Microsoft ADC Cybersecurity Skilling Program

Week 9 Lab Assignment

Student Name: Vincent Onchieku Collins

Student ID: ADC-CSS02-25052

Introduction

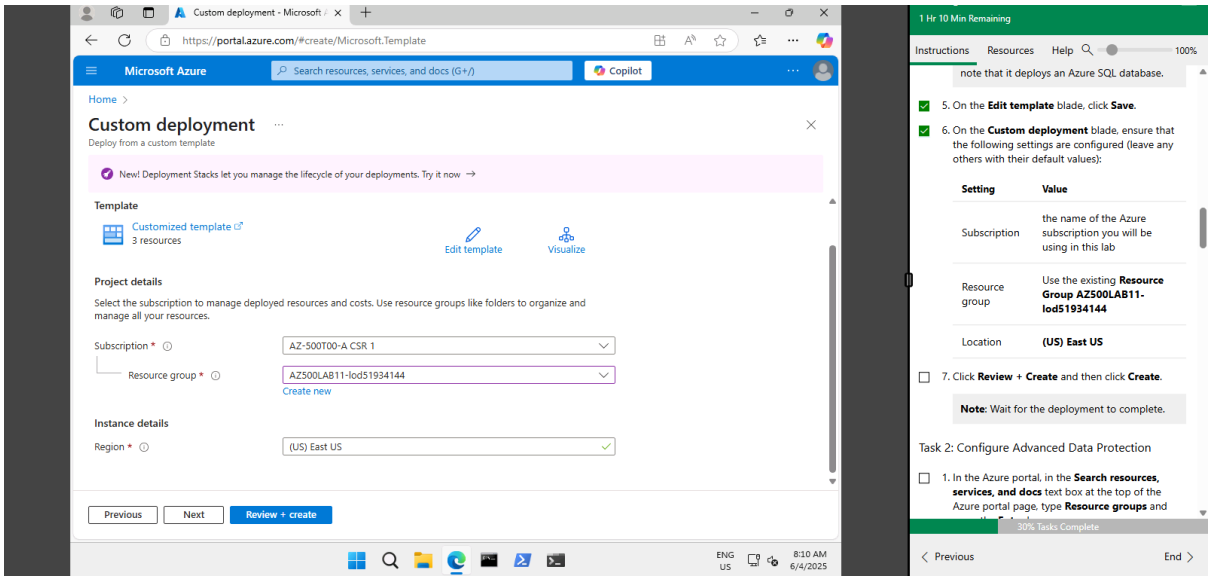
In this exercise, I implemented a range of security features for an Azure SQL Database to strengthen data protection, ensure regulatory compliance, and enhance monitoring and auditing capabilities. The main objective was to safeguard the database against threats such as SQL injection and data exfiltration, as well as classify sensitive data and audit access and activity logs. This hands-on lab guided me through deploying the SQL infrastructure, configuring Microsoft Defender for SQL, classifying data, and setting up auditing at both the server and database levels. These steps represent fundamental tasks in ensuring a secure, compliant, and monitored data environment within Azure.
It included the following tasks:

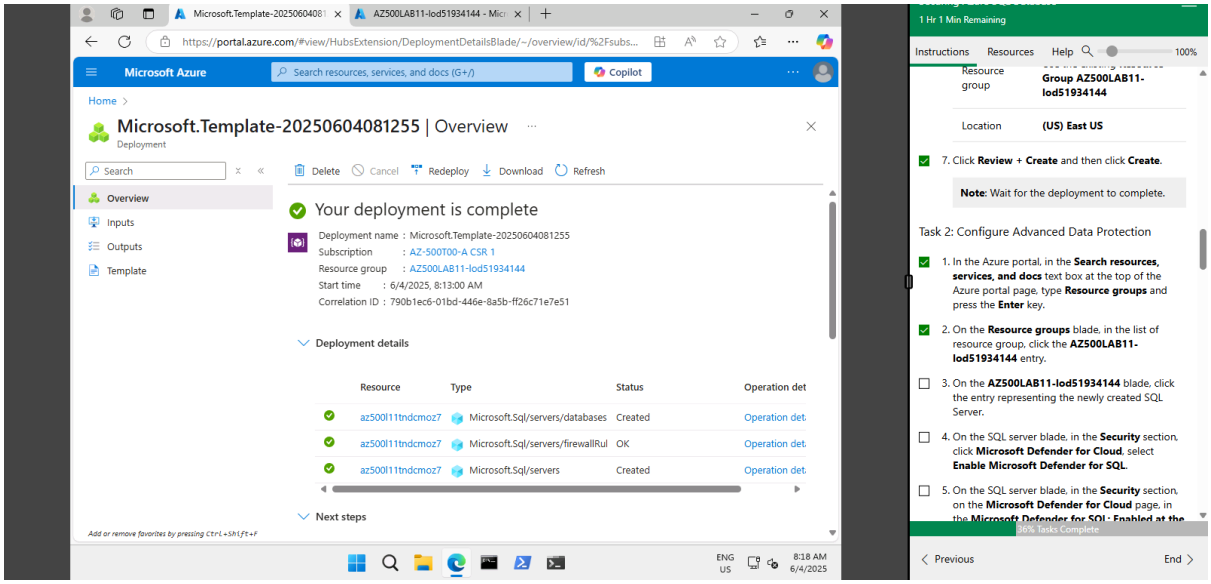
- **Task 1: Deploy an Azure SQL Database**
- **Task 2: Configure Advanced Data Protection**
- **Task 3: Configure Data Classification**
- **Task 4: Configure Auditing**

