

Lab 9: Azure SQL Database Security and Auditing

CST8912_011

ZheZhang

041109657

March 19, 2025

Submitted to: Prof. Tanishq Bansal

Title

Azure SQL Database Security and Auditing

Introduction or Purpose

The purpose of this lab is to explore the security features provided by **Microsoft Azure for SQL Databases**. Specifically, we will implement security measures such as **SQL injection protection, advanced threat protection, data classification, and auditing**. These features are essential to ensure the confidentiality, integrity, and availability of data stored in the cloud.

This lab covers:

- **Deploying an Azure SQL Database**
- **Configuring Advanced Data Protection**
- **Setting up Data Classification**
- **Enabling and Testing Auditing for Database Security**
- **Reviewing and Analyzing Audit Logs**

Steps Covered in the Lab

Task 1: Deploy an Azure SQL Database

1. Logged in to **Azure Portal** (<https://portal.azure.com>).
2. Navigated to **SQL Databases** and clicked **Create**.
3. Entered the following values:
 - **Subscription**: Selected my Azure subscription.
 - **Resource group**: CST8912demo
 - **Database name**: db8912
 - **Server**: Created a new SQL Server with **Canada Central** as location.
 - **Authentication**: Chose SQL authentication and provided a strong password.
4. Configured **Networking**:
 - Chose **Public endpoint**.
 - Allowed **Azure services and client IP** to access the database.

5. Clicked **Review + Create** and deployed the SQL database.

The screenshot shows the Azure portal interface for a SQL database. The left sidebar contains navigation options: Overview, Activity log, Tags, Diagnose and solve problems, Query editor (preview), Mirror database in Fabric (preview), Resource visualizer, Settings, Compute + storage, Connection strings, Properties, Locks, Data management, and Integrations. The main content area shows the 'Overview' page for the database 'db8912 (db8912demo/db8912)'. It includes a search bar, action buttons (Copy, Restore, Export, Set server firewall, Delete, Connect with..., Feedback), and a 'JSON View' link. The 'Essentials' section lists key properties: Resource group (CST8912demo), Status (Online), Location (Canada Central), Subscription (Azure for Students), and Subscription ID (913a8401-361d-4f42-8d7d-e2ff44f75da2). It also shows Server name (db8912demo.database.windows.net), Connection strings (Show database connection strings), Pricing tier (Free - General Purpose - Serverless: Gen5, 2 vCores), Overage billing (Disabled), Free monthly vCore (100,000 vCore seconds remaining), and Earliest restore point (No restore point available). Below this is a 'Getting started' section with tabs for Monitoring, Properties, Features, Notifications (0), Integrations, and Tutorials. The 'Getting started' tab is active, displaying the text 'Start working with your database' and a link to 'Learn more'.

Task 2: Configure Advanced Data Protection

1. Navigated to **SQL Server > Security > Microsoft Defender for Cloud**.
2. Enabled **Microsoft Defender for SQL**.
3. Configured **Vulnerability Assessment Settings** and reviewed **Threat Protection Settings**.
4. Checked for any **security recommendations or alerts**.

The screenshot shows the Microsoft Defender for Cloud interface. It displays four main sections: Recommendations (0), Security alerts (0), Findings (2), and Enablement Status (Enabled at the subscription-level). There are links to 'Learn more' about Microsoft Defender for Cloud and Microsoft Defender for SQL.

