BILLY GIBENDI
ADC-SOA01-24014
Microsoft ADC Cybersecurity Skilling Program

WEEK 7 ASSIGNMENT

Introduction

The purpose of this Azure Lab assignment is to explore and implement various Azure security technologies, including Azure Monitor, Microsoft Defender for Cloud, and Microsoft Sentinel. The lab exercises focus on deploying resources, configuring monitoring and security settings, and exploring the functionalities of these services.

Azure Monitor Lab

In the Azure Monitor lab, I performed several critical tasks to deploy and configure a virtual machine (VM) and set up monitoring for effective resource management. Below is a detailed account of the processes and code used to complete these tasks, focusing on the use of Azure CLI for seamless execution.

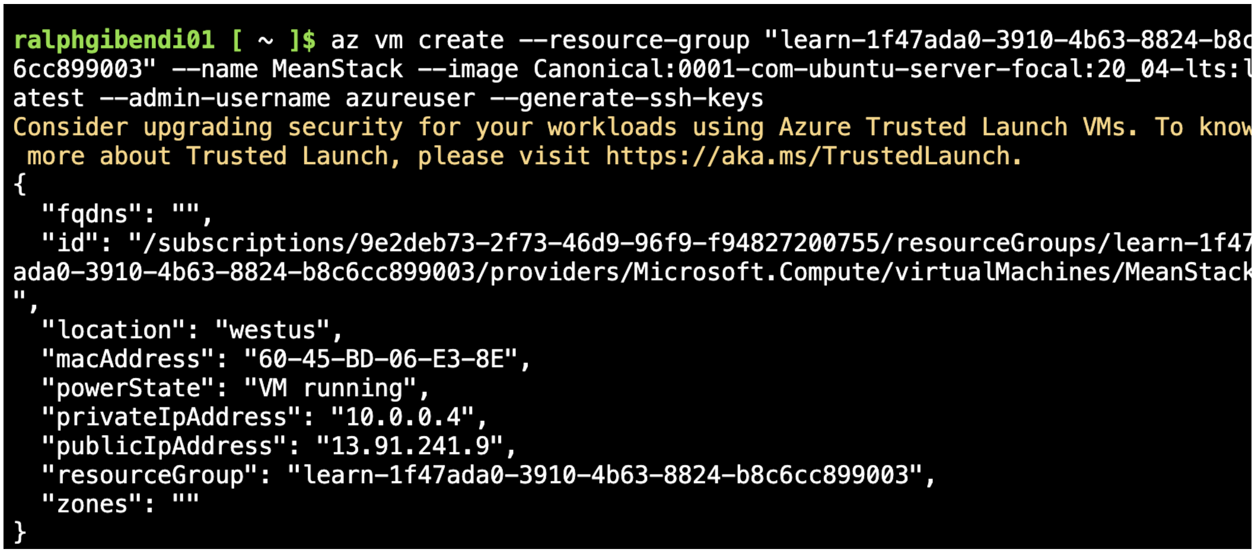
Exercise 1: Deploy an Azure Virtual Machine

To deploy a new Azure Virtual Machine named "MeanStack" in the East US region, I used the Azure CLI. Here is the step-by-step process:

1. Create the Virtual Machine:
   I executed the following Azure CLI command to create a VM with the specified configuration:

```
az vm create \
  --resource-group "learn-1f47ada0-3910-4b63-8824-b8c6cc899003" \
  --name MeanStack \
  --image Canonical:0001-com-ubuntu-server-focal:20_04-lts:latest \
  --admin-username azureuser \
  --generate-ssh-keys
```

This command created a VM with the Ubuntu Server 20.04 LTS image and generated SSH keys for secure access. The process took about two minutes, and upon completion, it provided output similar to this:

