Lab 9 CST8912_011

Tarang Savaj

Sava0207

March 24, 2025

Submitted to:

Prof. Tanishq Bansal

Lab-9

Title

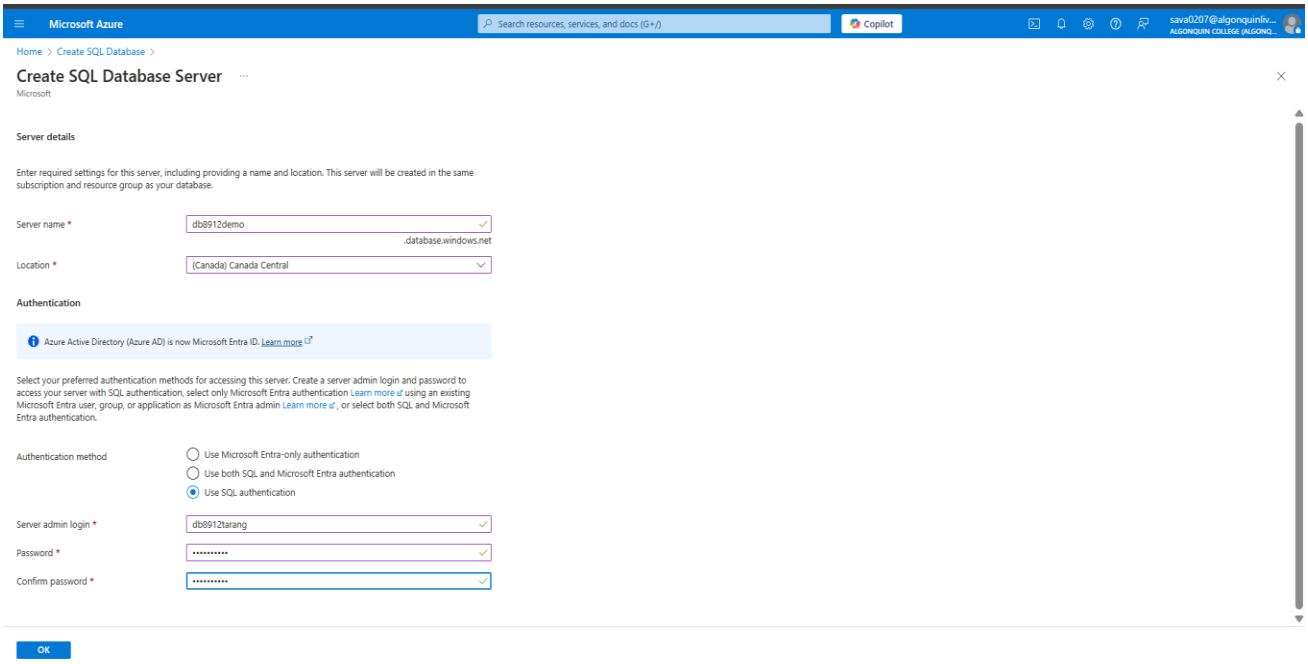
- Securing Azure SQL Database: Implementation of Encryption, Threat Protection, and Auditing

