

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.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

save0207@algonquiniv...

ALGONQUIN COLLEGE (ALSONQ...

Home > Create SQL Database >

Create SQL Database Server

Microsoft

Server details

Enter required settings for this server, including providing a name and location. This server will be created in the same subscription and resource group as your database.

Server name *

db8912demo

.database.windows.net

Location *

(Canada) Canada Central

Authentication

Azure Active Directory (Azure AD) is now Microsoft Entra ID. [Learn more](#)

Select your preferred authentication methods for accessing this server. Create a server admin login and password to access your server with SQL authentication, select only Microsoft Entra authentication [Learn more](#) or using an existing Microsoft Entra user, group, or application as Microsoft Entra admin [Learn more](#), or select both SQL and Microsoft Entra authentication.

Authentication method

Use Microsoft Entra-only authentication

Use both SQL and Microsoft Entra authentication

Use SQL authentication

Server admin login *

db8912tarang

Password *

Confirm password *

OK

1.1 Creating SQL database server

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

save0207@algonquiniv...

ALGONQUIN COLLEGE (ALSONQ...

Home > Microsoft SQL Database > New Database > New Server > c243fda7b459415bae57a | Overview >

db8912 (db8912demo/db8912)

SQL database

Search

Copy Restore Export Set server firewall Delete Connect with... Feedback

Overview

Activity log

Tags

Diagnose and solve problems

Query editor (preview)

Mirror database in Fabric (preview)

Resource visualizer

Settings

Data management

Integrations

Power Platform

Security

Intelligent performance

Monitoring

Automation

Help

Resource group (mouse)

CS18912demo

Status

Online

Location

Canada Central

Subscription (mouse)

Azure for Students

Subscription ID

fc12c2a4-1b36-460b-9a72-d18c25fbb97

Tags (edit)

Add tags

Server name

db8912demo.database.windows.net

Connection strings

Show database connection strings

Pricing tier

General Purpose - Serverless Gen5, 1 vCore

Auto-pause delay

1 hour

Earliest restore point

No restore point available

Getting started

Monitoring

Properties

Features

Notifications (0)

Integrations

Tutorials

Compute + storage

Service tier

General Purpose

Compute tier

Serverless

vCores

1 vCore

Max storage

32 GB

Auto-pause delay

1 hour

Networking

Public access

Enabled

Firewall rules

1 firewall rule

Virtual networks

0 virtual network service endpoints

Private access

0 private endpoint connections

Connections

Primary endpoint

db8912demo.database.windows.net

Authentication

Authentication method

SQL

SQL admin

db8912tarang

Security

Microsoft Defender for SQL

Disabled

System assigned identity

Disabled

User assigned identities

0 identities

Primary identity

Not configured

Ledger database

Disabled

Ledger automatic digest storage

Not configured

Availability

Zone redundancy

Disabled

Replication

0 Replicas

Availability Zone

NoPreference

Backups

Differential backup frequency

12 hours

PITR retention

7 days

Weekly LTR

...

Monthly LTR

...

Yearly LTR

...

Storage redundancy

Locally-redundant backup storage

1.2 Overview of SQL database

Microsoft Azure

Search resources, services, and docs (S+)

Copilot

Home

VA1143 - 'dbo' user should not be used for normal service operation

Severity: ▲ Medium

Status: ✖ Unhealthy

Scan time: 3/24/2025

Description

The 'dbo', or database owner, is a user account that has implied permissions to perform all activities in the database. Members of the sysadmin fixed server role are automatically mapped to dbo. This rule checks that dbo is not the only account allowed to access this database. Please note that on a newly created clean database this rule will fail until additional roles are created.

Impact

A compromised service that accesses the database with the 'dbo' user account will have full control of the database. To avoid this situation, lower privileged users should be defined for normal service operation, while the 'dbo' account should only be used for administrative tasks that require this privilege.

Benchmark

- FedRAMP

Remediation

Create users with low privileges to access the DB and any data stored in it with the appropriate set of permissions.

There is no remediation script for this rule.