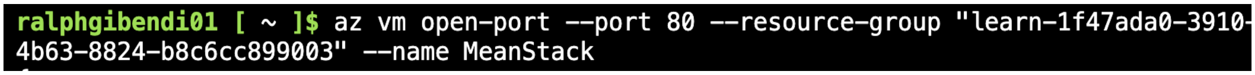


```
ralphgibendi01 [ ~ ]$ az vm create --resource-group "learn-1f47ada0-3910-4b63-8824-b8c
6cc899003" --name MeanStack --image Canonical:0001-com-ubuntu-server-focal:20_04-lts:l
atest --admin-username azureuser --generate-ssh-keys
Consider upgrading security for your workloads using Azure Trusted Launch VMs. To know
 more about Trusted Launch, please visit https://aka.ms/TrustedLaunch.
{
  "fqdns": "",
  "id": "/subscriptions/9e2deb73-2f73-46d9-96f9-f94827200755/resourceGroups/learn-1f47
ada0-3910-4b63-8824-b8c6cc899003/providers/Microsoft.Compute/virtualMachines/MeanStack
",
  "location": "westus",
  "macAddress": "60-45-BD-06-E3-8E",
  "powerState": "VM running",
  "privateIpAddress": "10.0.0.4",
  "publicIpAddress": "13.91.241.9",
  "resourceGroup": "learn-1f47ada0-3910-4b63-8824-b8c6cc899003",
  "zones": ""
}
```

The VM was named "MeanStack" for easy identification in future commands.

2. Open Port 80 for HTTP Traffic:

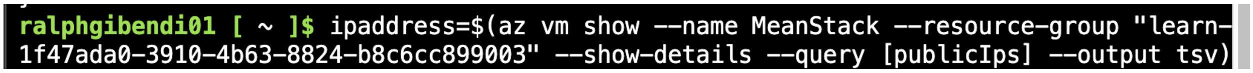
To allow incoming HTTP traffic to the web application, I opened port 80 using the following Azure CLI command:



```
ralphgibendi01 [ ~ ]$ az vm open-port --port 80 --resource-group "learn-1f47ada0-3910-
4b63-8824-b8c6cc899003" --name MeanStack
```

3. Create an SSH Connection to the VM:

I stored the VM's public IP address in a Bash variable named `ipaddress` by running:



```
ralphgibendi01 [ ~ ]$ ipaddress=$(az vm show --name MeanStack --resource-group "learn-
1f47ada0-3910-4b63-8824-b8c6cc899003" --show-details --query [publicIps] --output tsv)
```

Then, I connected to the VM via SSH using the command:

```
ssh azureuser@$ipaddress
```

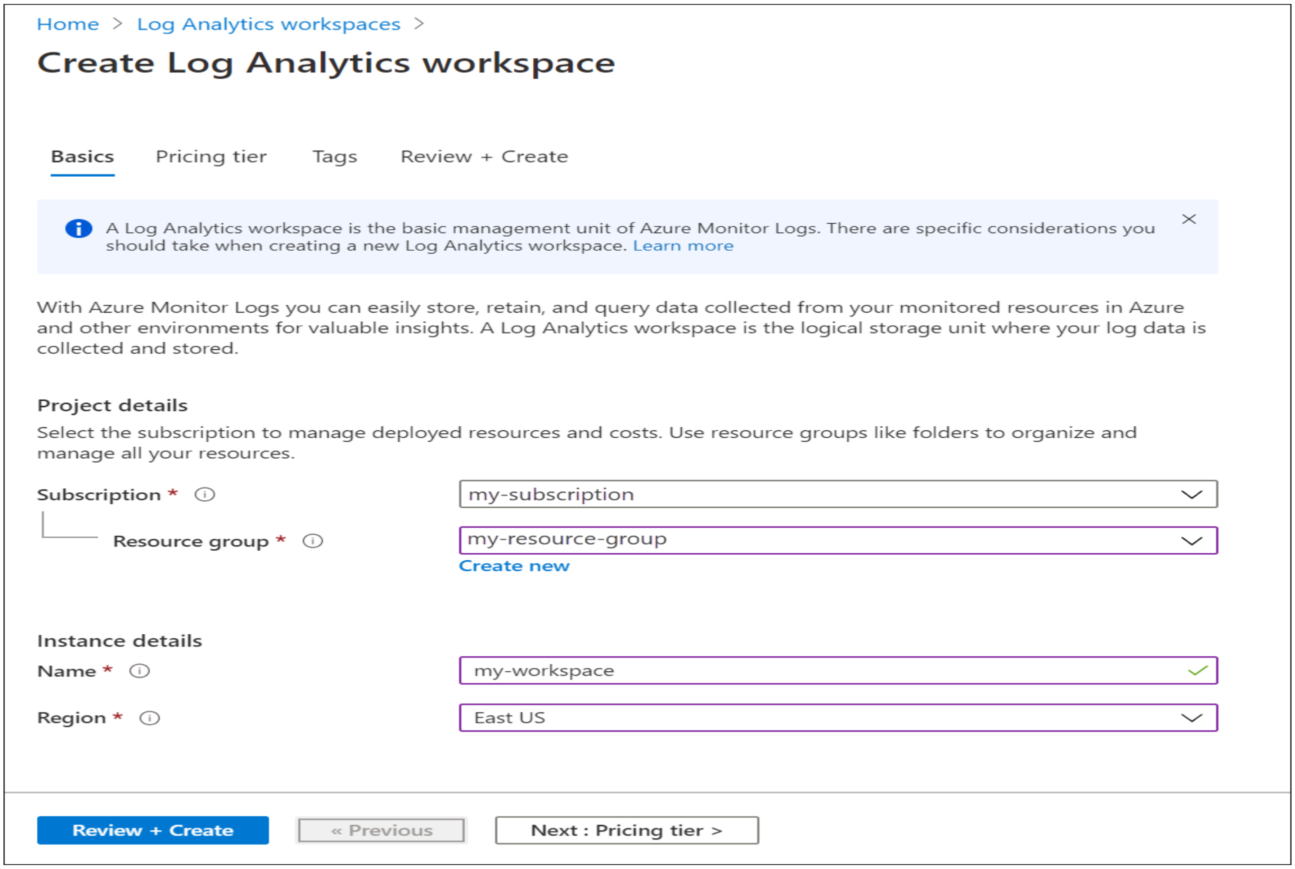
This SSH connection allowed me to securely access and configure the software on the VM.