Introduction

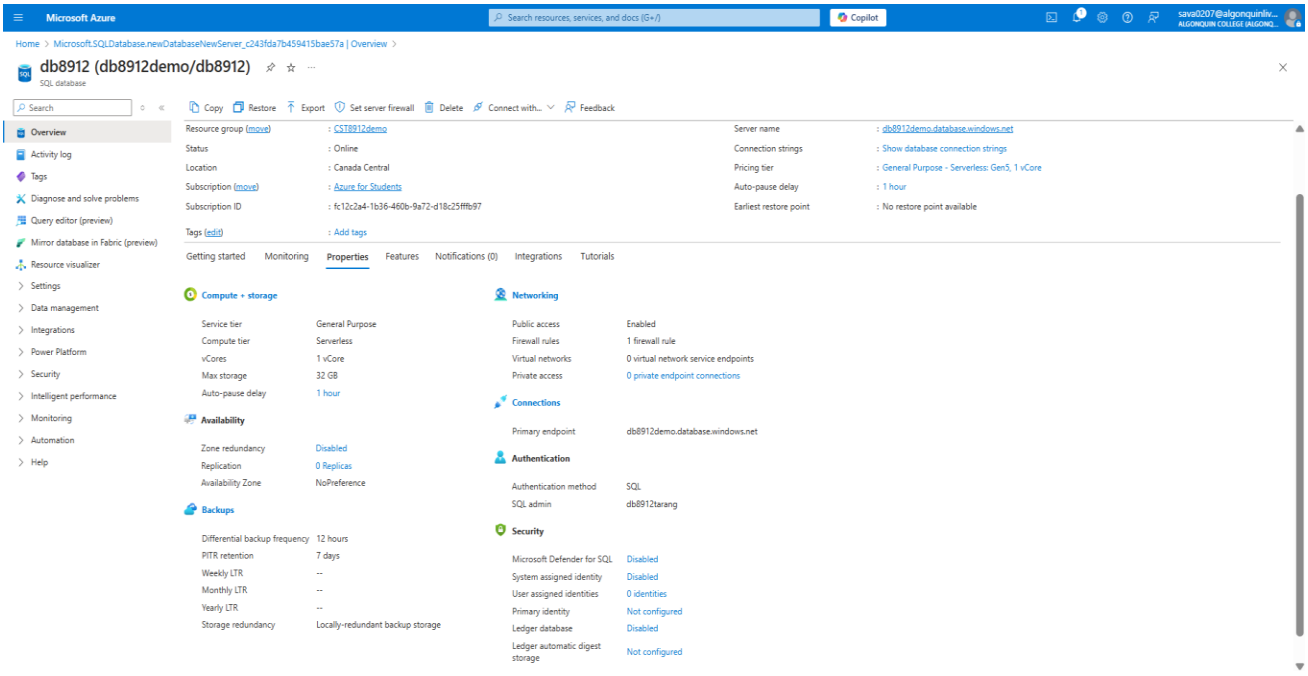
- This lab adopts an approach to put security features in place for Azure SQL Database to protect against cyber threats and manage compliance risks. The security features provided support encryption for data at rest and advanced protection systems and data classification capabilities and audit features for monitoring database operations. Users completing this lab can learn through practical experience the configuration of security controls which enhances cloud-based database resilience and conformity with best practices for cloud security.