Tasks:

Task 1: Deploy an Azure SQL Database

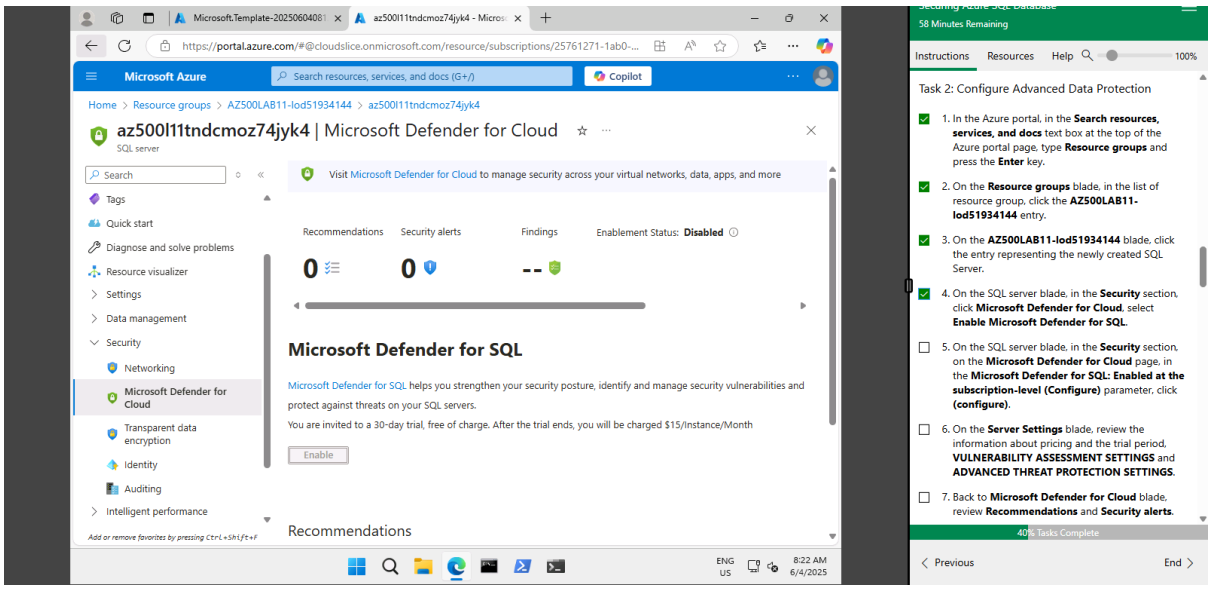
The first task involved deploying an Azure SQL Database using a pre-defined ARM (Azure Resource Manager) template. I accessed the “Deploy a custom template” feature in the Azure portal, loaded the azuredeploy.json file, and set the deployment parameters such as subscription, existing resource group, and location (East US). This template deployed the SQL server and database infrastructure necessary for the lab. This task was essential as it laid the foundation for applying subsequent security features. Reviewing the template before deployment gave insight into the infrastructure-as-code approach to resource provisioning.

