

Cyber Shujaa

Cloud Security Specialist

Assignment 17 - Lab 5: Securing Azure SQL Database

NAME: WELDON KIPKIRUI KENEI

CS NO: ADC-CSS02-25027

Introduction

In this lab scenario, we have been tasked with reviewing the security features for the Azure SQL database. Specifically, we are interested in protecting against attacks such as SQL injection and data exfiltration. The ability to discover and classify database information, such as Confidential, and the ability to audit database server and database queries, and log events.

Implementing SQL Database security features

In this task, we will: Deploy an Azure SQL Database, configure Advanced Data Protection, configure Data Classification, and configure Auditing.

We deploy an Azure SQL database using a template as shown.

The screenshot shows the Azure Portal interface for a custom deployment. The main window displays the 'Custom deployment' blade with the 'Review + create' tab selected. The 'Summary' section shows a 'Customized template' with '3 resources'. The 'Terms' section includes a link to 'Azure Marketplace Terms' and a paragraph of legal terms. A task pane on the right, titled 'Securing Azure SQL Database', provides instructions and a table of settings.

Instructions:

- Note: Review the content of the template and 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-lod51888494
Location	(US) East US

7. Click **Review + Create** and then click **Create**.

30% Tasks Complete

< Previous End >

After the database is set, we then configure advanced data protections in the portal. This will be done by enabling Microsoft Defender for SQL.

The screenshot shows the Microsoft Azure portal interface. The main content area displays the 'Microsoft Defender for SQL' page, which includes a section for 'Recommendations', 'Security alerts', and 'Findings'. The 'Enablement Status' is currently 'Disabled'. A prominent blue 'Enable' button is visible at the bottom of the main content area, highlighted with a red rectangular box. To the right, a task pane titled 'Securing Azure SQL Database' provides a list of instructions. The first instruction (3) states: 'On the AZ500LAB11-lod51888494 blade, click the entry representing the newly created SQL Server.' The second instruction (4) states: 'On the SQL server blade, in the Security section, click Microsoft Defender for Cloud, select Enable Microsoft Defender for SQL.' The third instruction (5) states: 'On the SQL server blade, in the Security section, on the Microsoft Defender for Cloud page, in the Microsoft Defender for SQL: Enabled at the subscription-level (Configure) parameter, click (configure).' The fourth instruction (6) states: 'On the Server Settings blade, review the information about pricing and the trial period, VULNERABILITY ASSESSMENT SETTINGS and ADVANCED THREAT PROTECTION SETTINGS.' The fifth instruction (7) states: 'Back to Microsoft Defender for Cloud blade, review Recommendations and Security alerts.'

Next, we will discover and classify information in the SQL database for GDPR and data protection compliance.

The screenshot shows the Microsoft Azure portal interface, specifically the 'AZ500LabDb' blade. The 'Classification' tab is selected, and the 'Accept selected recommendations' button is highlighted with a red rectangular box. The main content area displays the 'AZ500LabDb (az500l1b5ecnjzqbqivc/AZ500LabDb)' page, which includes a section for '15 columns with classification recommendations'. Below this section, there are buttons for 'Accept selected recommendations', 'Dismiss selected recommendations', and 'Show dismissed recommendations'. The 'Accept selected recommendations' button is highlighted with a red rectangular box. To the right, a task pane titled 'Securing Azure SQL Database' provides a list of instructions. The sixth instruction (6) states: 'On the Server Settings blade, review the information about pricing and the trial period, VULNERABILITY ASSESSMENT SETTINGS and ADVANCED THREAT PROTECTION SETTINGS.' The seventh instruction (7) states: 'Back to Microsoft Defender for Cloud blade, review Recommendations and Security alerts.' The eighth instruction (8) states: 'Once you have completed your review click Save.' The ninth instruction (9) states: 'Back on the Data Discovery & Classification blade Overview tab, note that it has been updated to account for the latest classification information.'

Next, we will first configure server-level auditing and then configure database-level auditing. Shown below is server-level auditing. The default auditing settings include all the queries and stored procedures executed against the database, as well as successful and failed logins.

The screenshot shows the Azure portal interface for configuring server-level auditing. The main pane displays the 'az50011b5ecnjzqbqivc | Auditing' blade. The 'Enable Azure SQL Auditing' toggle is turned on. The 'Audit log destination' is set to 'Storage'. A 'Save' button is highlighted. On the right, a task pane titled 'Securing Azure SQL Database' shows instructions for creating a storage account and setting retention.

Since we already have the server-level auditing, we can configure the database-level auditing.

The screenshot shows the Azure portal interface for configuring database-level auditing. The main pane displays the 'AZ500LabDb (az50011b5ecnjzqbqivc/AZ500LabDb) | Auditing' blade. The 'Save' button is highlighted. A success message 'Successfully saved Auditing settings.' is displayed. Below, it shows 'Server-level Auditing: Enabled'. On the right, a task pane titled 'Securing Azure SQL Database' shows instructions for logging analytics workspace or event hub.

We can view the unified audit logs from the audit page for both server-level and database-level.

Conclusion

To conclude, the lab has equipped us with the ability to configure advanced secure data protection from the Azure portal for Azure SQL, identify and classify sensitive information in our database, and finally, how to audit our database and database servers through stored logs.