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:

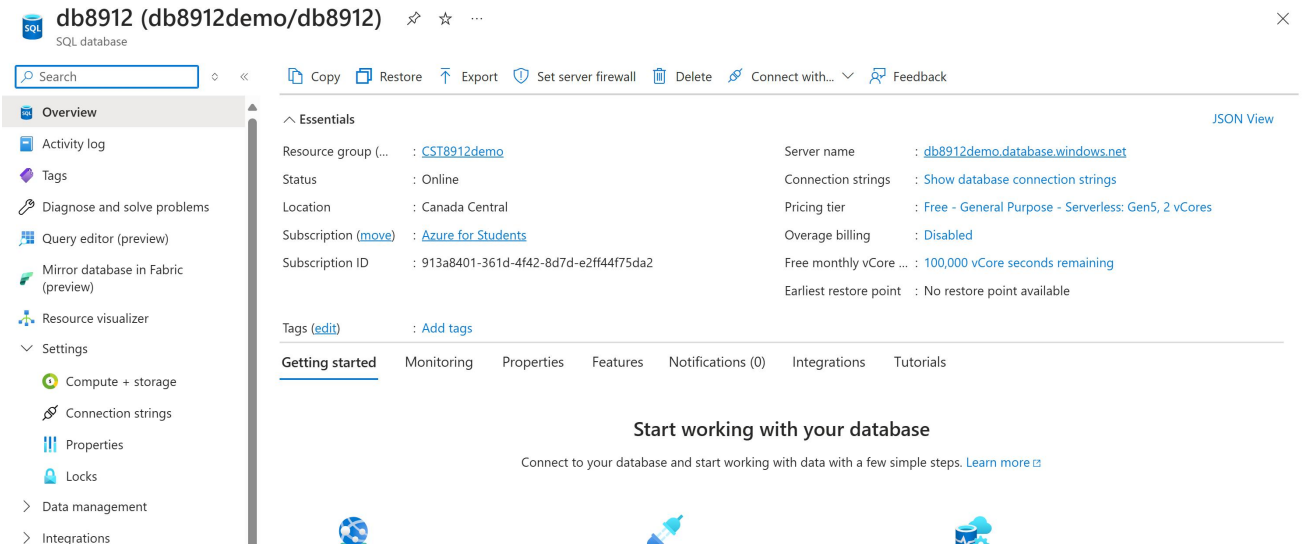
- **Deploying an Azure SQL Database**
- **Configuring Advanced Data Protection**
- **Setting up Data Classification**
- **Enabling and Testing Auditing for Database Security**
- **Reviewing and Analyzing Audit Logs**

Steps Covered in the Lab

Task 1: Deploy an Azure SQL Database

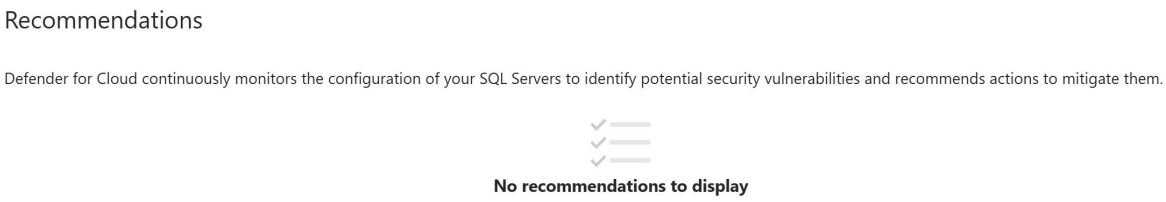
1. Logged in to **Azure Portal** (https://portal.azure.com).
2. Navigated to **SQL Databases** and clicked **Create**.
3. Entered the following values:
    - **Subscription**: Selected my Azure subscription.
    - **Resource group**: CST8912demo
    - **Database name**: db8912
    - **Server**: Created 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.