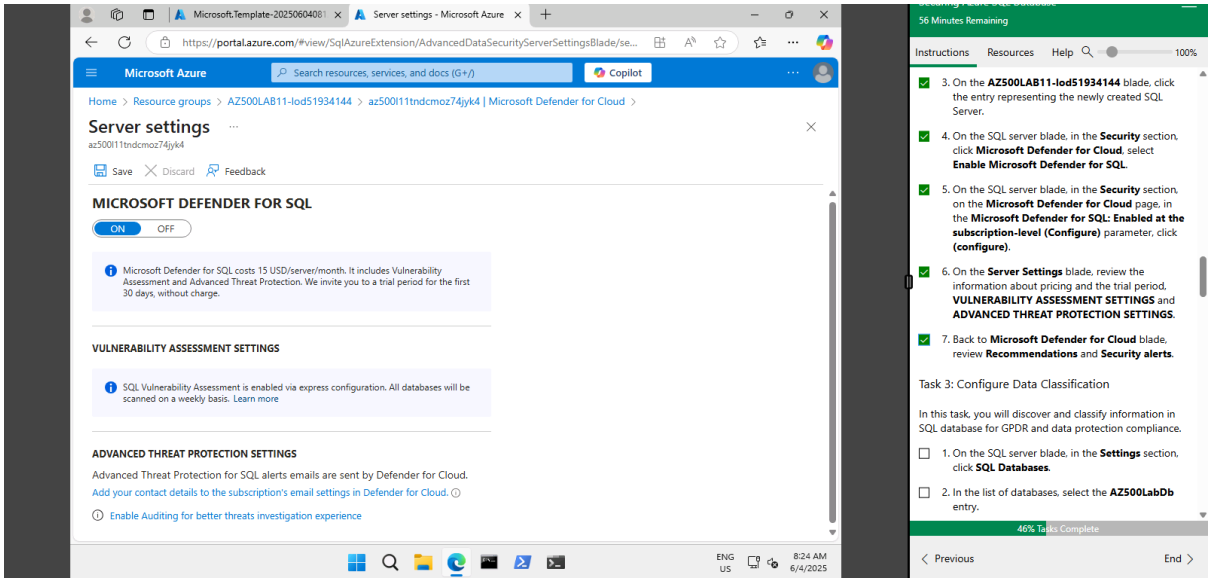

Custom deployment - Microsoft
https://portal.azure.com/#create/Microsoft.Template
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
Custom deployment
Deploy from a custom template
New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now
Template
Customized template
3 resources
Edit template
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 *
AZ-500T00-A CSR 1
Resource group *
AZ500LAB11-lod51934144
Create new
Instance details
Region *
(US) East US
Previous
Next
Review + create
ENG
US
8:10 AM
6/4/2025
1 Hr 10 Min Remaining
Instructions
Resources
Help
100%
note that it deploys an Azure SQL database.
5. On the Edit template blade, click Save.
6. 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 will be using in this lab
Resource group
Use the existing Resource Group AZ500LAB11-lod51934144
Location
(US) East US
7. Click Review + Create and then click Create.
Note: Wait for the deployment to complete.
Task 2: Configure Advanced Data Protection
1. 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
30% Tasks Complete
Previous
End


Microsoft.Template-20250604081255 | Overview
AZ500LAB11-lod51934144 - Micr
https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubs...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
Microsoft.Template-20250604081255 | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Your deployment is complete
Deployment name : Microsoft.Template-20250604081255
Subscription : AZ-500T00-A CSR 1
Resource group : AZ500LAB11-lod51934144
Start time : 6/4/2025, 8:13:00 AM
Correlation ID : 790b1ec6-01bd-446e-8a5b-ff26c71e7e51
Deployment details
Resource
Type
Status
Operation det
az500l11tndcmoz7
Microsoft.Sql/servers/databases
Created
Operation det
az500l11tndcmoz7
Microsoft.Sql/servers/firewallRul
OK
Operation det
az500l11tndcmoz7
Microsoft.Sql/servers
Created
Operation det
Next steps
Add or remove favorites by pressing Ctrl+Shift+F
ENG
US
8:18 AM
6/4/2025
1 Hr 1 Min Remaining
Instructions
Resources
Help
100%
Resource group
Group AZ500LAB11-lod51934144
Location
(US) East US
7. Click Review + Create and then click Create.
Note: Wait for the deployment to complete.
Task 2: Configure Advanced Data Protection
1. 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.
2. On the Resource groups blade, in the list of resource group, click the AZ500LAB11-lod51934144 entry.
3. On the AZ500LAB11-lod51934144 blade, click the entry representing the newly created SQL Server.
4. On the SQL server blade, in the Security section, click Microsoft Defender for Cloud, select Enable Microsoft Defender for SQL.
5. On the SQL server blade, in the Security section, on the Microsoft Defender for Cloud page, in
36% Tasks Complete
Previous
End

