

Cyber Shujaa

Cloud Security Specialist

**Assignment 22 - Lab 8: Azure Monitor,
Microsoft Defender for cloud, Enable Just-In
Time Access in VMs, Microsoft Sentinel**

NAME: WELDON KIPKIRUI KENEI

CS NO: ADC-CSS02-25027

Introduction

In this lab, we will learn and achieve the following objectives:

- Create a Log Analytics Workspace, Azure Storage Account, and Data Collection Rule (DCR)
- Configuring Microsoft Defender for Cloud Enhanced Security Features for Servers
- Enable just-in-time access on VMs
- Microsoft Sentinel

This report will demonstrate the steps taken to complete the tasks.

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

In this lab, we will implement a solution that collects security events, system logs, and performance counters. We will configure the Azure Monitor Agent (AMA) along with Data Collection Rules (DCRs) to centralize log collection and performance monitoring.

Deploying an Azure VM

In this step, we will use the Azure Cloud Shell to deploy an Azure VM as shown below.

The screenshot shows the Azure Cloud Shell interface. On the left, a terminal window displays PowerShell commands for creating a new VM. The command `New-AzVm` is being run, and it prompts for credentials. The user 'localadmin' is specified as the User, and a password is provided. The VM details are listed at the bottom of the terminal.

```
PS /home/labuser-52278487> 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: *****

ResourceGroupName      : AZ500LAB131415
Id                   : /subscriptions/2e4c9a12-5165-4a7e-9ff0-e16ed7d338e5/resourceGroups/AZ500LAB131415/providers/Microsoft.Compute/virtualMachines/myVM
VmId                 : ae50ed50-e729-43f7-b6ed-0959ba8df8c0
Name                 : myVM
Type                 : Microsoft.Compute/virtualMachines
```

On the right, a task pane titled 'Azure Monitor, Microsoft Defender for cloud, Enable...' shows a step-by-step guide. Step 10 is checked, and it asks for credentials, with 'User' set to 'localadmin'. Step 11 is a task: '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.' A PowerShell command is provided: `Get-AzVM -Name 'myVM' -ResourceGroup AZ500LAB131415`.

Creating a Log Analytics workspace

In this task, we will create a log analytics workspace to store and manage our logs.

Microsoft.LogAnalyticsOMS | Overview

Your deployment is complete

Deployment name : Microsoft.LogAnalyticsOMS
Subscription : MOC Subscription-1d050727277
Resource group : AZ500LAB131415
Start time : 6/17/2025, 3:32:38 AM
Correlation ID : a0835b4d-1d95-40f3-a03c-957617ef4e63

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

Creating an Azure storage account

In this task, we will create an Azure storage account.

lab22storage_1750156672823 | Overview

Your deployment is complete

Deployment name: lab22... Start time: 6/17/2025, 3:38:19 AM
Subscription: MOC Subsc... Correlation ID: 9114f4cc-0e62-411i...
Resource group: AZ500...

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

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

Estimated timing: 15 minutes

Create a Data Collection Rule

In this task, we will create a data collection rule from the Azure portal.

The screenshot shows a Microsoft Azure browser window. The main content area displays the 'Microsoft.DataCollectionRules | Overview' page. A red box highlights the 'Your deployment is complete' section, which contains the following deployment details:

- Deployment name : Microsoft.DataCollectionRules
- Subscription : MOC Subscription-1cd50727277
- Resource group : AZ500LAB131415
- Start time : 6/17/2025, 3:47:12 AM
- Correlation ID : 60266e95-f311-4189-a363-0b4d8898e20e

To the right of the main content, there is a sidebar with the following information:

- Instructions**: Step 15: Click **Create**.
- Results**: You 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.
- Note**: Do not remove the resources from this lab, as they are needed for the Microsoft Defender for Cloud lab, the 'Enable just-in-time access on VMs' lab, and the Microsoft Sentinel lab.
- Congratulations!**: You have successfully completed this Lab. Click **Next** to advance to the next Lab.

At the bottom of the sidebar, it says '31% Tasks Complete' with 'Previous' and 'Next' buttons.