Steps

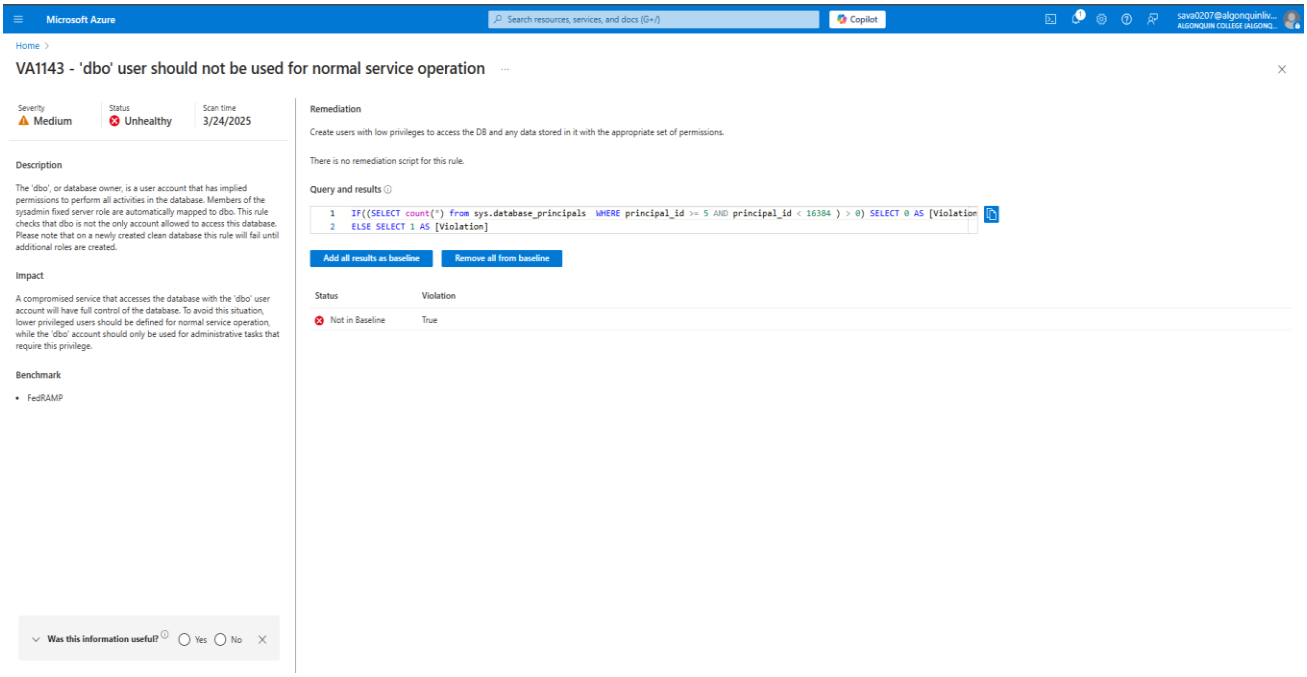
- The initial part of this lab requires setting authentication methods and networking parameters and backup protection levels before deploying an Azure SQL Database. Advanced Data Protection functionality from Microsoft Defender for SQL will become enabled during your second step to protect your system from possible threats. Afterwards you will enable Data Classification to create categories for sensitive data using your organization's regulatory mandates. You will enable Auditing as a security measure at both server and database levels to record all database activities and security events. The cleanup process will remove all created resources to achieve efficiency in cloud costs while ensuring effective management of the cloud environment.