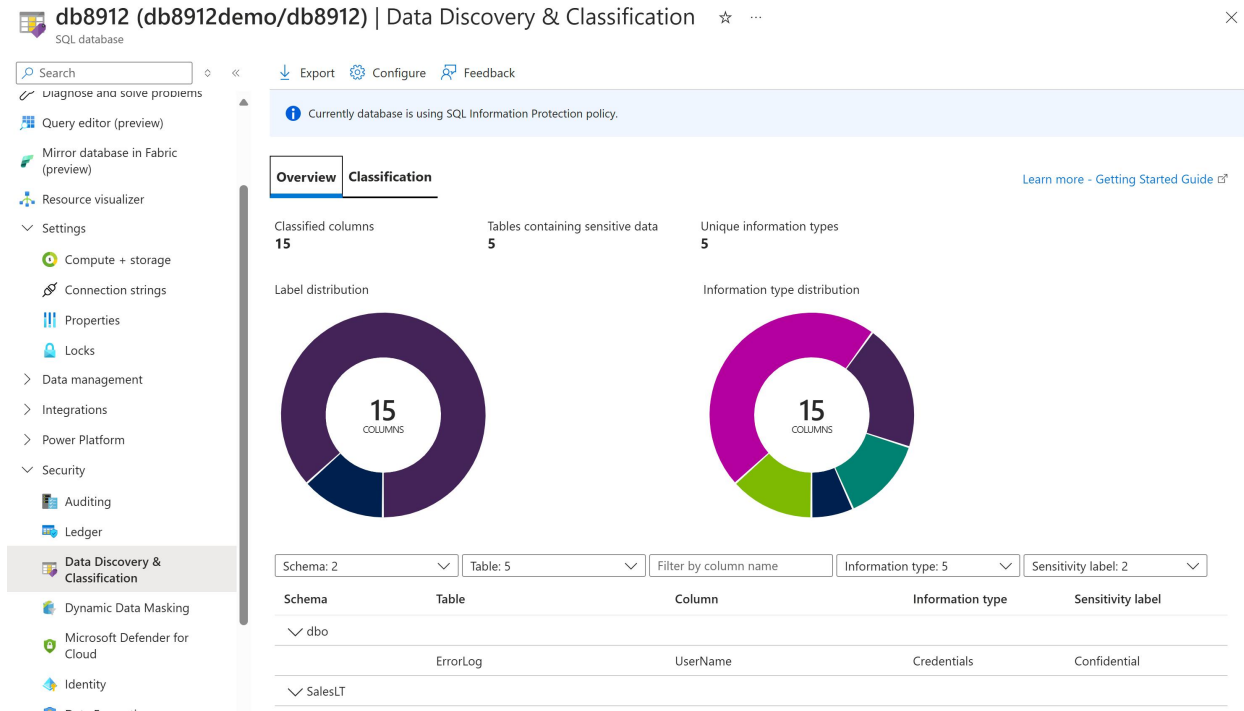
Recommendations

Defender for Cloud continuously monitors the configuration of your SQL Servers to identify potential security vulnerabilities and recommends actions to mitigate them.


No recommendations to display


Task 3: Configure Data Classification

1. Navigated to **SQL Database > Security > Data Discovery & Classification**.
2. Clicked the **Classification** tab and reviewed the recommended **sensitivity labels**.
3. Accepted all suggested classifications and saved the changes.
4. Verified that the **classification summary** was updated.



Task 4: Configure and Test Database Auditing



1. Navigated to **SQL Database > Security > Auditing**.
2. Enabled **Database Auditing** and selected **Storage Account** for storing audit logs.
3. Set the **Retention Period** to 5 days.
4. Clicked **Save** to apply settings.

 [Feedback](#)

Azure SQL Auditing

Azure SQL Auditing tracks database events and writes them to an audit log in your Azure Storage account, Log Analytics workspace or Event Hub.


[Learn more about Azure SQL Auditing](#)

Enable Azure SQL Auditing  


Audit log destination (choose at least one):

☒ Storage


Subscription ^{*}


Azure for Students 

Storage account ^{*}


cst8912demo 


[Create new](#)


Storage Authentication Type 


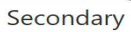
Managed Identity 

Advanced properties

Retention (Days) 

 5

Storage access key 

Testing Auditing with SQL Queries

1. Opened **Query Editor (preview)** in Azure Portal.
2. **Attempted a failed login** with an incorrect password to test authentication logs.
3. **Successfully logged in** and executed the following SQL commands:

```
CREATE TABLE AuditTest (  
    ID INT PRIMARY KEY IDENTITY,  
    Name NVARCHAR(100),  
    Age INT );  
  
INSERT INTO AuditTest (Name, Age) VALUES ('Alice', 25);  
  
SELECT * FROM AuditTest;
```

4. Verified that all **login attempts** and **SQL queries** were recorded in the audit logs.

>>

Query 1 ×

▶ Run ☐ Cancel query ⬇ Save query ⬇ Export data as ▾ 🟩 Show only Editor

```
1 SELECT TOP 5 * FROM SalesLT.Customer;  
2
```

Results Messages

🔍 Search to filter items...