From this objective, we have 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.

Configuring Microsoft Defender for Cloud Enhanced Security Features for Servers

In this task, we will follow steps to enable Microsoft Defender for Servers in Microsoft Defender for Cloud to provide advanced threat protection and security monitoring for both Azure VMs and hybrid servers.

Configure Microsoft Defender for Cloud Enhanced Security Features for Servers

Using the Azure portal, we configured and deployed Microsoft Defender for Cloud plan 2. The screenshot below shows more about the plan.

The screenshot displays two side-by-side windows from the Azure portal.

Left Window: Plan selection

- The title bar says "Plan selection - Microsoft Azure".
- The URL is https://portal.azure.com/#view/Microsoft_Azure_Security/CloudWorkloadProtectionBlade/CloudWorkloadProtectionBlade.
- The main content shows "Microsoft Defender for cloud environments".
- A sidebar on the left lists "Cloud Workload Protection" categories: Plan (Servers, App Service, Databases, Storage, Containers, AI Services). The "Servers" icon is highlighted with a red box.
- The "Microsoft Defender for Servers Plan 2" section is highlighted with a red box:
 - Cost: \$15/Server/Month
 - Status: Recommended
 - Details:
 - Microsoft Defender for Endpoint
 - Microsoft Defender vulnerability management
 - Automatic agent onboarding, alert and data integration
 - Generates detailed, context-based, security alerts easily integrated with any SIEM

Right Window: Azure Monitor, Microsoft Defender for cloud, Enable...

- The title bar says "Azure Monitor, Microsoft Defender for cloud, Enable..."
- The URL is <https://labclient.labondemand.com/LabClient/844851b7-7e31-461c-91a3-4fc09ff0b63b>.
- The page shows "4 Hr 32 Min Remaining".
- Instructions:
 - In the Settings blade, under Defender plans, expand Cloud Workload Protection (CWP).
 - 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.
 - 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.
- Two screenshots are shown: one of the "Plan selection" blade and another of the "Settings blade" showing the "Cloud Workload Protection (CWP)" settings.
- Progress: 35% Tasks Complete.
- Navigation buttons: < Previous and Next >

Enabling just-in-time access on VMs

In this scenario, we will enable JIT access on our deployed VMs. This will mitigate the continuous open access to our VMs, hence protecting them from known brute-force attacks.

Enabling JIT on your VMs from Azure virtual machines

In our Azure portal Virtual Machines pages, we will enable the JIT on our deployed VM as shown below;

The screenshot shows a Microsoft Azure browser window and a Microsoft Defender for Cloud task pane side-by-side.

Azure Portal (Left):