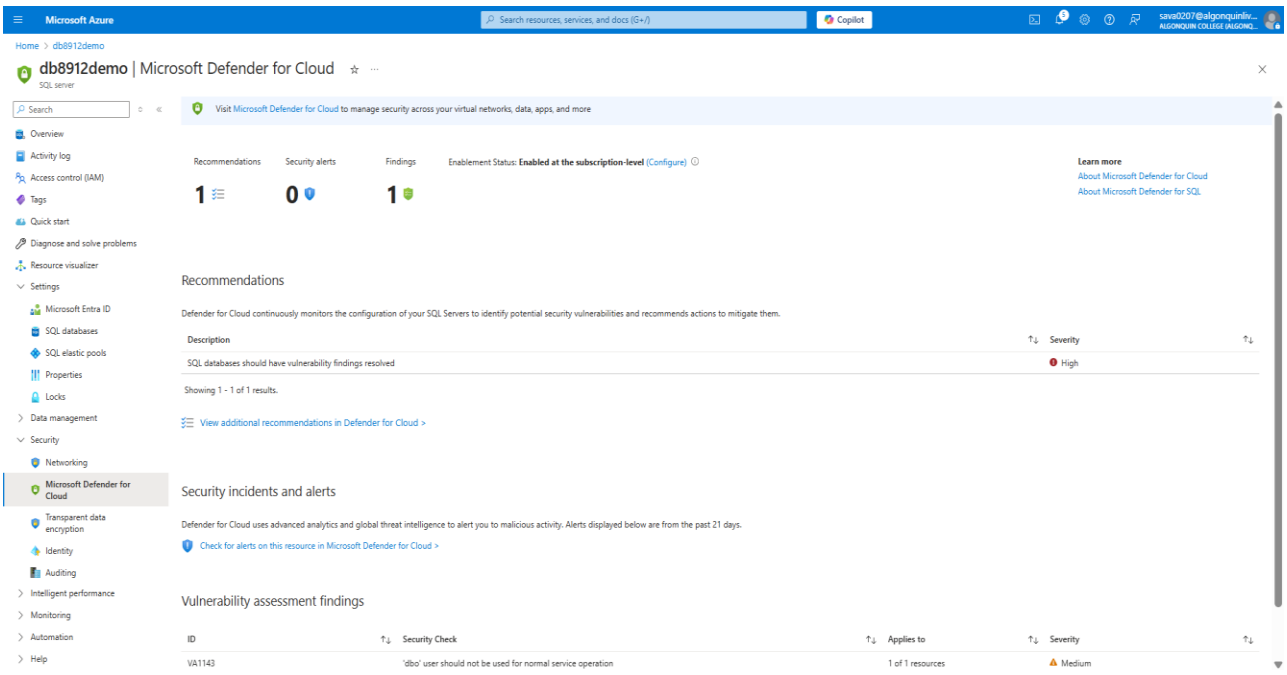
1.1 Creating SQL database server



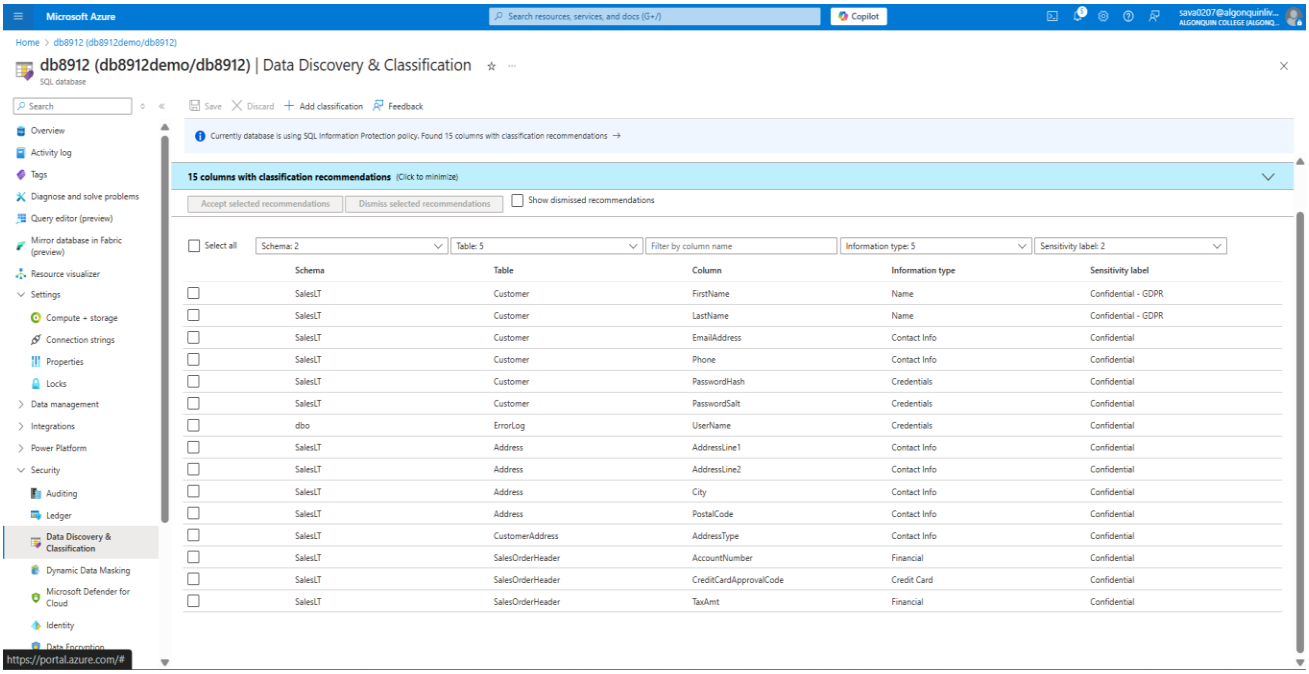
