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

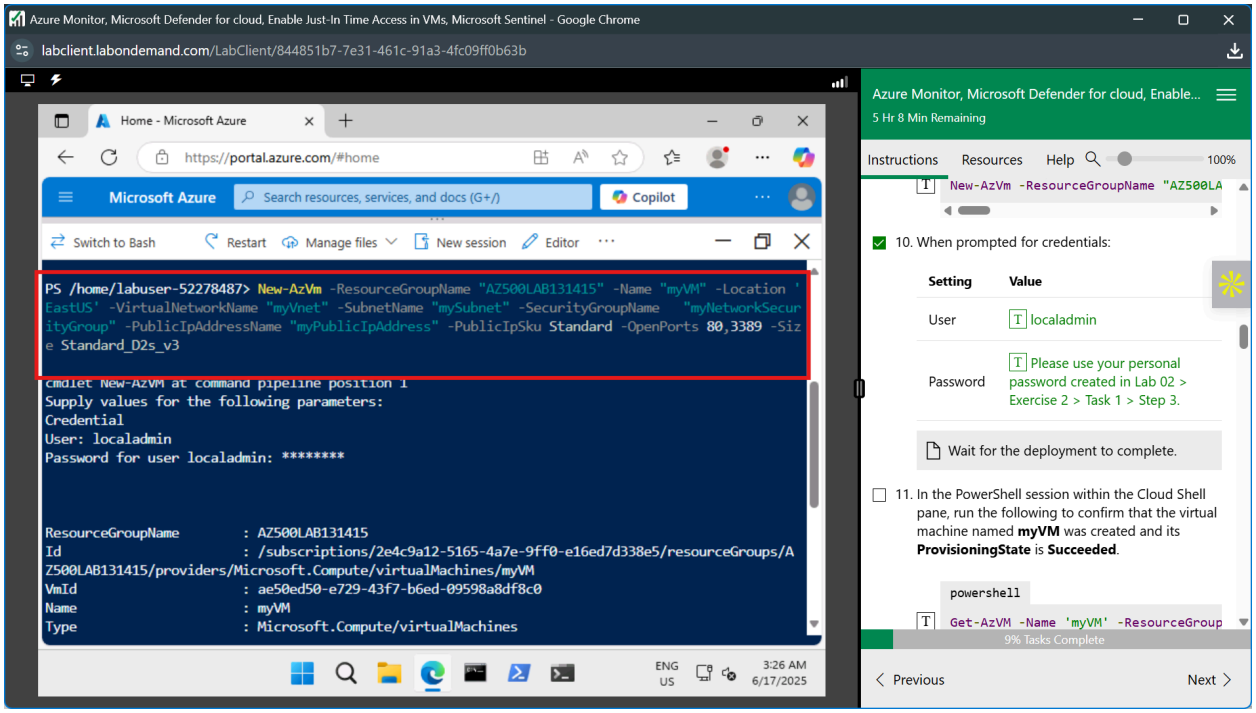
This report will demonstrate the steps taken to complete the tasks.

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.