Task 2: Configure Advanced Data Protection

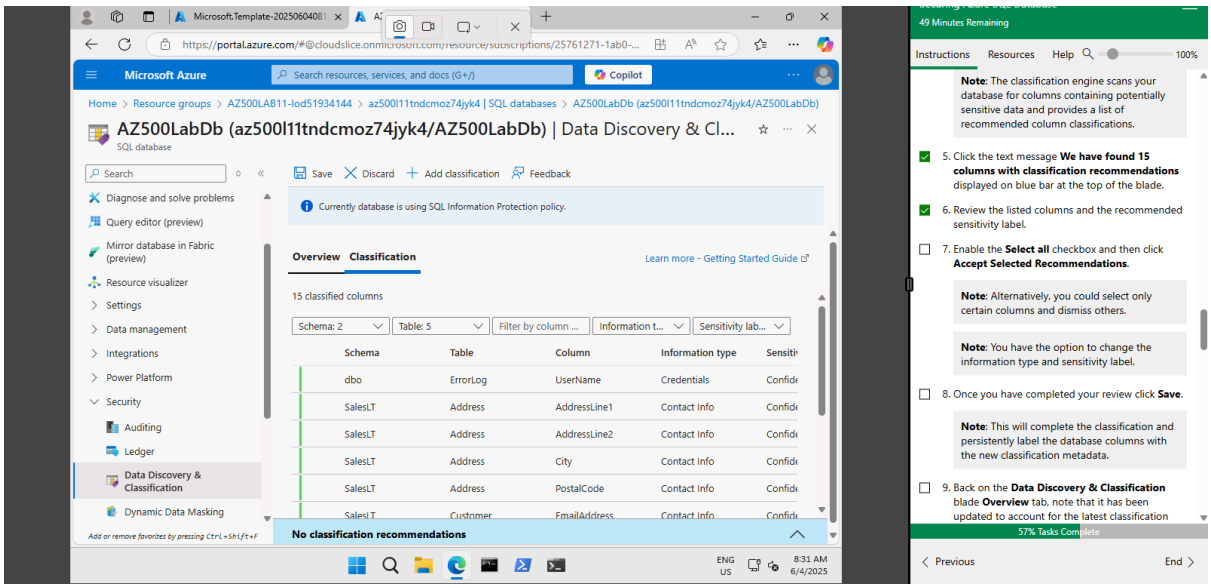
In the second task, I enabled Microsoft Defender for SQL on the SQL server, providing advanced security capabilities such as vulnerability assessments and threat detection. I navigated to the Security section of the SQL server and enabled the feature, which is integrated with Microsoft Defender for Cloud. I reviewed the configuration options for advanced threat protection and vulnerability assessment, which help detect anomalous activities like SQL injection attempts. I also viewed existing security recommendations and alerts, highlighting potential areas for improving database security posture.