1.2 Overview of SQL database



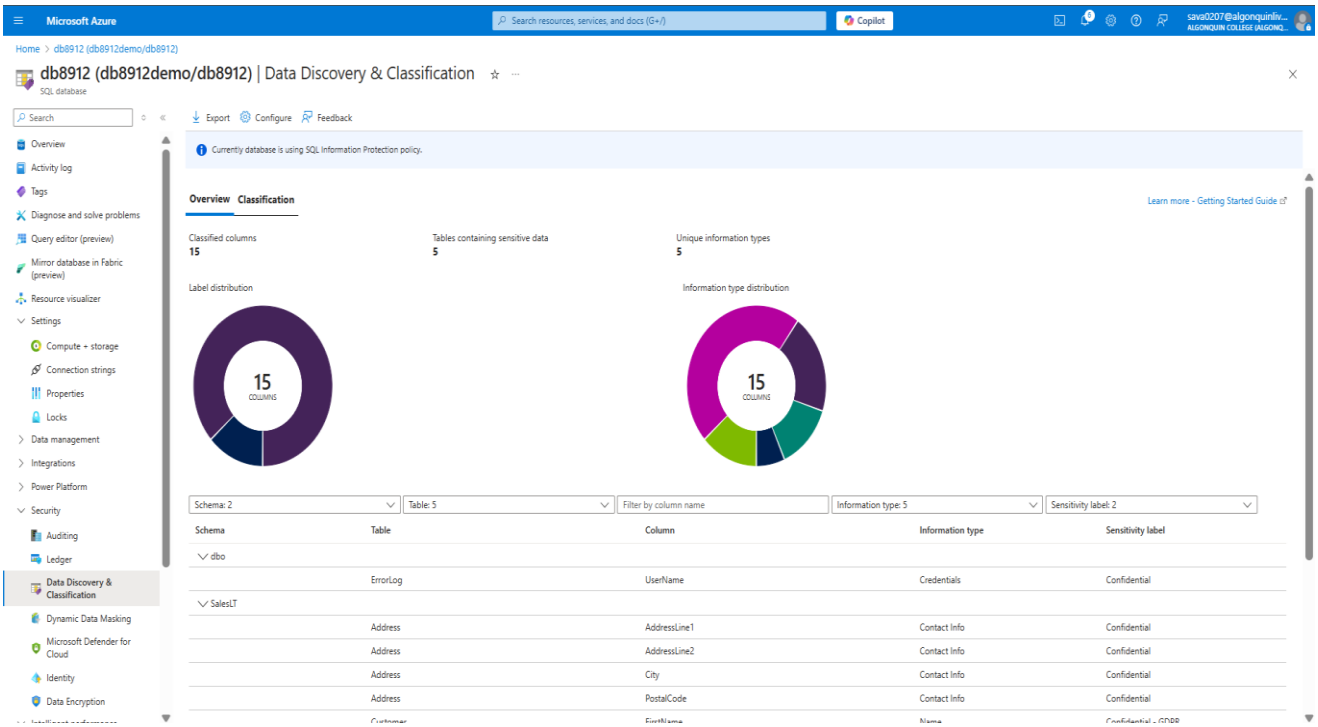
2.1 Vulnerability Assessment