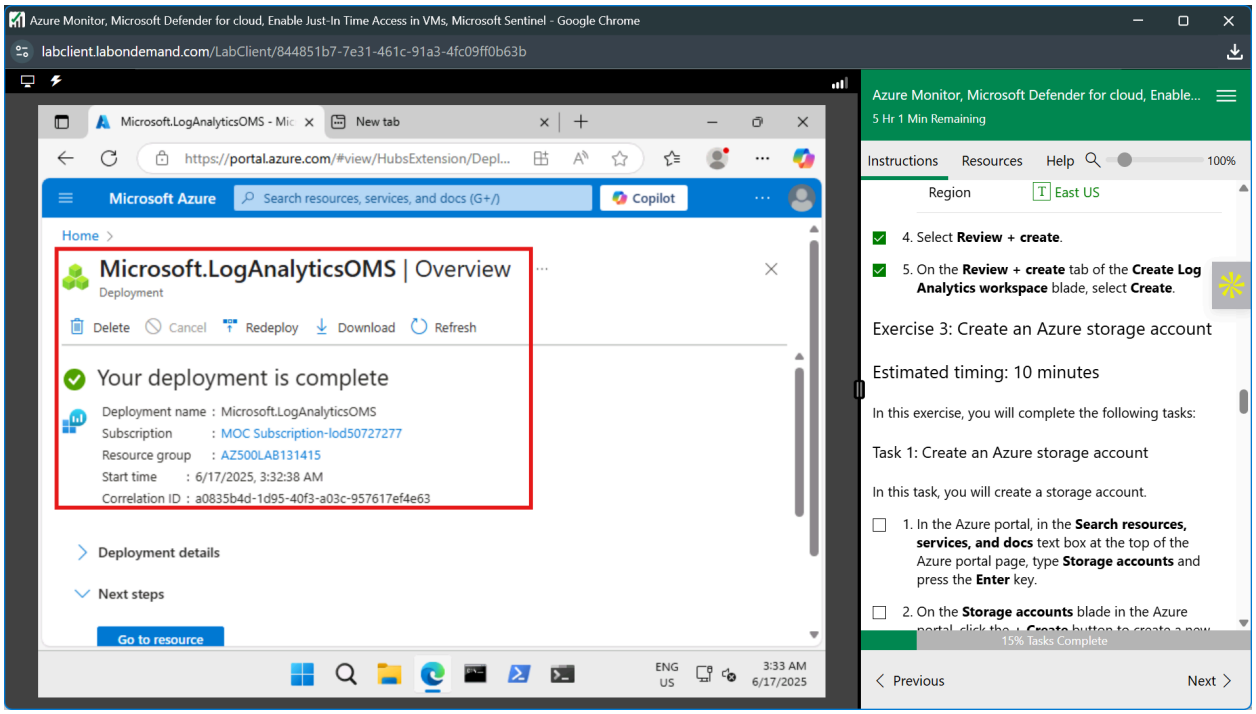
Deploying an Azure VM

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



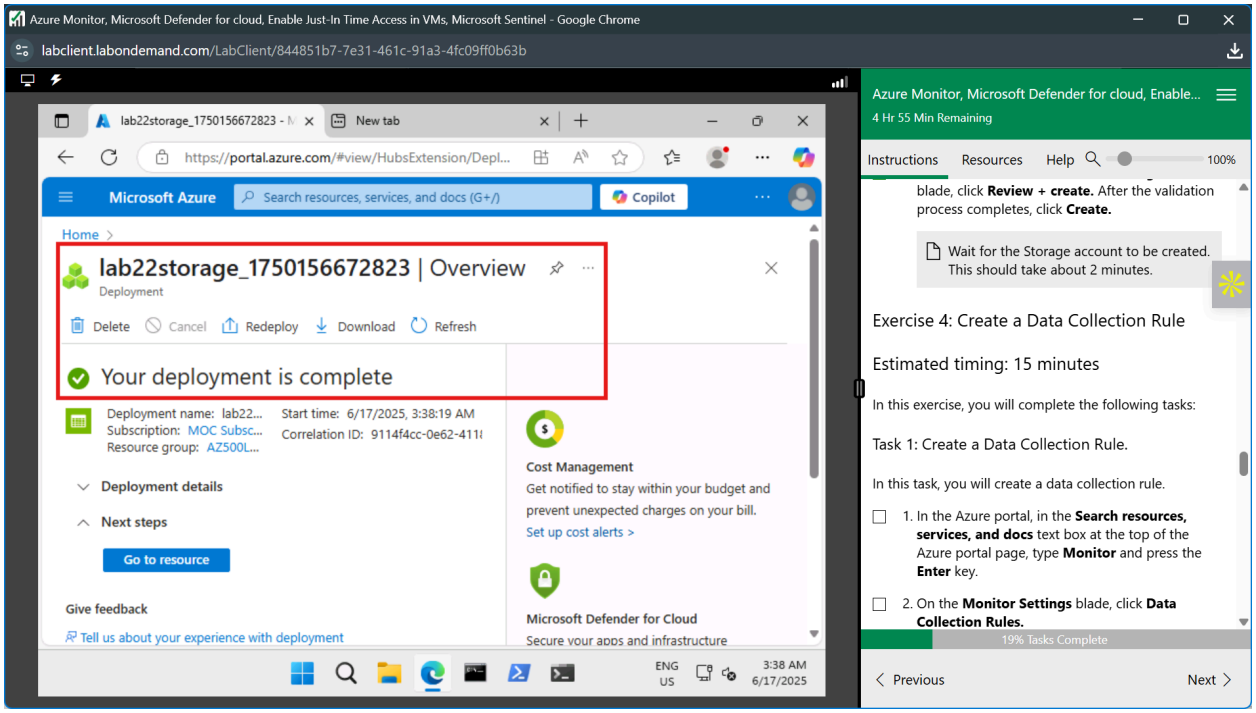
Creating a Log Analytics workspace

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



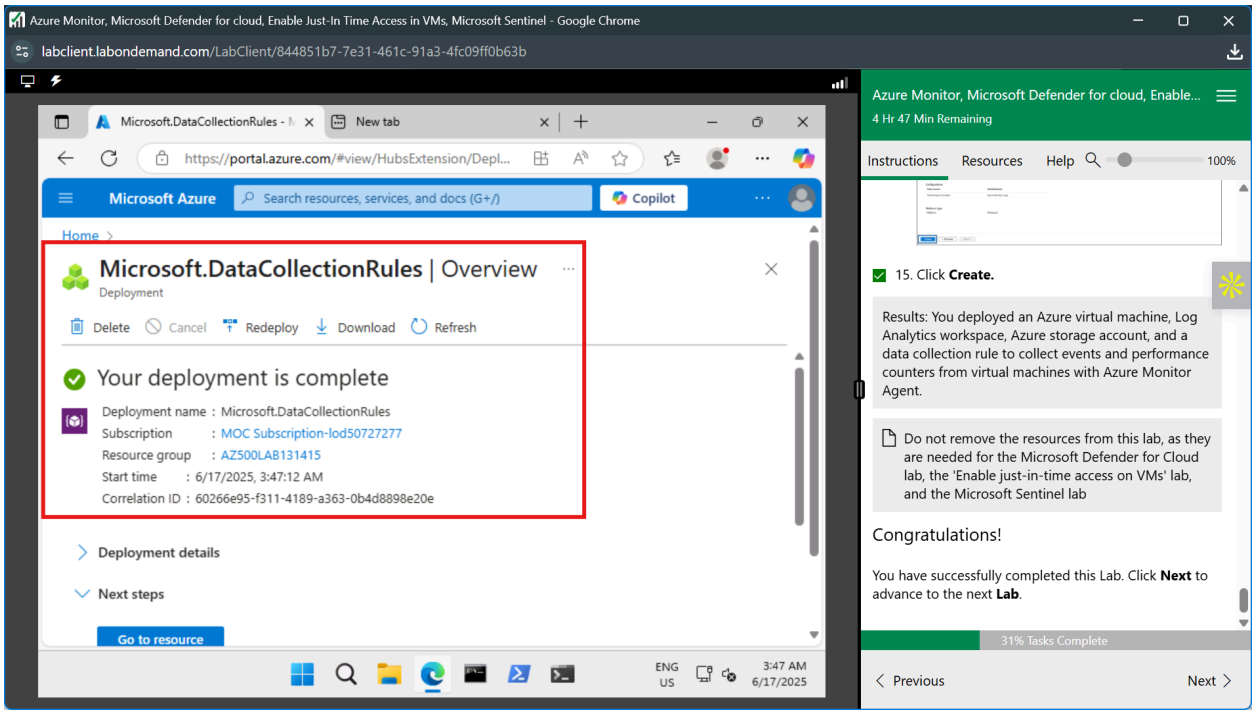
Creating an Azure storage account

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