Query and results

```
1 IF((SELECT count(*) from sys.database_principals WHERE principal_id >= 5 AND principal_id < 16384 ) > 0) SELECT @ AS [Violation]
2 ELSE SELECT 1 AS [Violation]
```

[Add all results as baseline](#) [Remove all from baseline](#)

Status	Violation
✖ Not in Baseline	True

Was this information useful? ☐ Yes ☐ No

2.1 Vulnerability Assessment

Microsoft Azure

Search resources, services, and docs (S+)

Copilot

Home > db8912demo

db8912demo | Microsoft Defender for Cloud

SQL server

Visit Microsoft Defender for Cloud to manage security across your virtual networks, data, apps, and more

Overview

Activity log

Access control (IAM)

Tags

Quick start

Diagnose and solve problems

Resource visualizer

Settings

- Microsoft Entra ID
- SQL databases
- SQL elastic pools
- Properties
- Locks

Data management

Security

- Networking
- Microsoft Defender for Cloud
- Transparent data encryption
- Identity
- Auditing

Intelligent performance

Monitoring

Automation

Help

Recommendations

Security alerts

Findings

Enablement Status: **Enabled at the subscription-level** (Configure)

Learn more

About Microsoft Defender for Cloud

About Microsoft Defender for SQL

1 Recommendations

0 Security alerts

1 Findings

Recommendations

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

Description	Severity
SQL databases should have vulnerability findings resolved	High

Showing 1 - 1 of 1 results.

[View additional recommendations in Defender for Cloud >](#)

Security incidents and alerts

Defender for Cloud uses advanced analytics and global threat intelligence to alert you to malicious activity. Alerts displayed below are from the past 21 days.

[Check for alerts on this resource in Microsoft Defender for Cloud >](#)

Vulnerability assessment findings

ID	Security Check	Applies to	Severity
VA1143	'dbo' user should not be used for normal service operation	1 of 1 resources	Medium

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

Microsoft Azure

Home > db8912 (db8912demo/db8912) | Data Discovery & Classification

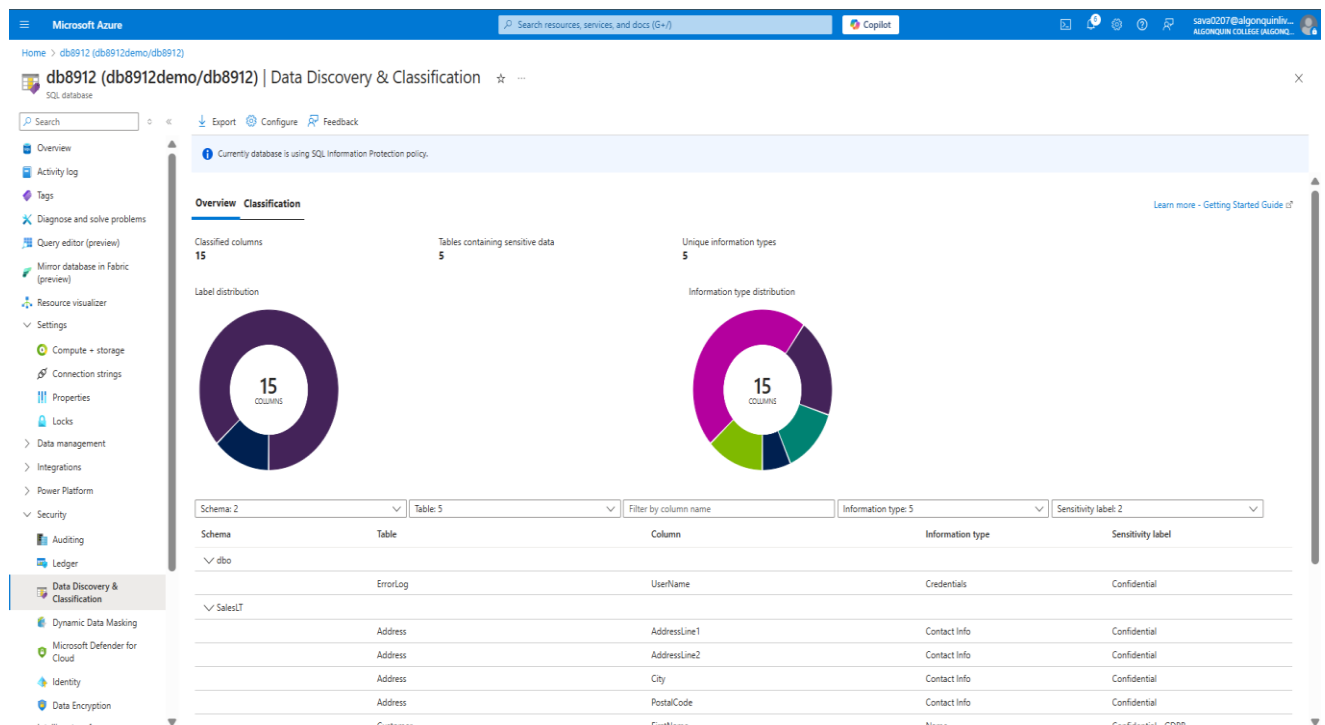
15 columns with classification recommendations (Click to minimize)