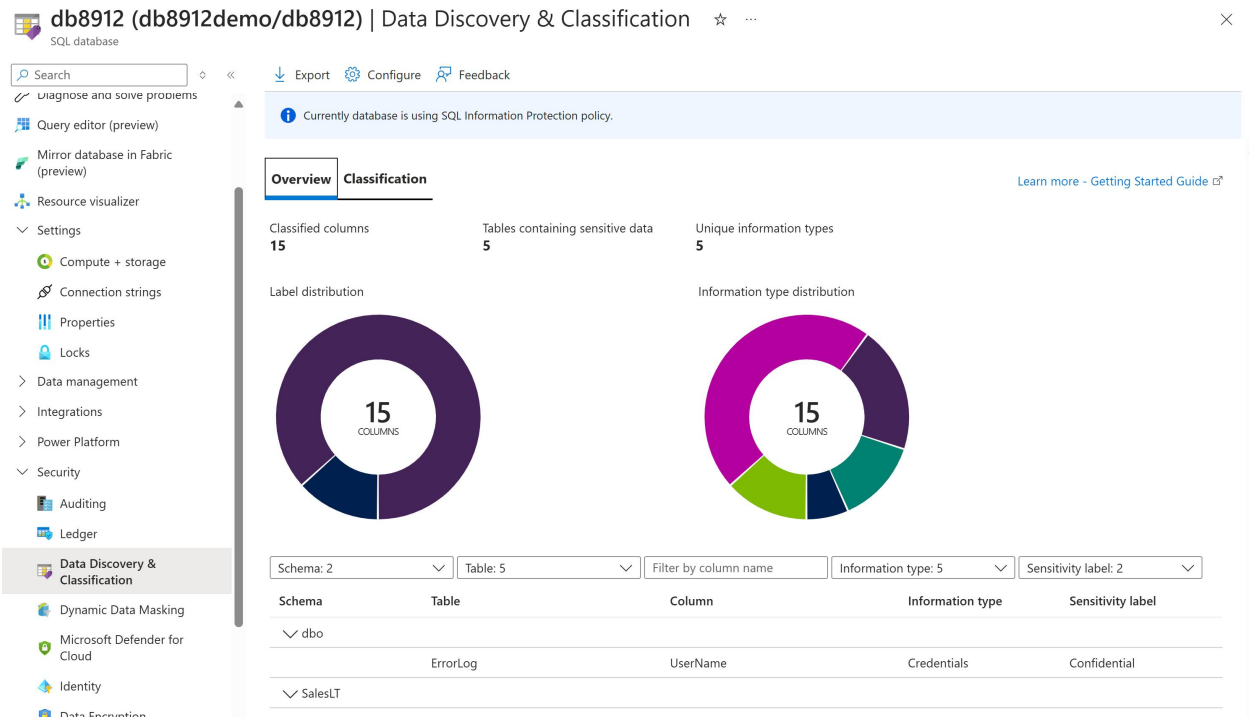
Task 2: Configure Advanced Data Protection

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**.



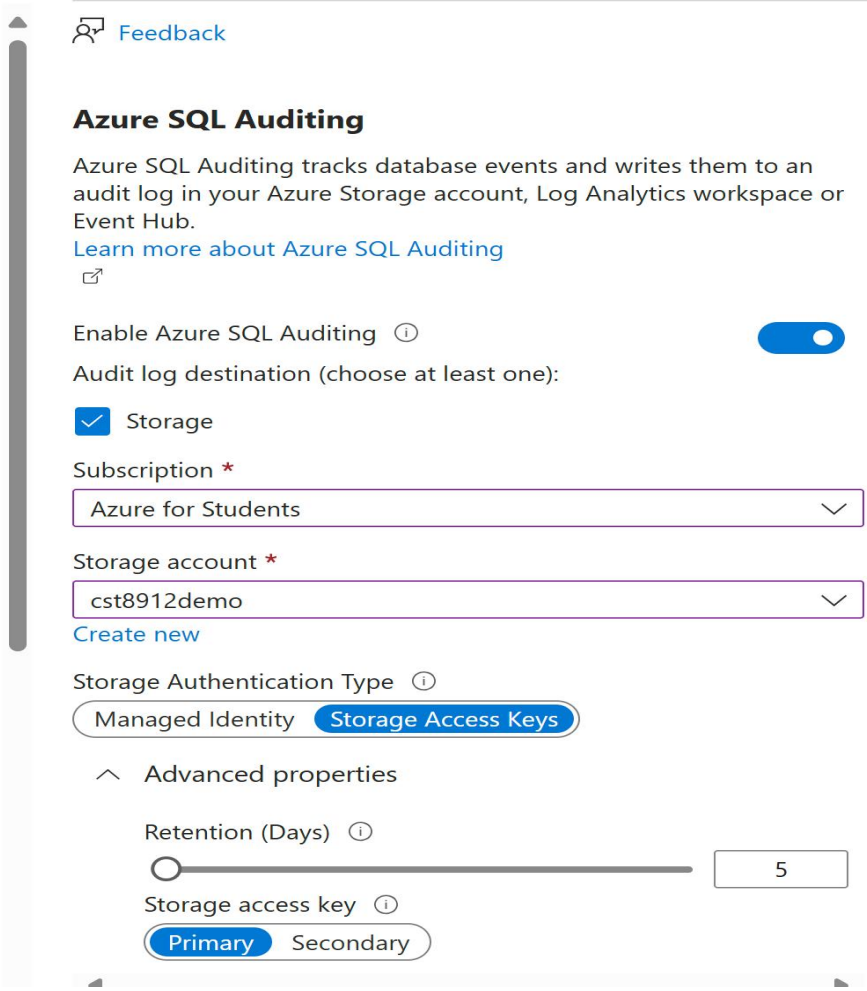
Task 3: Configure Data Classification

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.