Create a Data Collection Rule

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



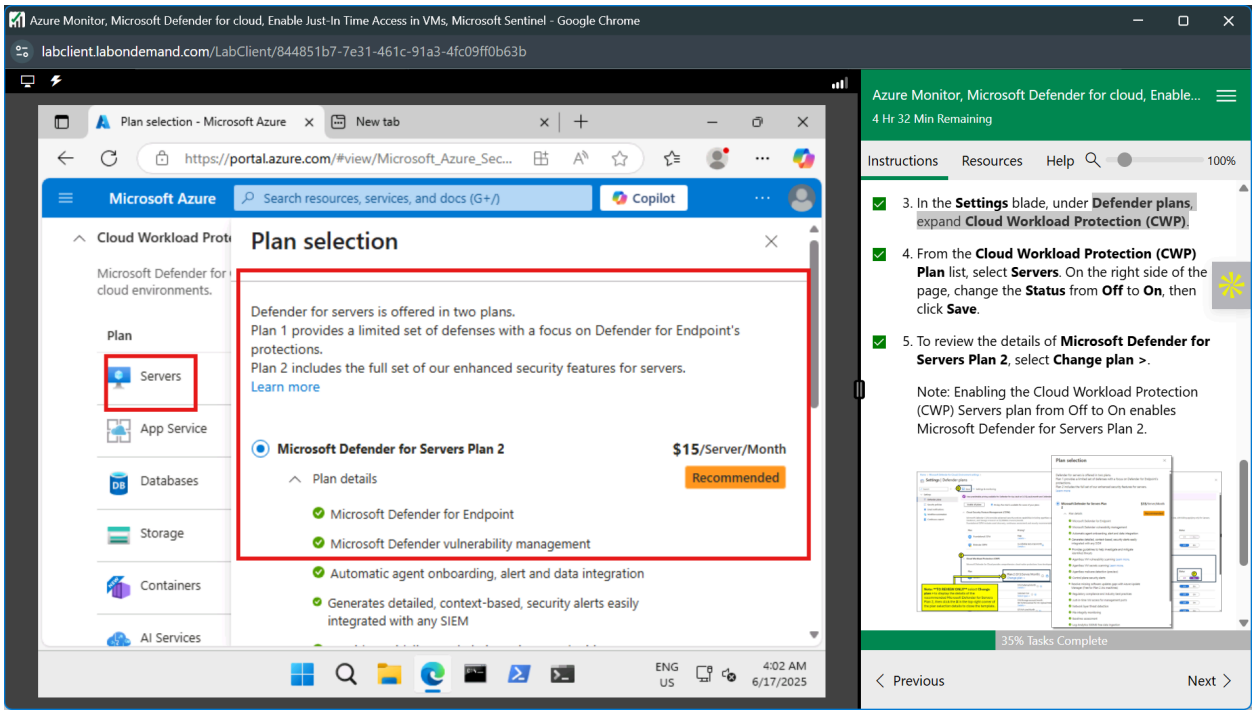
From this objective, we have deployed an Azure virtual machine, Log Analytics workspace, Azure storage account, and a data collection rule to collect events and performance counters from virtual machines with Azure Monitor Agent.

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.