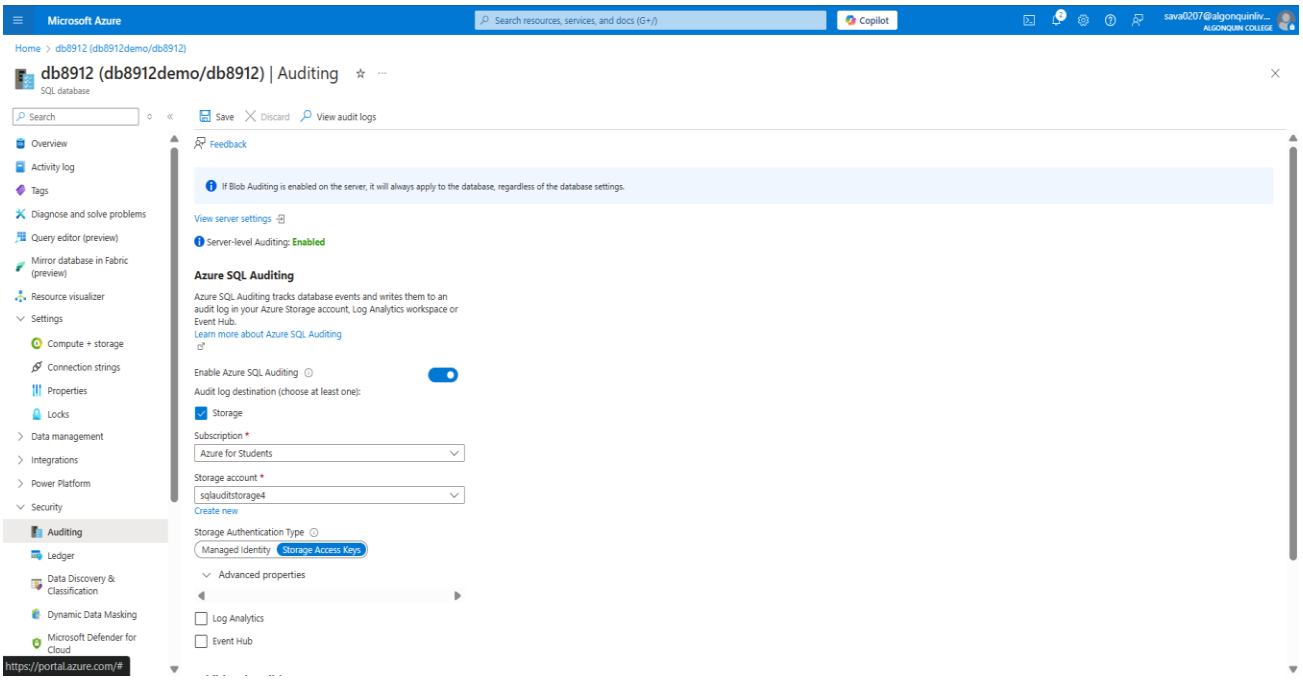
2.2 Overview of Microsoft defender for cloud showing recommendation, security alerts and finding