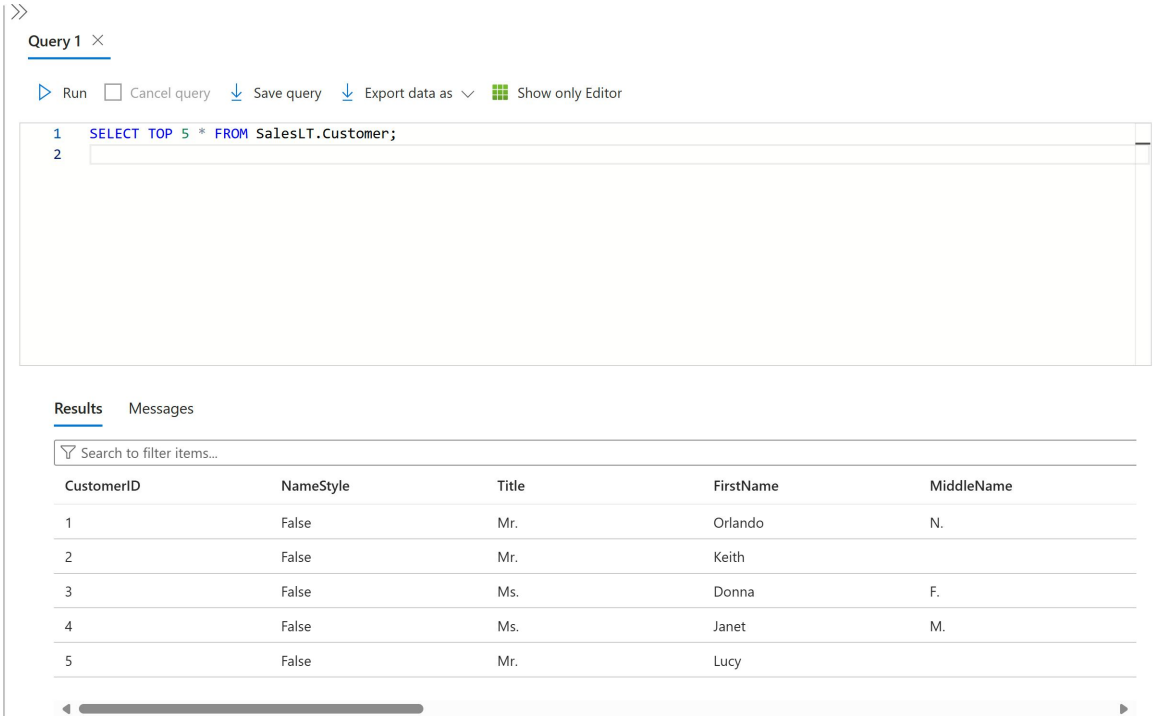


Testing Auditing with SQL Queries

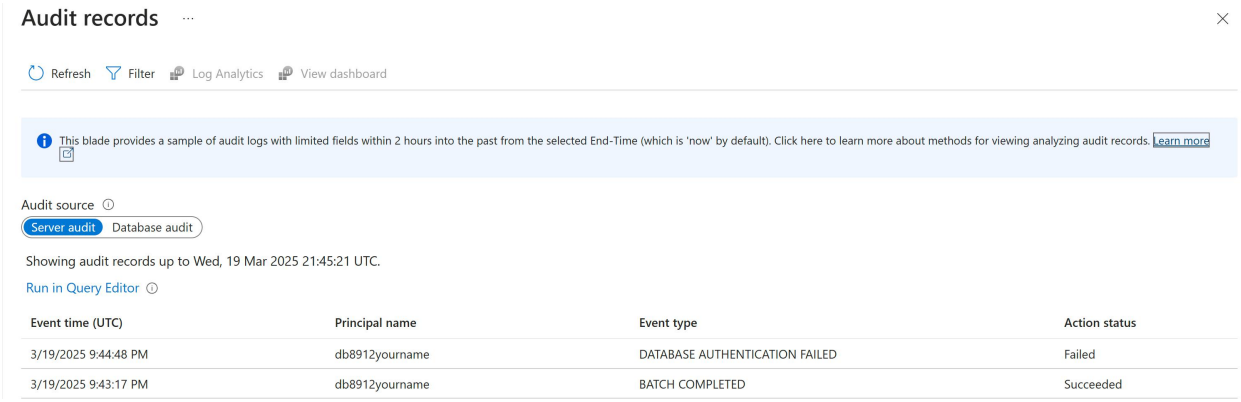
1. Opened **Query Editor (preview)** in Azure Portal.
2. **Attempted a failed login** with an incorrect password to test authentication logs.
3. **Successfully logged in** and executed the following SQL commands:

```
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.



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 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