Exercise 2: Create a Log Analytics Workspace

I created a Log Analytics workspace named "my-workspace" to collect and analyze logs from my Azure resources. Here's how I did it:

Creating the Workspace: From the Azure portal, I navigated to the "Log Analytics workspaces" section and clicked on "Add." I provided a name for the workspace ("my-workspace") and selected the East US region to ensure it was in close proximity to my VM for better performance and reduced latency.

Configuring Pricing: I selected the "Pay-as-you-go" pricing tier, which offers flexibility and cost-effectiveness, especially suitable for my lab setup where I expect variable usage.



Create Log Analytics workspace

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

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

Subscription * : my-subscription

Resource group * : my-resource-group

Instance details

Name * : my-workspace

Region * : East US

Exercise 3: Create an Azure Storage Account

For this exercise, I set up an Azure Storage Account named "mystorageaccount" to store and manage data. Here are the detailed steps:

Creating the Storage Account: In the Azure portal, I went to the "Storage accounts" section and clicked on "Create." I provided the name "mystorageaccount" and chose the East US region to maintain consistency with my other resources.

Enabling Blob Soft Delete: To protect against accidental deletions, I enabled the blob soft delete feature and set the retention period to 7 days. This ensures that any deleted blobs can be recovered within this period, adding an extra layer of data protection.

Exercise 4: Create a Data Collection Rule

The final exercise involved setting up a Data Collection Rule named "myDataCollectionRule" to collect performance metrics from my VM and send them to my Log Analytics workspace. Here's how I accomplished this:

Creating the Data Collection Rule: From the Azure portal, I navigated to the "Monitor" service and selected "Data Collection Rules." I clicked on "Add" and provided the name "myDataCollectionRule."

Configuring Performance Counters: I specified that the rule should collect performance counters for CPU and memory usage from the "myVM" virtual machine. This would enable me to monitor the VM's performance and detect any potential issues.