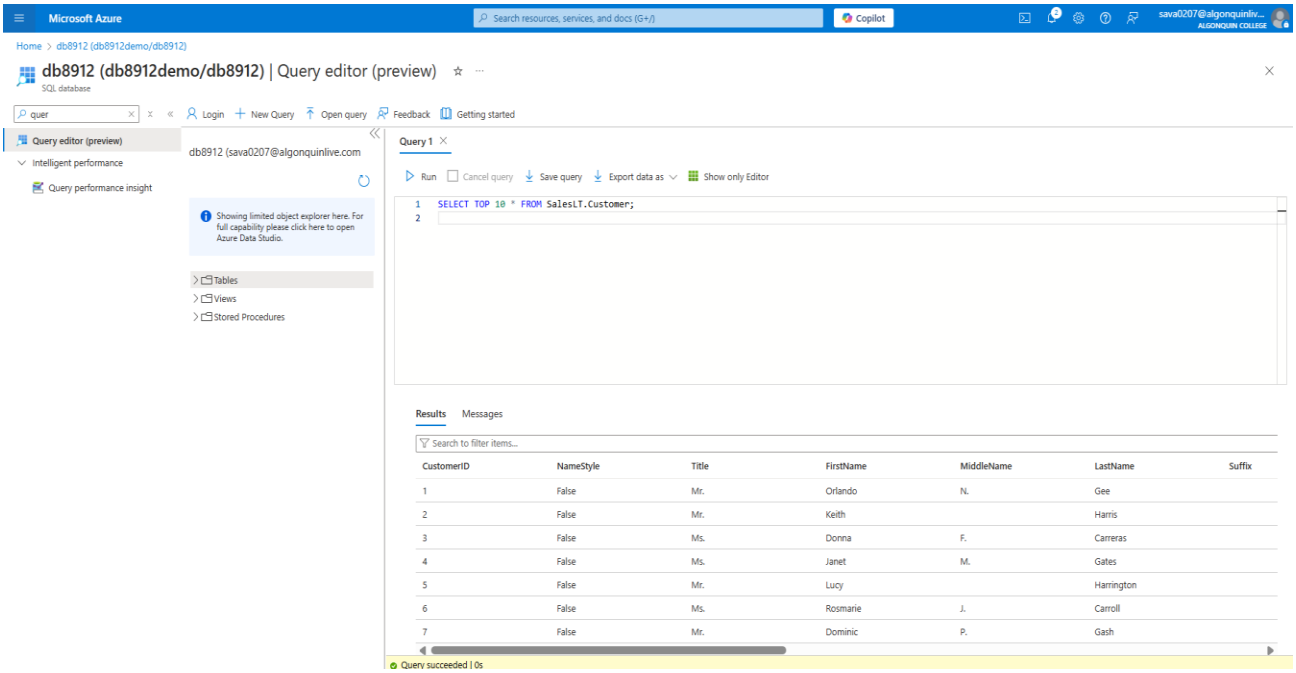
3.1 Showing Data Discovery & Classification with 15 columns