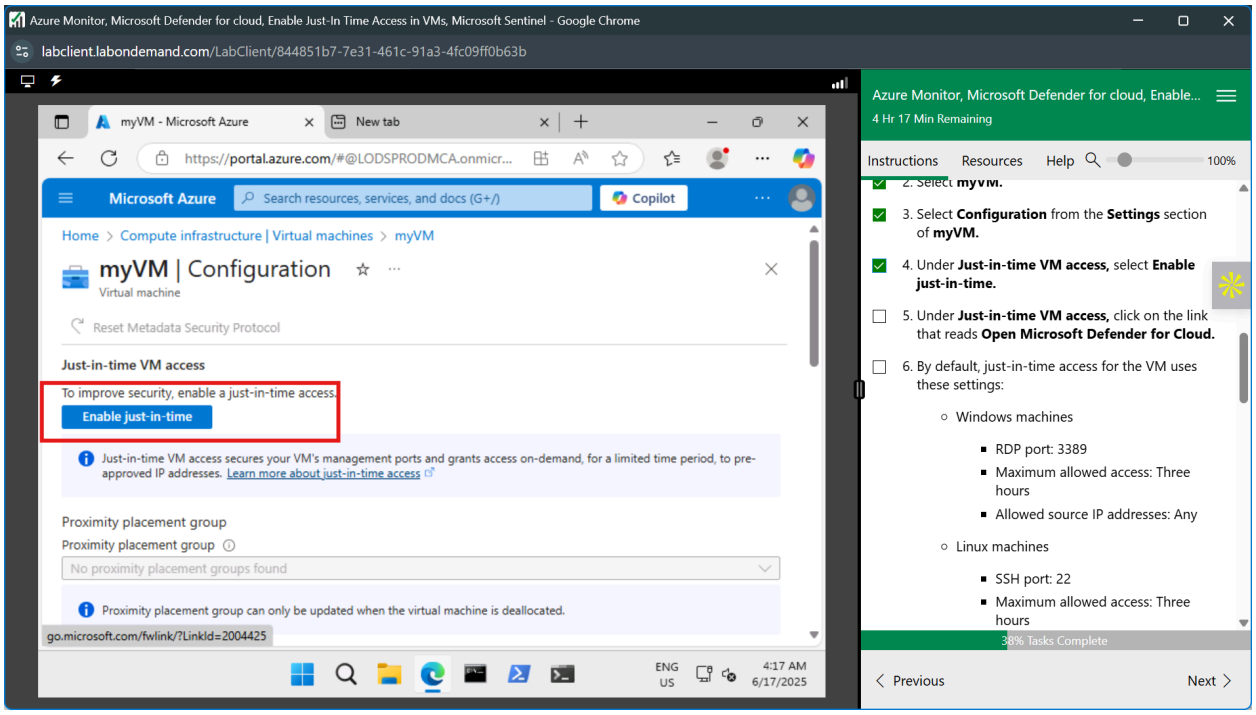


Enabling just-in-time access on VMs

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.

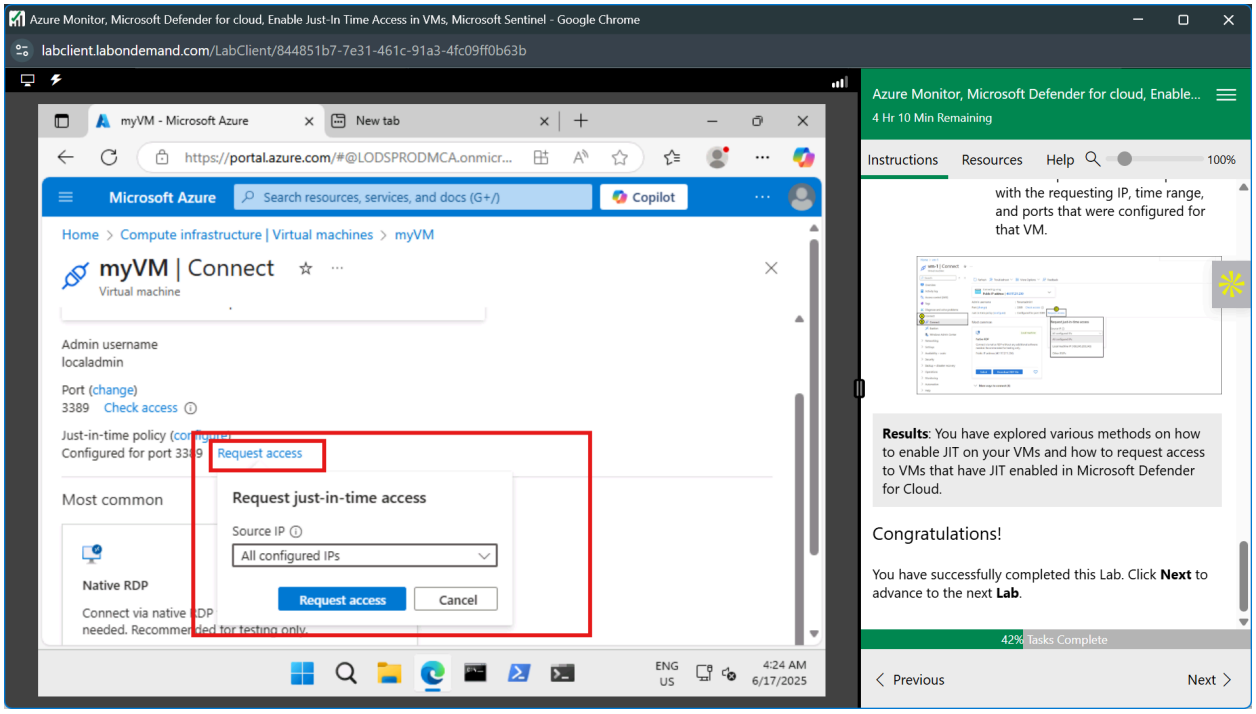
Enabling JIT on your VMs from Azure virtual machines

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



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.