CustomerID	NameStyle	Title	FirstName	MiddleName
1	False	Mr.	Orlando	N.
2	False	Mr.	Keith	
3	False	Ms.	Donna	F.
4	False	Ms.	Janet	M.
5	False	Mr.	Lucy	

1. Returned to **Auditing > View Audit Logs** to analyze recorded activities.
2. Switched between **Server audit** and **Database audit** to compare logs.
3. Confirmed that authentication failures, SELECT queries, and data modifications were recorded.

Audit records ...

🔄 Refresh 🔍 Filter 📊 Log Analytics 📄 View dashboard

i This blade provides a sample of audit logs with limited fields within 2 hours into the past from the selected End-Time (which is 'now' by default). Click here to learn more about methods for viewing analyzing audit records. [Learn more](#)

Audit source ⓘ

Server audit Database audit

Showing audit records up to Wed, 19 Mar 2025 21:45:21 UTC.

[Run in Query Editor](#) ⓘ

Event time (UTC)	Principal name	Event type	Action status
3/19/2025 9:44:48 PM	db8912yourname	DATABASE AUTHENTICATION FAILED	Failed
3/19/2025 9:43:17 PM	db8912yourname	BATCH COMPLETED	Succeeded

Audit source ⓘ

Server audit

Database audit

Showing audit records up to Wed, 19 Mar 2025 21:50:29 UTC.

[Run in Query Editor](#) ⓘ

Event time (UTC)	Principal name	Event type	Action status
3/19/2025 9:50:07 PM	db8912yourname	BATCH COMPLETED	Succeeded
3/19/2025 9:50:07 PM	db8912yourname	DATABASE AUTHENTICATIO...	Succeeded
3/19/2025 9:50:00 PM	db8912yourname	BATCH COMPLETED	Succeeded
3/19/2025 9:50:00 PM	db8912yourname	DATABASE AUTHENTICATIO...	Succeeded
3/19/2025 9:49:52 PM	db8912yourname	BATCH COMPLETED	Succeeded
3/19/2025 9:49:52 PM	db8912yourname	DATABASE AUTHENTICATIO...	Succeeded
3/19/2025 9:49:40 PM	db8912yourname	BATCH COMPLETED	Succeeded
3/19/2025 9:49:40 PM	db8912yourname	DATABASE AUTHENTICATIO...	Succeeded
3/19/2025 9:49:14 PM	db8912yourname	BATCH COMPLETED	Succeeded
3/19/2025 9:49:14 PM	db8912yourname	DATABASE AUTHENTICATIO...	Succeeded

Task 5: Cleanup Resources

1. Deleted the **SQL Database** from the resource group.
2. Deleted the **SQL Server** to avoid additional costs.
3. Verified that all related resources were removed.

Results

The lab successfully demonstrated how to:

- ✓ Deploy an **Azure SQL Database** with security best practices.
- ✓ Enable **Microsoft Defender for SQL** to protect against attacks.
- ✓ Classify **sensitive data** for compliance.
- ✓ Configure and analyze **Database Auditing** logs.
- ✓ Review **authentication failures** and **data access logs**.

These security configurations ensure data integrity, confidentiality, and compliance with industry standards.

References

- Microsoft Learn: <https://learn.microsoft.com/en-us/azure/sql-database/>
- Azure Defender Documentation: <https://learn.microsoft.com/en-us/azure/security-center/security-center-defender-for-sql-introduction>