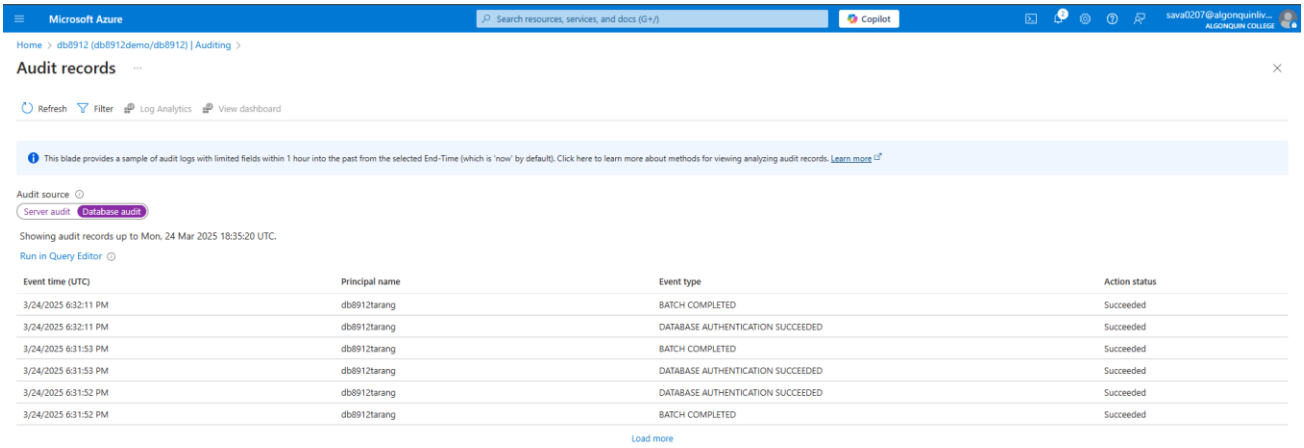
3.2 Overview of Classification



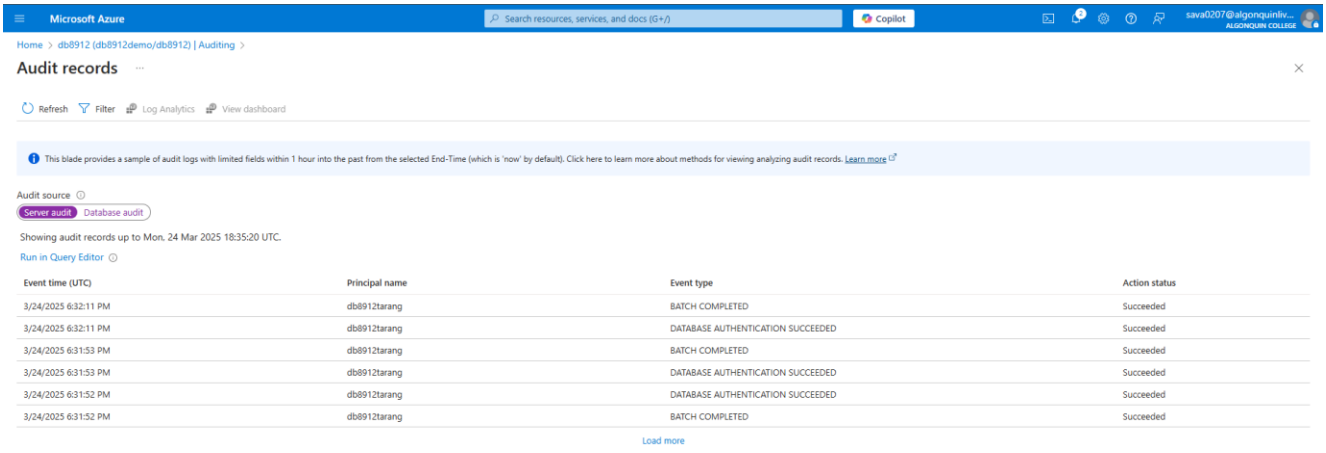
4.1 showing server level auditing is on



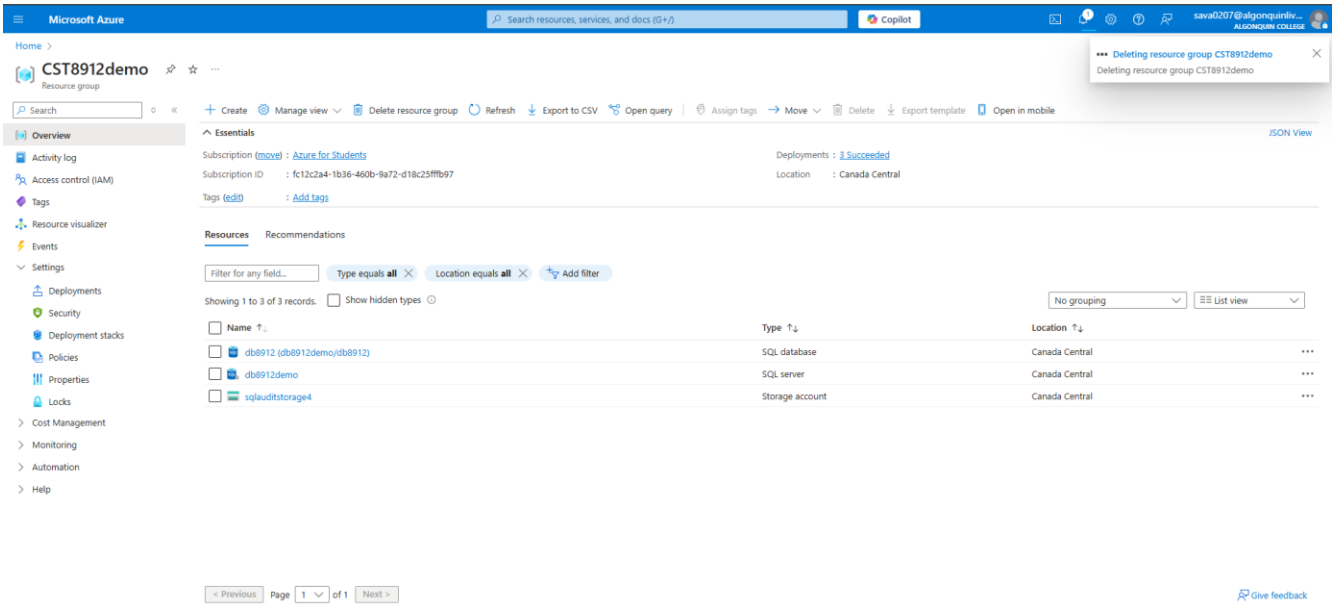
4.2 Run the query in query editor



4.3 Showing audit records of Database audit



4.4 showing audit records of server audit



4.5 deleting the resource group with all the resources created in the lab

References

- References for this task are taken from the provided lab file.