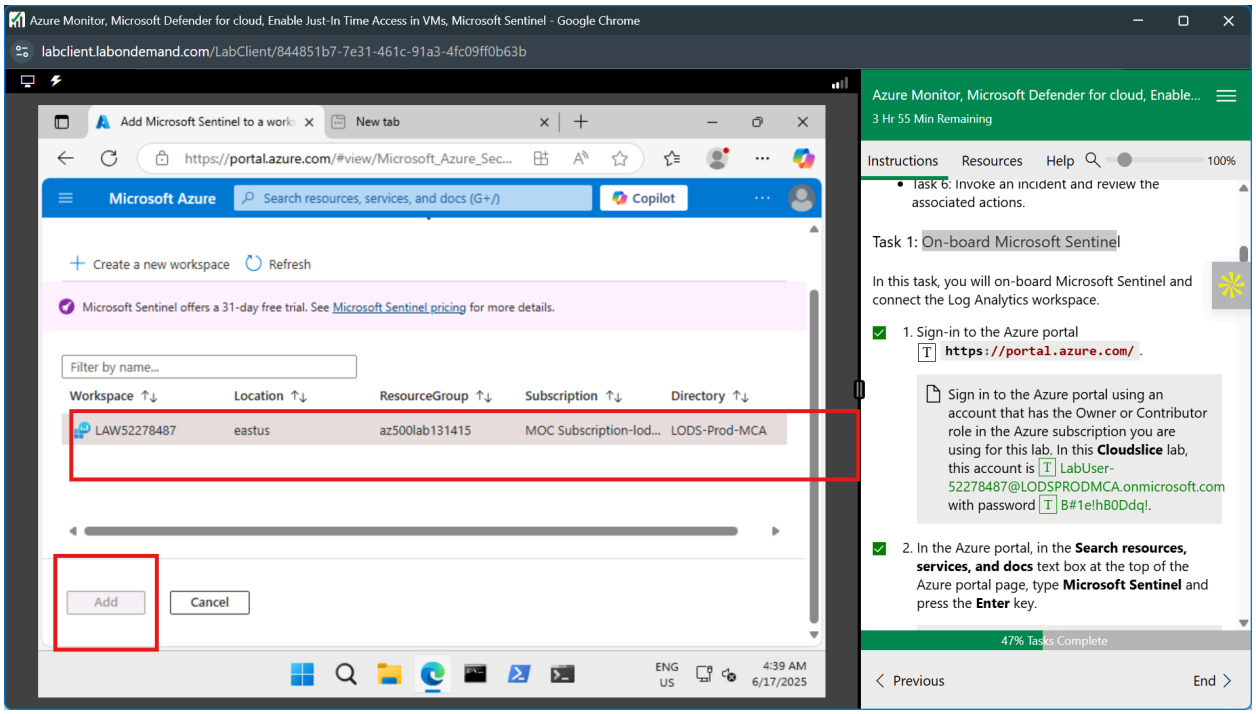


Microsoft Sentinel

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.

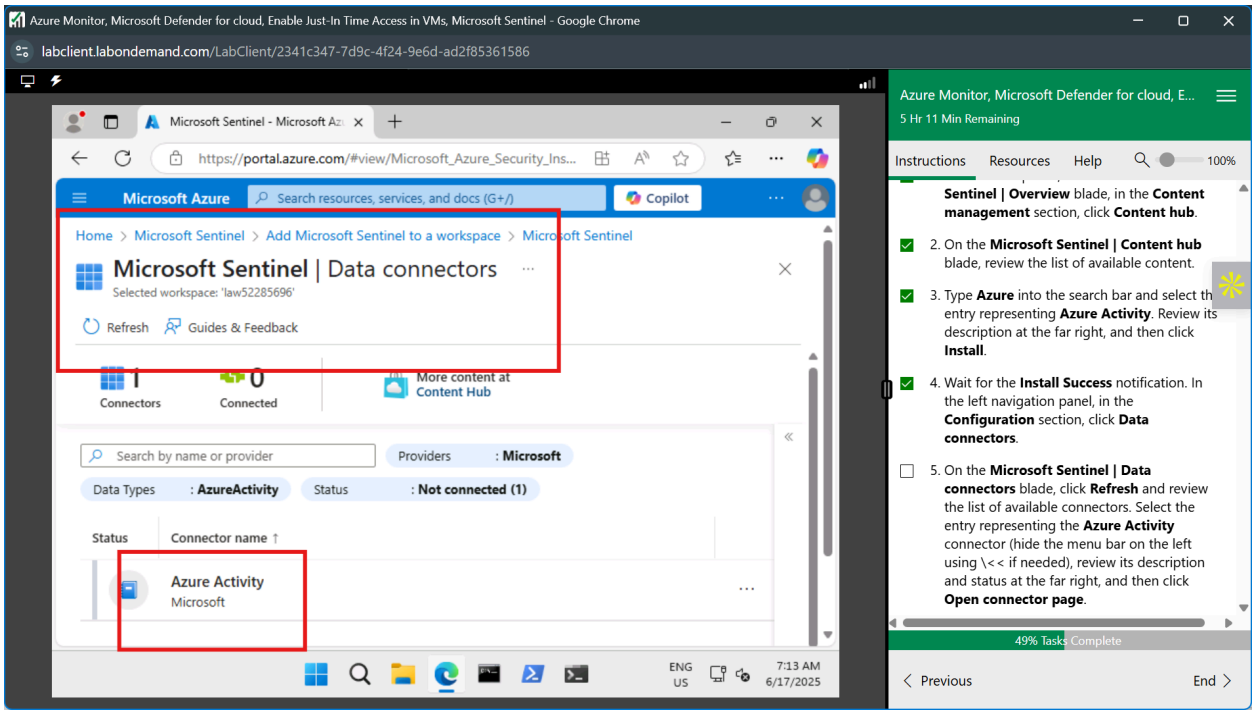
On-board Microsoft Sentinel

In this task, we will onboard MS Sentinel.