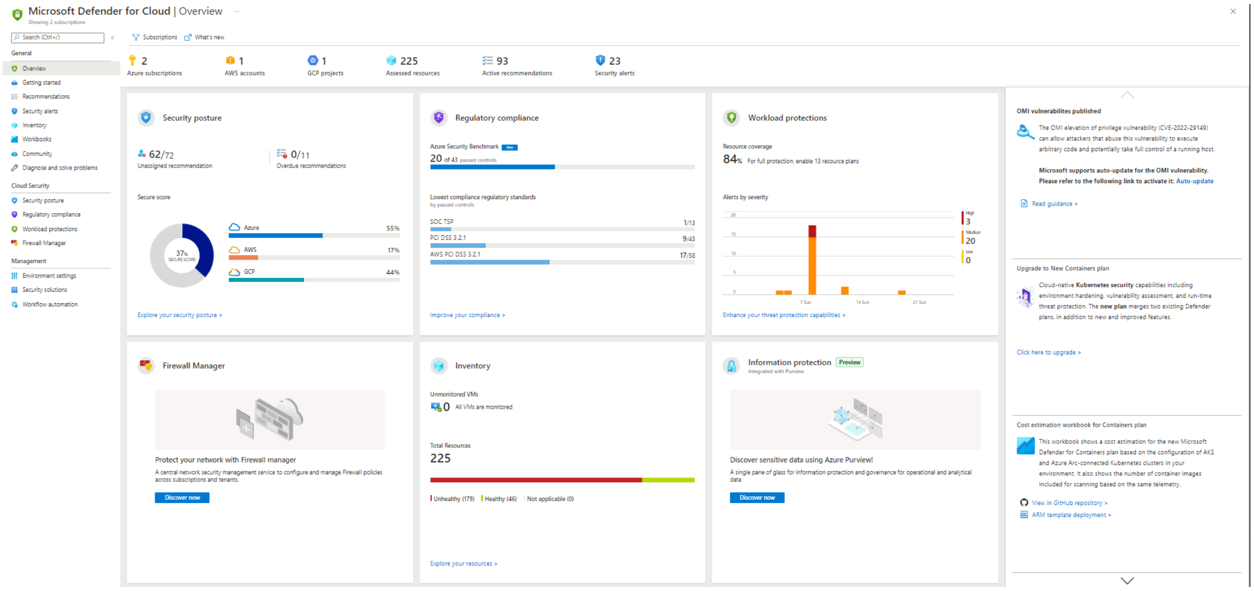
Linking to Log Analytics Workspace: Finally, I linked the data collection rule to the "myWorkspace" Log Analytics workspace. This ensures that all collected data is sent to the workspace for analysis and visualization.

Microsoft Defender for Cloud Lab

In this lab, I focused on implementing Microsoft Defender for Cloud to enhance the security posture of my Azure environment. Below are the steps I followed to set up and configure Microsoft Defender for Cloud.

Exercise 1: Implement Microsoft Defender for Cloud
Enabling Microsoft Defender for Cloud:

I started by logging into the Azure portal and navigating to the Microsoft Defender for Cloud service.
From there, I enabled Microsoft Defender for Cloud on my subscription to leverage its comprehensive security management and threat protection capabilities.



Protect your network with Firewall manager

A central network security management service to configure and manage Firewall policies across subscriptions and tenants.

Discover sensitive data using Azure Purview!

A single pane of glass for information protection and governance for operational and analytical data

OMI vulnerabilites published

The OMI elevation of privilege vulnerability (CVE-2022-29149) can allow attackers that abuse this vulnerability to execute arbitrary code and potentially take full control of a running host.

Microsoft supports auto-update for the OMI vulnerability. Please refer to the following link to activate it: Auto-update

Upgrade to New Containers plan

Cloud-native **Kubernetes security** capabilities including environment hardening, vulnerability assessment, and run-time threat protection. The **new plan** merges two existing Defender plans, in addition to new and improved features.

Cost estimation workbook for Containers plan

This workbook shows a cost estimation for the new Microsoft Defender for Containers plan based on the configuration of AKS and Azure Arc-connected Kubernetes clusters in your environment. It also shows the number of container images included for scanning based on the same telemetry.