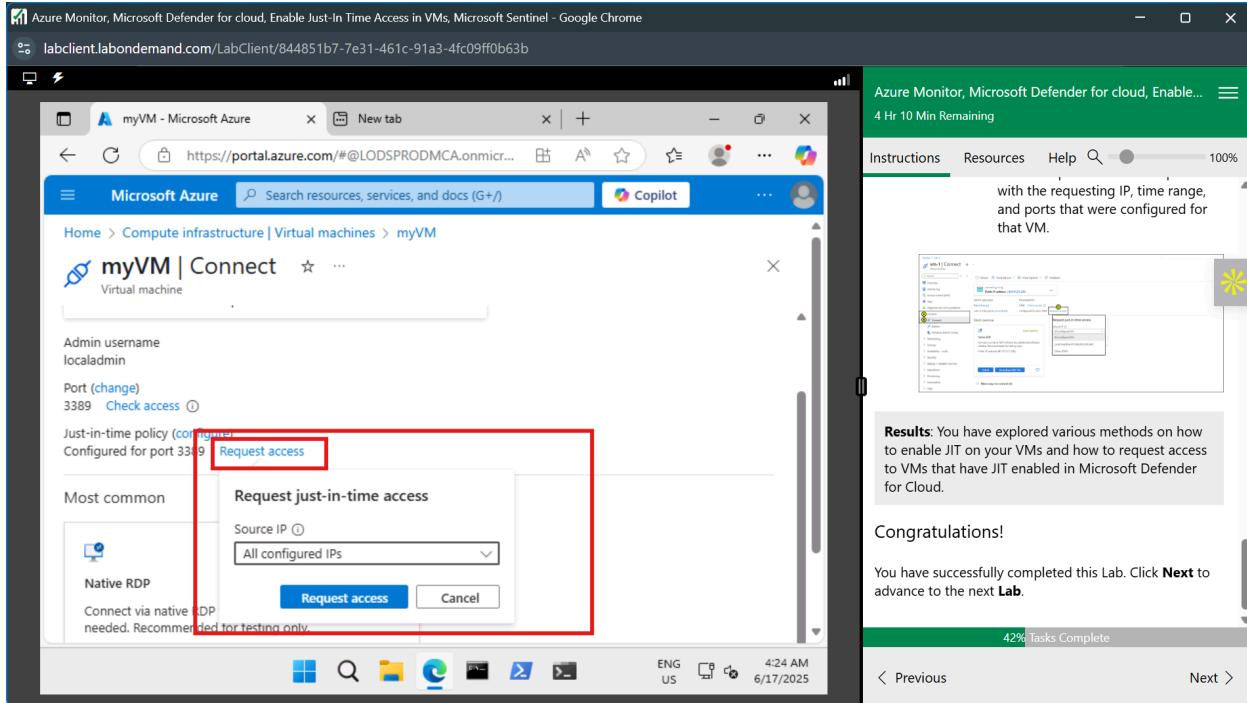
- The URL is <https://portal.azure.com/#@LODSPRODMCA.onmicrosoft.com>.
- The page title is "myVM | Configuration".
- The sub-page title is "Just-in-time VM access".
- A callout box highlights the "Enable just-in-time" button.
- Below the button, a note says: "To improve security, enable a just-in-time access." followed by "Learn more about just-in-time access".
- Other sections visible include "Proximity placement group" and "Windows machines".

Microsoft Defender for Cloud Task Pane (Right):

- The title is "Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome".
- The status bar shows "4 Hr 17 Min Remaining".
- The main content is a numbered list of steps:
 - Select myVM.
 - Select Configuration from the Settings section of myVM.
 - Under Just-in-time VM access, select Enable just-in-time.
 - Under Just-in-time VM access, click on the link that reads Open Microsoft Defender for Cloud.
 - 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
- A progress bar at the bottom indicates "38% Tasks Complete".

Requesting 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.



Microsoft Sentinel

In this scenario and task, we will create a proof of concept of Microsoft Sentinel-based threat detection and response. We will start collecting data from Azure Activity and Microsoft Defender for Cloud, add built-in and custom alerts, and review how Playbooks can be used to automate a response to an incident.

On-board Microsoft Sentinel

In this task, we will onboard MS Sentinel.

The screenshot shows a Microsoft Azure browser window. The main content area displays a list of workspaces, with one named 'LAW52278487' selected. A red box highlights the 'Add' button at the bottom left of the workspace list. The right side of the screen features a sidebar with task instructions and a progress bar indicating '47% Tasks Complete'. The task instructions for 'Task 1: On-board Microsoft Sentinel' include steps 1 and 2, both of which are checked. Step 1 describes signing in to the Azure portal with a specific URL. Step 2 describes searching for 'Microsoft Sentinel' in the Azure portal's search bar.

Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome
labclient.labondemand.com/LabClient/844851b7-7e31-461c-91a3-4fc09ff0b63b

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

Add Microsoft Sentinel to a workspace | New tab

Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

Filter by name...

Workspace ↑	Location ↑	ResourceGroup ↑	Subscription ↑	Directory ↑
LAW52278487	eastus	az500lab131415	MOC Subscription-lod...	LODS-Prod-MCA

Add Cancel

Azure Monitor, Microsoft Defender for cloud, Enable... 3 Hr 55 Min Remaining

Instructions Resources Help 100%

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-52278487@LODSPRODMCA.onmicrosoft.com` with password `B#1ehB0DdqI`.

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.

47% Tasks Complete

< Previous End >

Configure Microsoft Sentinel to use the Azure Activity data connector.