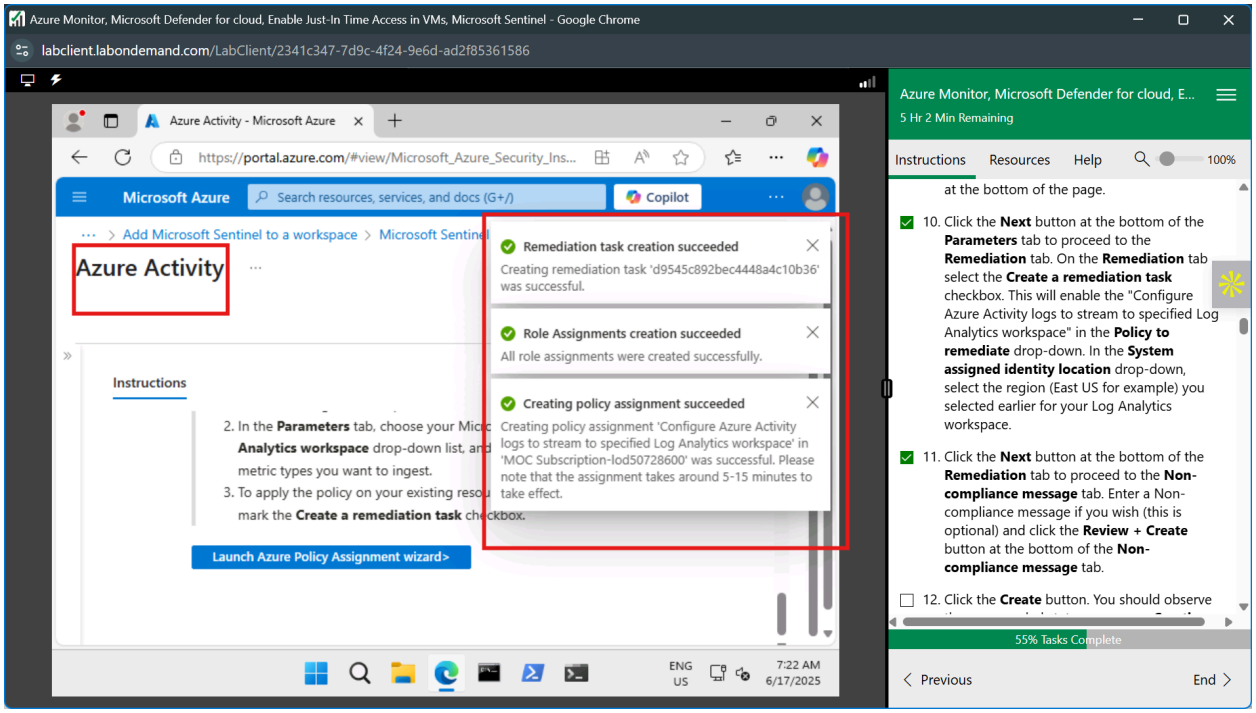


Configure Microsoft Sentinel to use the Azure Activity data connector.

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

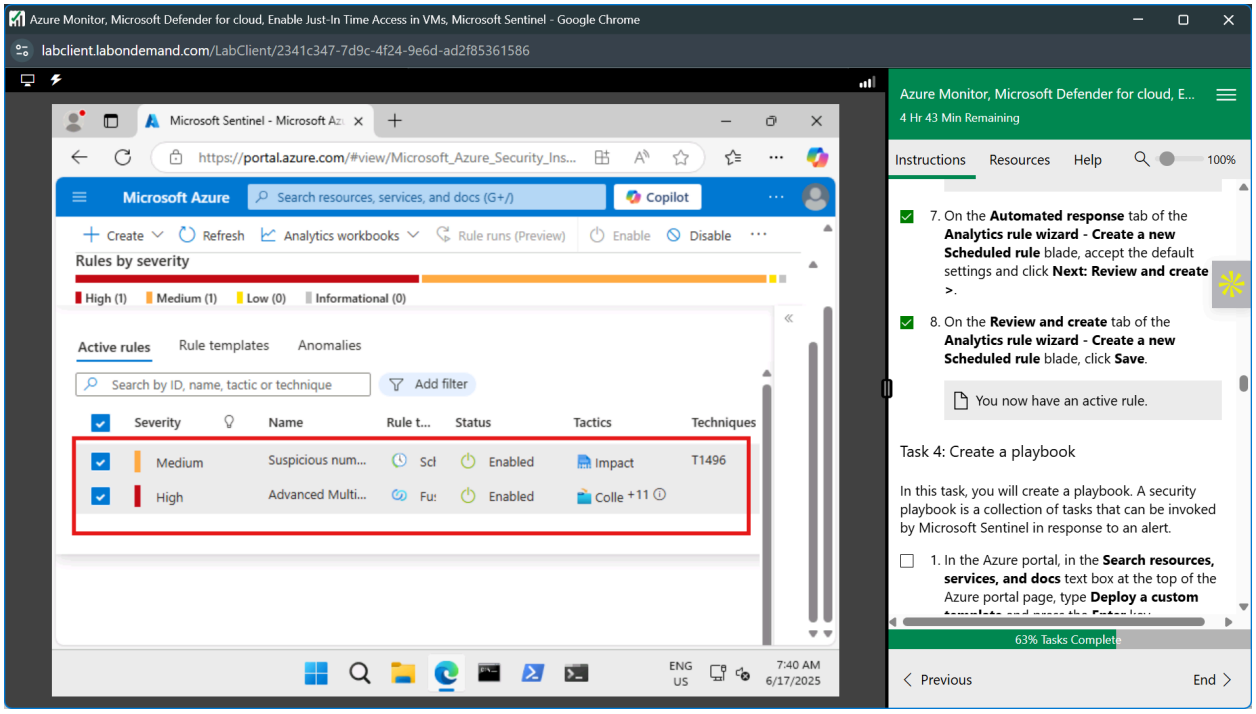


Configuration of policy assignment, remediation tasks for already existing resources and role assignment were created successfully as show below.