Configuring the Pricing Tier:

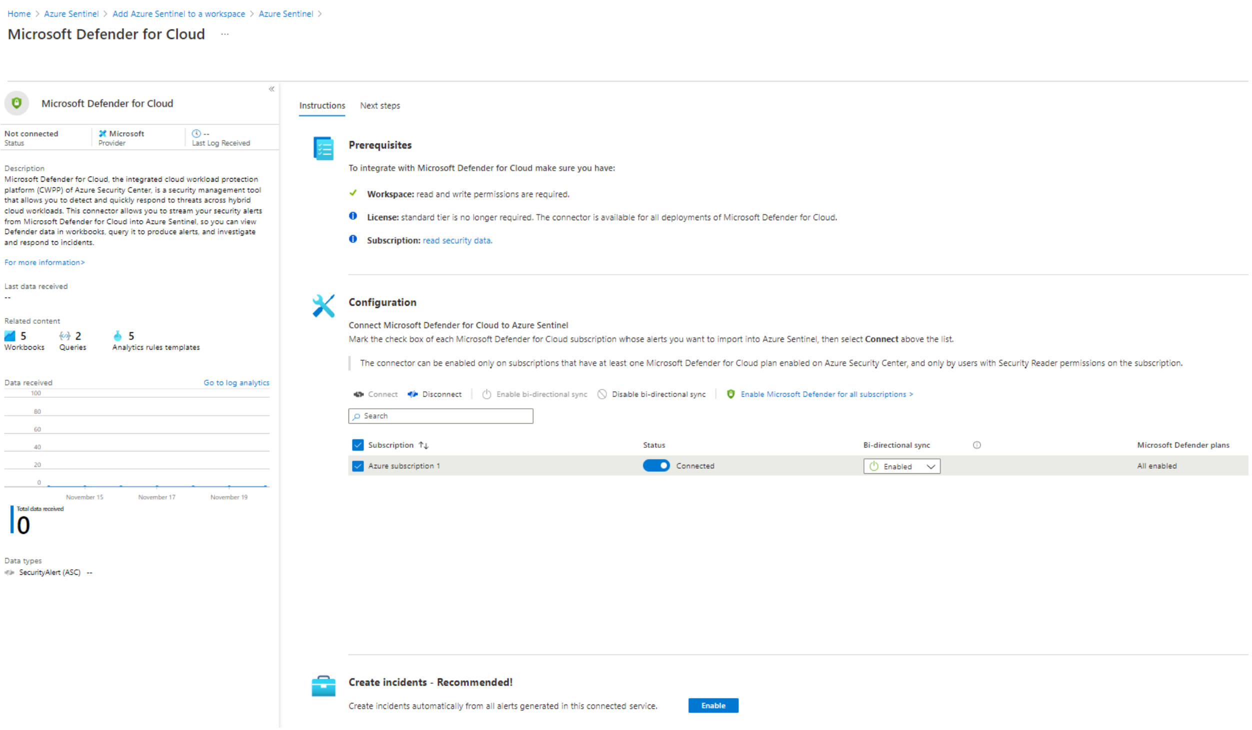
I configured the pricing tier to "Standard" for all supported resource types. The Standard tier offers advanced security features, including continuous assessment, threat protection, and vulnerability management, which are essential for a robust security posture.

Enabling Microsoft Defender Plans:

Azure Defender for App Service: I enabled this plan to provide advanced threat protection for my web applications. This includes monitoring for common web vulnerabilities and offering actionable recommendations to secure the applications.
Azure Defender for Storage: This plan was enabled to protect my storage accounts against threats such as data exfiltration, malware, and ransomware. It provides anomaly detection and alerts for any unusual activities in my storage accounts.
Azure Defender for Kubernetes: To secure my containerized workloads, I enabled Azure Defender for Kubernetes. This plan offers threat detection for Kubernetes clusters, including monitoring for suspicious activities and providing insights into potential vulnerabilities within the clusters.

Microsoft Sentinel Lab

In this lab, I focused on implementing Microsoft Sentinel, a cloud-native security information and event management (SIEM) and security orchestration automated response (SOAR) solution. This setup provided me with a powerful platform to detect, prevent, and respond to security threats within my Azure environment. Below are the detailed steps I followed to set up Microsoft Sentinel.


Home > Azure Sentinel > Add Azure Sentinel to a workspace > Azure Sentinel >

Microsoft Defender for Cloud ···

Microsoft Defender for Cloud

Not connected
Status

Microsoft
Provider

--
Last Log Received

Description
Microsoft Defender for Cloud, the integrated cloud workload protection platform (CWPP) of Azure Security Center, is a security management tool that allows you to detect and quickly respond to threats across hybrid cloud workloads. This connector allows you to stream your security alerts from Microsoft Defender for Cloud into Azure Sentinel, so you can view Defender data in workbooks, query it to produce alerts, and investigate and respond to incidents.

