 ...	Azure subscription 1	Windows Azure Security R...
Delete JIT Network Access Policie	Started	4 minutes a...	Sun Aug 03 ...	Azure subscription 1	mutayi.denise@gmail.com
Delete JIT Network Access Policie	Succeeded	4 minutes a...	Sun Aug 03 ...	Azure subscription 1	mutayi.denise@gmail.com
Create or Update Network Securi	Started	4 minutes a...	Sun Aug 03 ...	Azure subscription 1	Windows Azure Security R...
Create or Update Network Securi	Accepted	4 minutes a...	Sun Aug 03 ...	Azure subscription 1	Windows Azure Security R...
Update Automation Rules	Succeeded	7 minutes a...	Sun Aug 03 ...	Azure subscription 1	mutayi.denise@gmail.com
Update Alert Rules	Succeeded	7 minutes a...	Sun Aug 03 ...	Azure subscription 1	mutayi.denise@gmail.com
Create role assignment	Succeeded	24 minutes ...	Sun Aug 03 ...	Azure subscription 1	mutayi.denise@gmail.com

Deleted JIT Network Access Policies entry.

The screenshot shows the Microsoft Defender | Default Directory Incidents interface. The left sidebar contains navigation options: Home, Exposure management, Investigation & response (selected), Threat intelligence, Assets, Microsoft Sentinel, Endpoints, Email & collaboration, Cases, SOC optimization, and Reports. The main pane displays the 'Incidents' section with a message about the incident queue. Below, the 'Most recent incidents and alerts' section shows a table of incidents. The table has columns for Incident name, Incident ID, Tags, Severity, Investigation state, and Category. Two incidents are listed: 'Playbook Demo' with a severity of 'Medium' and 'Suspicious Resource deployment involving one user' with a severity of 'Low'.

Incident name	Incident ID	Tags	Severity	Investigation state	Category
Playbook Demo	2		Medium		Initial acce
Suspicious Resource deployment involving one user	1		Low		Impact

An incident of medium seniority.

```
Microsoft Azure Upgrade Search resources, services, and docs (G+) Copilot mutayi.denise@gmail.com
Switch to Bash Restart Manage files New session Editor Web preview Settings Help
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.

MOTD: SqlServer has been updated to Version 22!

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/denise> Remove-AzResourceGroup -Name "AZ500LAB131415" -Force -AsJob

Id      Name      PSJobTypeName      State      HasMoreData      Location      Command
--      -
1      Long Running O... AzureLongRunni... Running      True      localhost      Remove-AzResourceGroup

PS /home/denise> 
```

Cleaning up resources

Conclusion

By completing these labs, I implemented a full-stack security monitoring and automation solution on Azure. I successfully deployed the infrastructure, enabled Microsoft Defender for Servers, configured just-in-time VM access, and integrated Azure Activity logs into Microsoft Sentinel. I created analytics rules and a custom playbook that responded to specific security events, such as the removal of a JIT access policy.

This process allowed me to observe how Microsoft Sentinel and Defender for Cloud work together to detect threats, trigger alerts, and respond through automation. The hands-on experience gave me practical skills in setting up cloud-based threat protection, monitoring, and incident response mechanisms using Microsoft's native security tools.