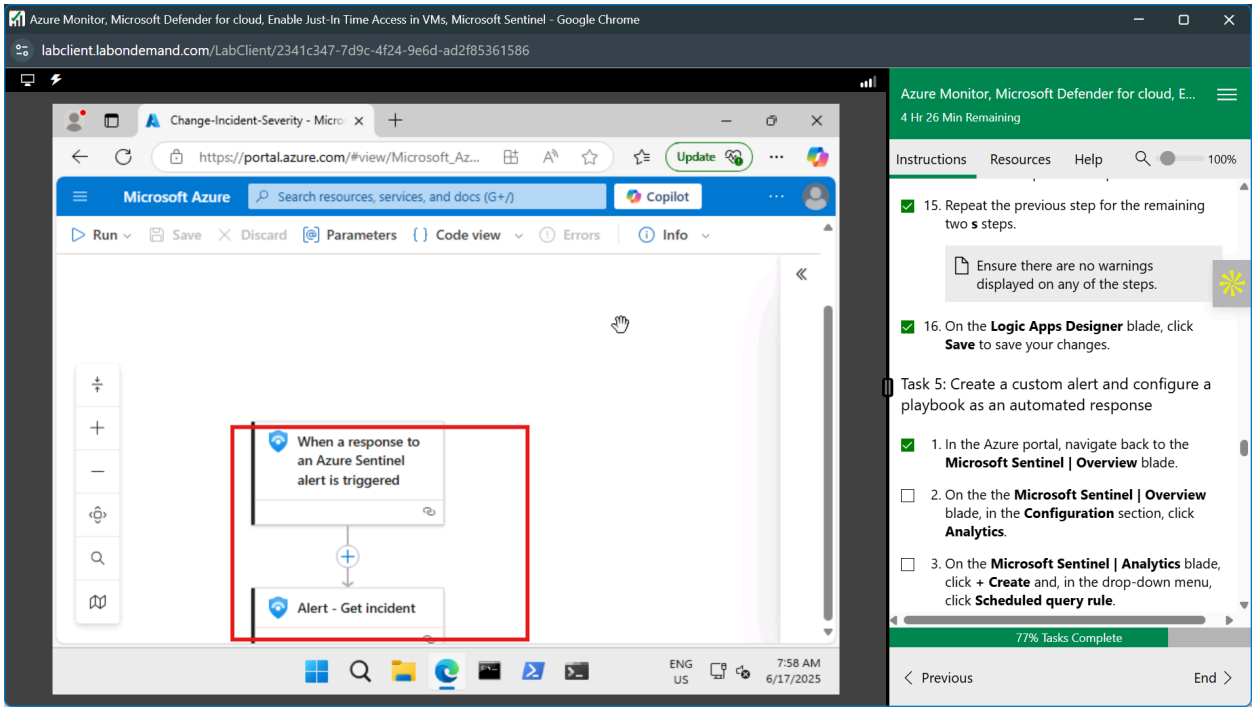
Create a rule that uses the Azure Activity data connector.