For more information>

Last data received
--

Related content
5 Workbooks
2 Queries
5 Analytics rules templates

Data types
SecurityAlert (ASC) --

Prerequisites

To integrate with Microsoft Defender for Cloud make sure you have:

✓ **Workspace:** read and write permissions are required.

License: standard tier is no longer required. The connector is available for all deployments of Microsoft Defender for Cloud.

Subscription: read security data.

Configuration

Connect Microsoft Defender for Cloud to Azure Sentinel
Mark the check box of each Microsoft Defender for Cloud subscription whose alerts you want to import into Azure Sentinel, then select **Connect** above the list.

> The connector can be enabled only on subscriptions that have at least one Microsoft Defender for Cloud plan enabled on Azure Security Center, and only by users with Security Reader permissions on the subscription.

Connect
Disconnect
Enable bi-directional sync
Disable bi-directional sync
Enable Microsoft Defender for all subscriptions >
Search

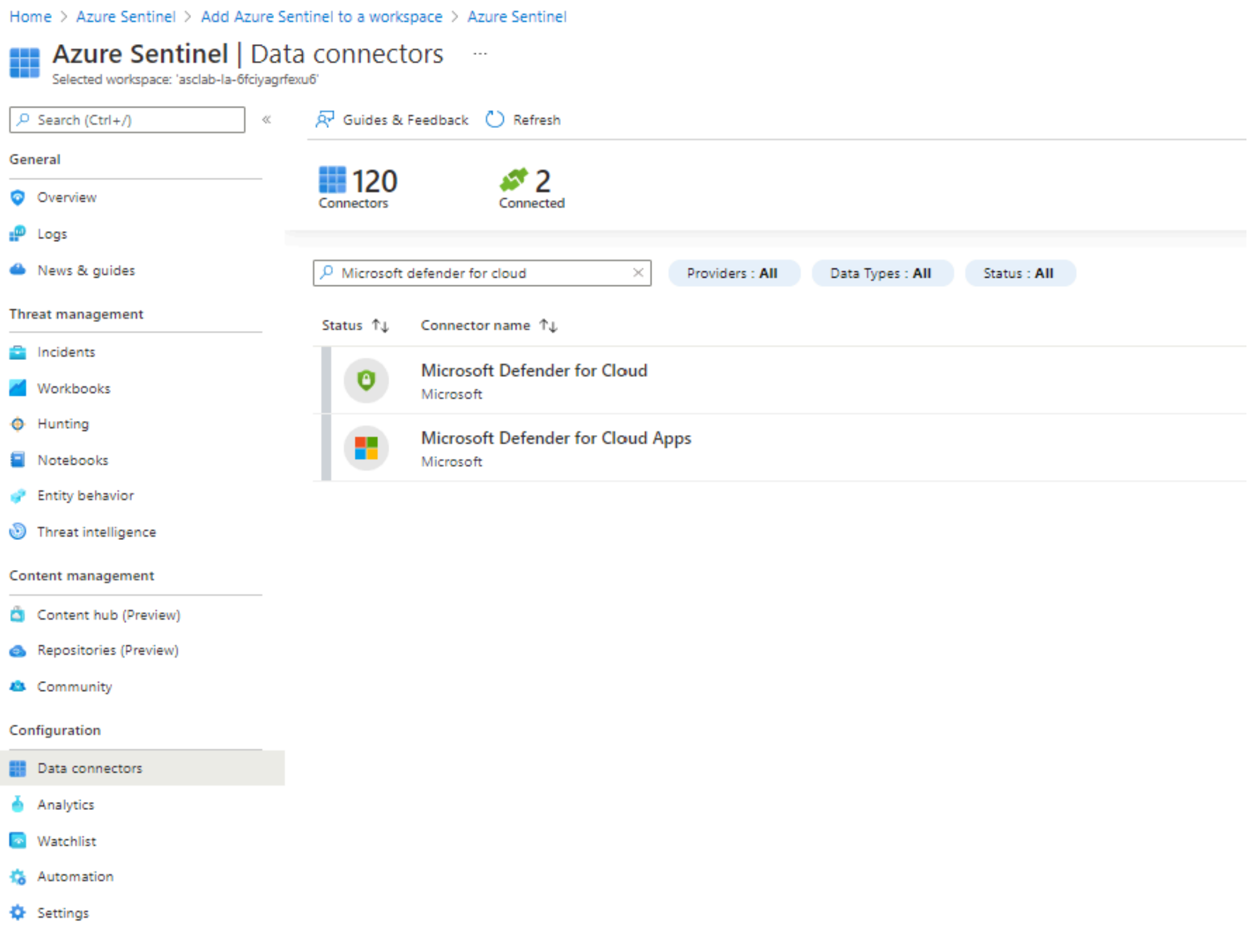
☑ Subscription ↑↓	Status	Bi-directional sync	Microsoft Defender plans
☑ Azure subscription 1	Connected	Enabled	All enabled