In this task, we configure Azure to use the Azure Activity data connectors as shown.

The screenshot shows two windows side-by-side. The left window is a browser showing the Microsoft Sentinel Data connectors page. A red box highlights the 'Azure Activity' connector under the 'Data Types' section. The right window is a task list titled 'Instructions' for 'Sentinel | Overview blade, in the Content management section, click Content hub.' It contains several steps, with the first three checked:

- 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**.

The task list continues with more steps, some of which are not yet completed (indicated by an empty checkbox).

Configuration of policy assignment, remediation tasks for already existing resources and role assignment were created successfully as show below.

The screenshot shows two windows side-by-side. The left window is a browser showing the 'Azure Activity' configuration page. A red box highlights the 'Azure Activity' section. The right window is a task list titled 'Instructions' for 'at the bottom of the page.' It contains several steps, with the first three checked:

- 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.
- 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.

The task list continues with more steps, some of which are not yet completed (indicated by an empty checkbox).

Create a rule that uses the Azure Activity data connector.

In this task we will create rules that will use Azure Activity data connector. We will use a **Suspicious number of resource creation or deployment** template for the rule.

The screenshot shows the Microsoft Sentinel interface. On the left, the 'Active rules' list is displayed with two entries highlighted by a red box:

Severity	Name	Status	Tactics	Techniques
Medium	Suspicious num...	Enabled	Impact	T1496
High	Advanced Multi...	Enabled	Collect	+11

On the right, a side panel titled 'Azure Monitor, Microsoft Defender for cloud, E...' displays the following instructions:

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**.

A message box indicates: **You now have an active rule.**

Task 4: Create a playbook

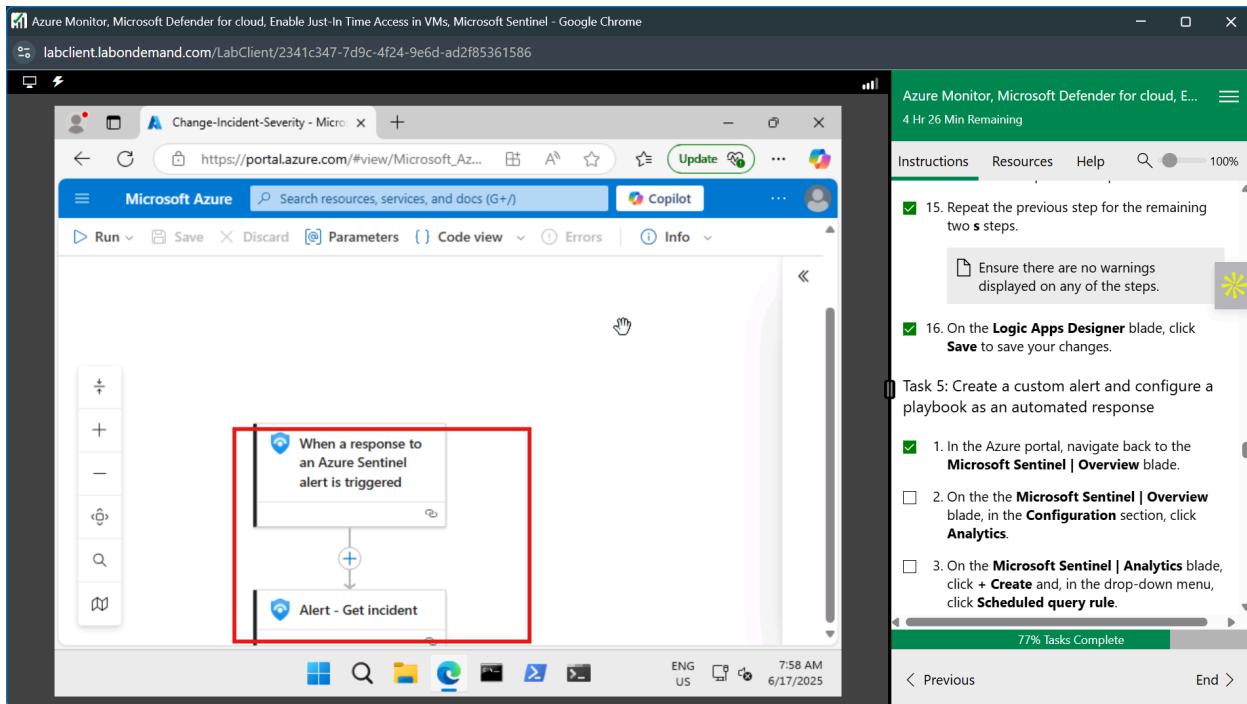
In this task, you will create a playbook. A security playbook is a collection of tasks that can be invoked by Microsoft Sentinel in response to an alert.