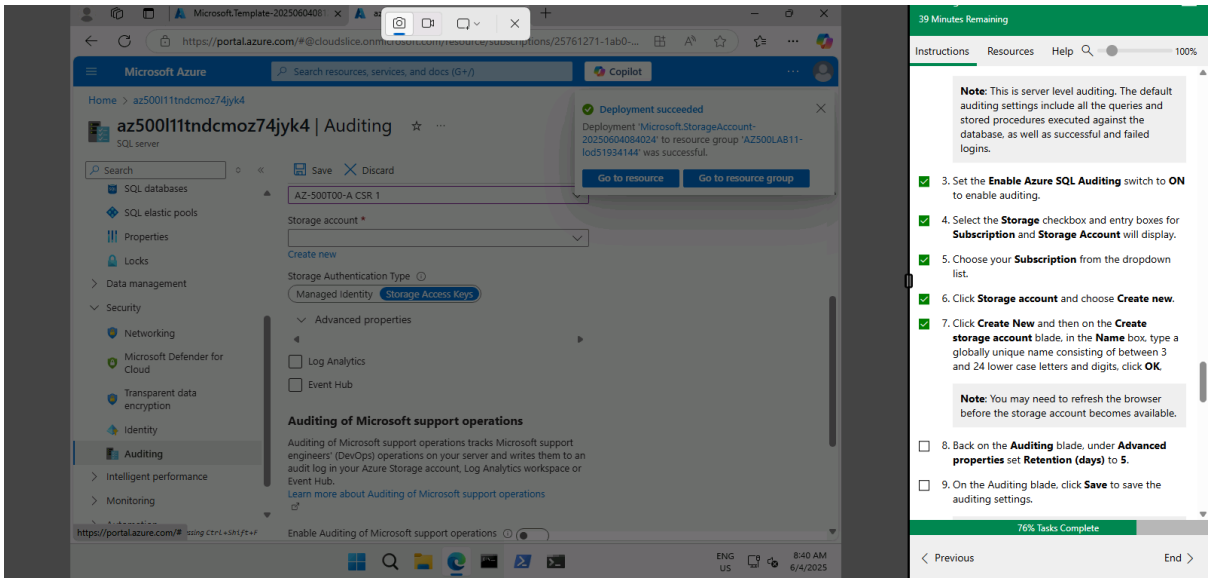
Task 3: Configure Data Classification

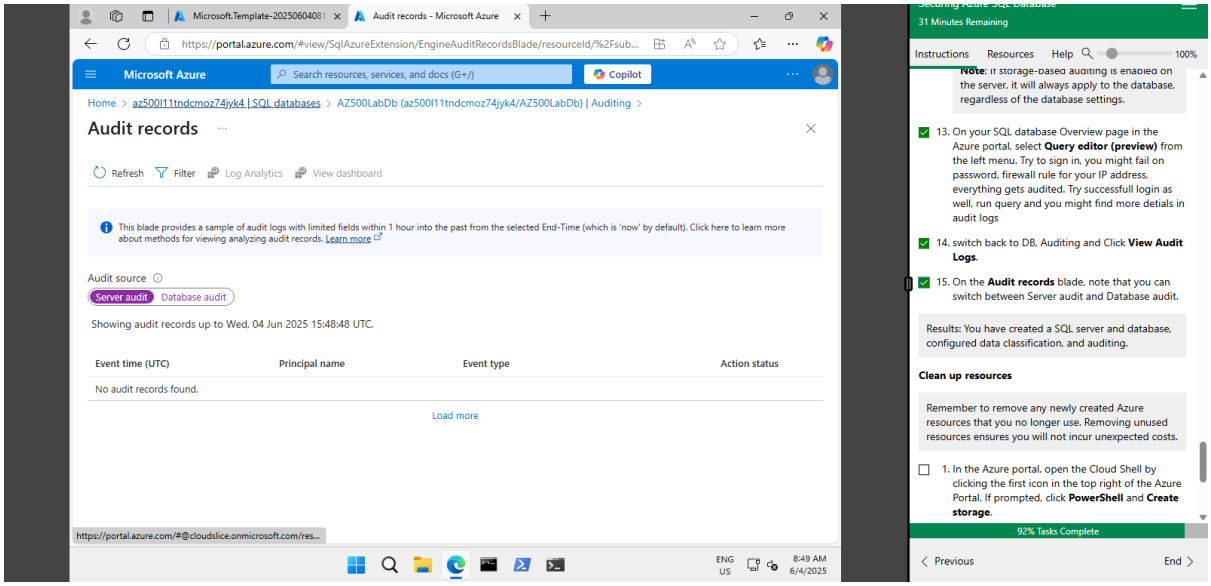
The third task focused on data discovery and classification to support data governance and compliance requirements such as GDPR. I accessed the SQL database's Data Discovery & Classification feature, where the classification engine scanned for columns with sensitive data. It identified 15 columns for classification, which I accepted and saved. This added metadata labels to the columns to indicate their sensitivity. This task helped me understand how Azure can help with data transparency, control, and compliance reporting through persistent column classification.



Task 4: Configure Auditing

In this task, I configured auditing at both the server and database levels to track access and changes to the SQL environment. I enabled Azure SQL Auditing on the server level, created a new storage account for storing logs, and configured log retention settings. I then enabled auditing on the database itself. The auditing setup captures successful and failed logins, query executions, and configuration changes. I also used the Query Editor (preview) to simulate activity and later viewed the Audit Logs to verify that the actions were recorded. This ensured that all database operations could be monitored for security and compliance purposes.





Conclusion

This lab provided valuable practical experience in implementing and managing security features for Azure SQL Database. By deploying a secure SQL infrastructure, enabling threat detection, classifying sensitive data, and configuring auditing, I learned how Azure can support compliance and protect against both internal and external threats. Each task built upon the previous, culminating in a well-secured and monitored SQL environment. These skills are crucial for any cloud administrator or security professional responsible for managing data in Azure. Overall, the lab successfully demonstrated how to apply security best practices to protect sensitive data in a cloud-based database system.