Create incidents - Recommended!

Create incidents automatically from all alerts generated in this connected service. Enable

Exercise 1: Implement Microsoft Sentinel
Creating a New Microsoft Sentinel Workspace:

I began by logging into the Azure portal and navigating to Microsoft Sentinel.
I created a new Microsoft Sentinel workspace named "mySentinelWorkspace" in the East US region. This workspace serves as the centralized hub for collecting and analyzing security data from various sources.



Azure Sentinel | Data connectors

Selected workspace: 'asclab-la-6fciyagrfexu6'

120 Connectors

2 Connected

Microsoft defender for cloud

Status	Connector name
	Microsoft Defender for Cloud Microsoft
	Microsoft Defender for Cloud Apps Microsoft

Onboarding a Virtual Machine as a Data Source:

To gather security-related data from my infrastructure, I onboarded the "myVM" virtual machine as a data source for Microsoft Sentinel.
This involved configuring the virtual machine to send logs and performance data to the "mySentinelWorkspace" for analysis and threat detection.
Enabling Microsoft Sentinel Data Connectors:

Azure Active Directory Identity Protection: I enabled this data connector to monitor identity-related activities and potential security threats targeting Azure Active Directory (AAD). This integration allows Sentinel to collect and analyze data on user sign-ins, risky sign-ins, and other identity protection events.
Azure Security Center: I also enabled the Azure Security Center data connector to gather security alerts and recommendations from Azure Security Center. This data integration enhances Sentinel's ability to detect and respond to security incidents by leveraging the comprehensive security insights provided by Azure Security Center.

Highlights

- Always double-check the workspace and storage account names and ensure they match the specified configurations.

Conclusion

The Azure Monitor lab provided a comprehensive hands-on experience in deploying and configuring Azure resources, setting up monitoring solutions, and ensuring secure access and data management. By utilizing Azure CLI, I was able to automate and streamline the deployment and configuration processes effectively. These exercises have enhanced my skills in cloud resource management, monitoring, and security, equipping me with practical knowledge to handle real-world scenarios efficiently.

The Microsoft Defender for Cloud lab felt like putting on a suit of armor for my virtual machine. I activated these advanced security features to protect it from all angles. It was like choosing the right shield for each type of threat, with different Defender plans for different parts of my system. This lab made it clear that strong security requires a layered approach, and I learned how to configure and manage these powerful tools within Azure.

The Microsoft Sentinel lab felt like building my own security war room. I set up a central platform to collect data from everywhere – like having a team of informants keeping me updated on any suspicious activity. By connecting different Azure services, I gave Sentinel a broader view of the landscape, making it even better at detecting and responding to threats. This lab emphasized the importance of a comprehensive security posture, and I learned how to use Microsoft Sentinel to be a proactive defender of my cloud environment.

These labs have given me a complete picture of cloud security management in Azure. Each one built on the skills from the last, and now I feel confident in my ability to monitor, protect, and respond to security threats in a structured and effective way. From the initial setup in Azure Monitor to the advanced security measures of Defender for Cloud and the comprehensive monitoring of Sentinel, these labs have equipped me with the practical experience I need to succeed. As a graduate of the Microsoft ADC Cybersecurity Skilling Program, I'm no longer just a trainee – I'm ready to face real-world cybersecurity challenges and keep the cloud safe.