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**

Progress bar: 63% Tasks Complete

Create a playbook

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



Create a custom alert and configure a playbook as an automated response

In this task, we create an analytic rule that identifies removal of Just-in-time VM access policies. This rule will then trigger an alert and an automated response from our earlier deployed logic app.

The screenshot shows the Microsoft Azure portal with the URL https://portal.azure.com/#view/Microsoft_Azure_Sentinel. The main window displays the 'Rules by severity' blade, which lists three rules:

Severity	Name	Rule ID	Status	Tactics	Techniques
Medium	Playbook Demo	Scl	Enabled	Initial Access	
Medium	Suspicious num...	Scl	Enabled	Impact	T1496
High	Advanced Multi...	Fut	Enabled	Collect	+11

A red box highlights the first rule, 'Playbook Demo'. The task pane on the right is titled 'Azure Monitor, Microsoft Defender for cloud, Enable Just-In Time Access in VMs, Microsoft Sentinel - Google Chrome' and shows the following content:

4 Hr 12 Min Remaining

Instructions Resources Help 100%

INSTRUCTIONS
Select the Change-incident-Severity logic app. On the Create new automation rule window, click Apply.

14. On the Automated response tab of the Analytic rule wizard - 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 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.

1. In the Azure portal, navigate to the Microsoft Defender for Cloud | Overview blade.

Check your secure score. By now it
88% Tasks Complete

< Previous End >

Invoke an incident and review the associated actions.

In this task, we will prove that our playbook and rules are working by invoking an incident and reviewing the associated actions.

We first deleted the JIT VM from defender and view the log as shown

The screenshot shows the Microsoft Azure portal with the URL https://portal.azure.com/#view/microsoft_azuremonitor/activitylog. The activity log blade is displayed, showing two recent events:

- 1. Delete JIT Net - Succeeded - 18 minutes ago - Tue Jun 17 ... - MOC Subscription-Id... - LabUser-52285696@LOD...
- 2. Delete JIT - Started - 18 minutes ago - Tue Jun 17 ... - MOC Subscription-Id... - LabUser-52285696@LOD...

A callout box highlights the second event, "Delete JIT - Started". To the right, a sidebar provides instructions for enabling JIT VMs in Microsoft Defender for Cloud:

- Note: If the VM is not listed in the Just-in-time VMs, navigate to Virtual Machine blade and click the Configuration, Click the Enable the Just-in-time VM's access. Repeat the above step to navigate back to the Microsoft Defender for Cloud and refresh the page, the VM will appear.
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.

93% Tasks Complete

Now from the Microsoft Sentinel overview page, we can see the alert and incident created.

The screenshot shows the Microsoft Sentinel overview page with the URL https://portal.azure.com/#view/Microsoft_AzureSentinel. The Open incidents section displays one incident:

Severity	Incident number	Title
High	1	Playbook Demo

A callout box highlights the "Playbook Demo" incident. To the right, a sidebar provides instructions for verifying the incident:

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 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 an Microsoft Sentinel workspace, connected it to Azure Activity logs,

Conclusion

To conclude, this lab has taught us how to create a Log Analytics Workspace, Azure Storage Account, and Data Collection Rule (DCR), and configure Microsoft Defender for Cloud enhanced Security Features for Servers, Enable just-in-time access on VMs and finally create a Microsoft Sentinel workspace, connect it to Azure Activity logs, acreate 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.