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



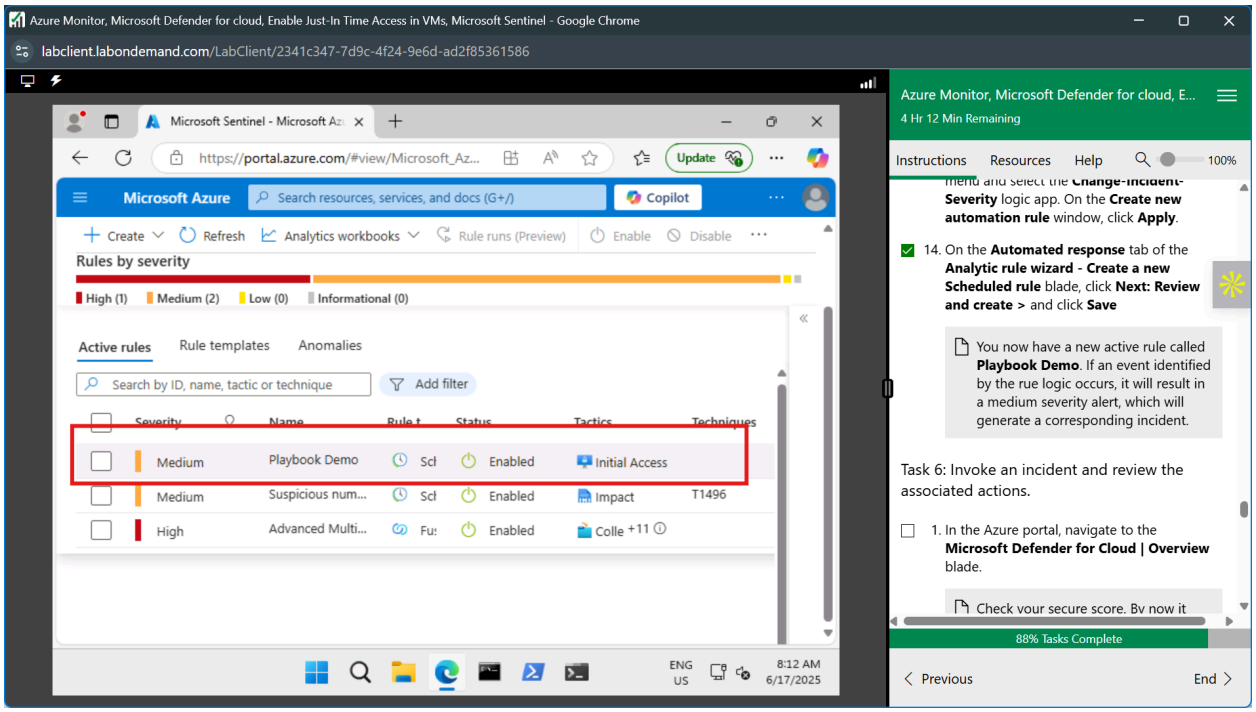
Create a playbook

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

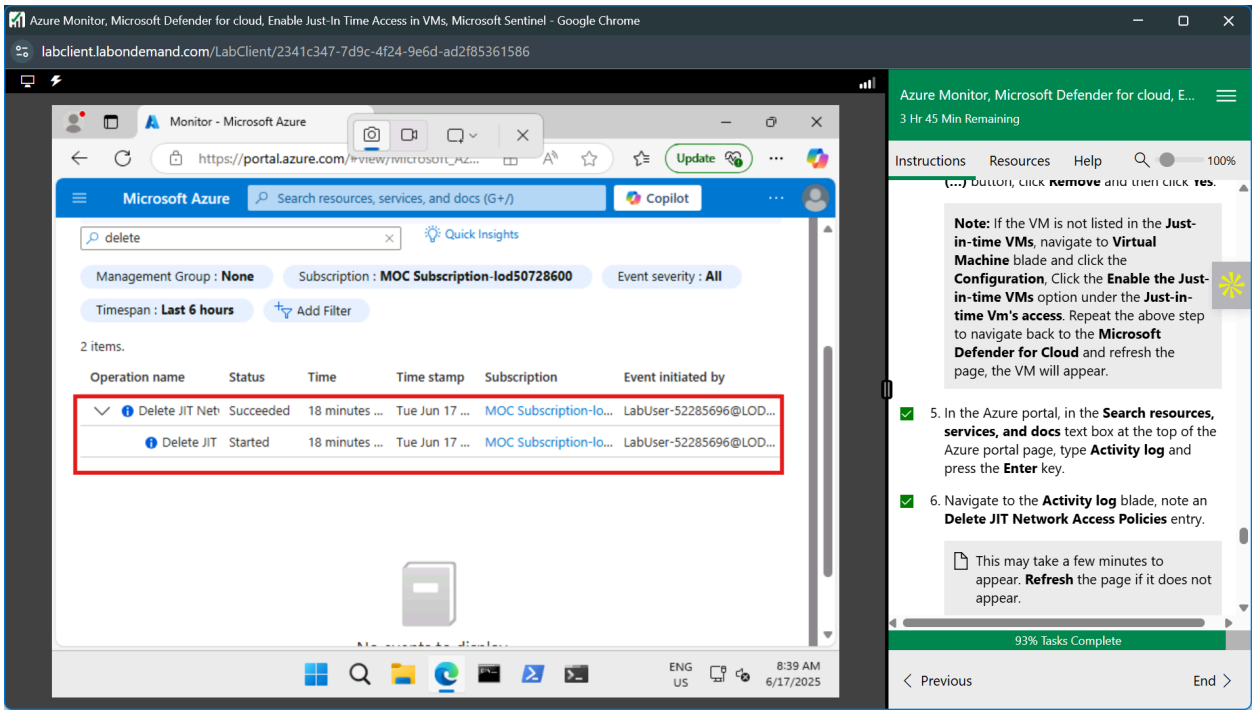
In this task, we create an analytic rule that identifies removal of Just-in-time VM access policies. This rule will then triger an alert and an automated response from our earlier deployed logic app.



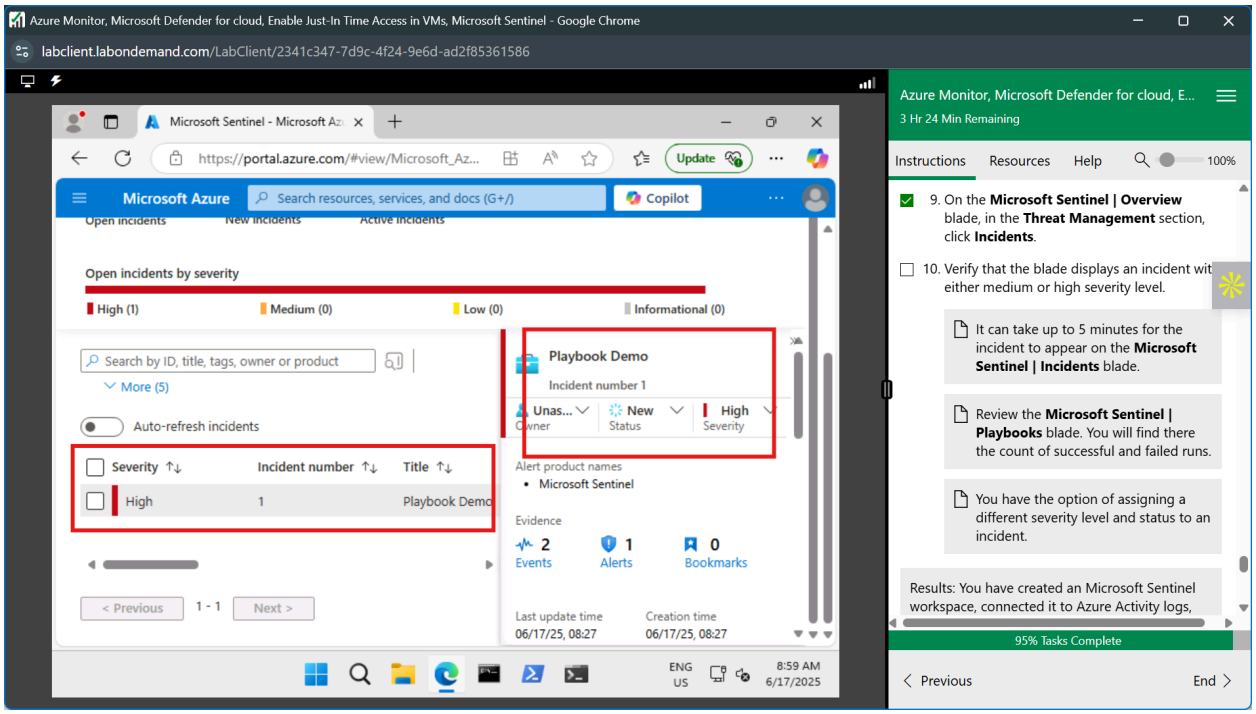
Invoke an incident and review the associated actions.

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



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



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.