Accept selected recommendations Dismiss selected recommendations Show dismissed recommendations

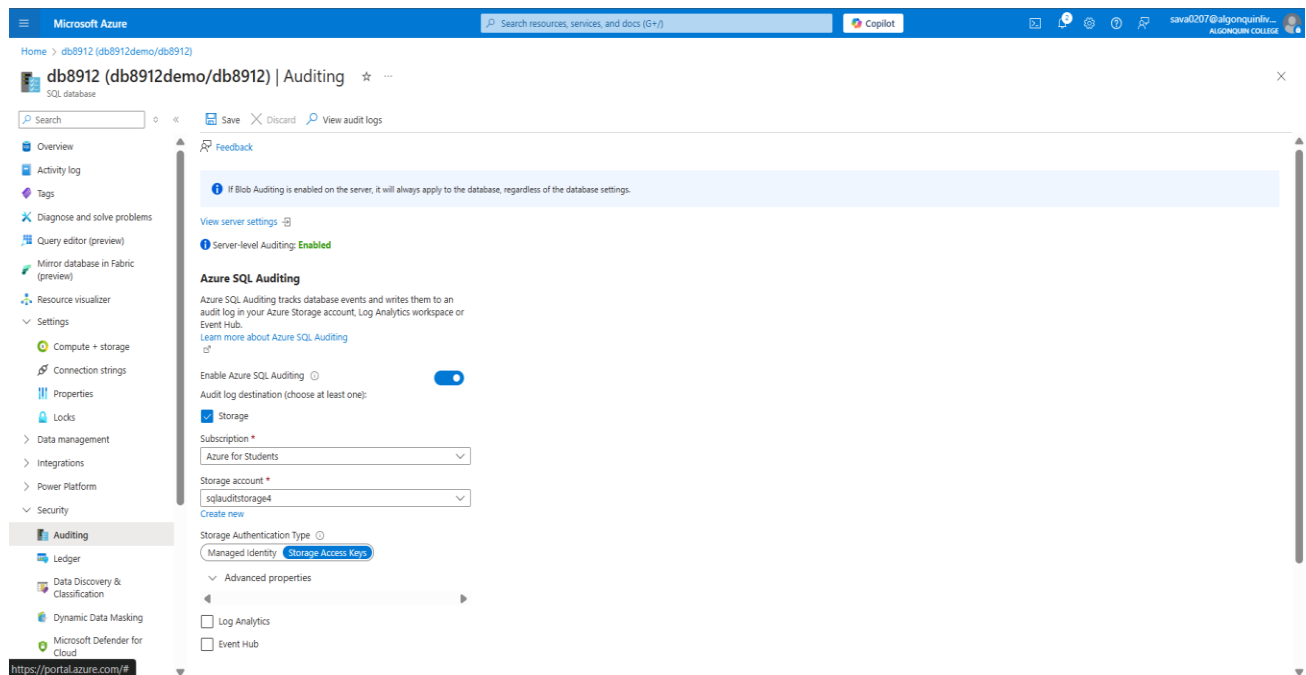
Select all	Schema: 2	Table: 5	Filter by column name	Information type: 5	Sensitivity label: 2
	Schema	Table	Column	Information type	Sensitivity label
<input type="checkbox"/>	SalesLT	Customer	FirstName	Name	Confidential - GDPR
<input type="checkbox"/>	SalesLT	Customer	LastName	Name	Confidential - GDPR
<input type="checkbox"/>	SalesLT	Customer	EmailAddress	Contact Info	Confidential
<input type="checkbox"/>	SalesLT	Customer	Phone	Contact Info	Confidential
<input type="checkbox"/>	SalesLT	Customer	PasswordHash	Credentials	Confidential
<input type="checkbox"/>	SalesLT	Customer	PasswordSalt	Credentials	Confidential
<input type="checkbox"/>	dbo	ErrorLog	UserName	Credentials	Confidential
<input type="checkbox"/>	SalesLT	Address	AddressLine1	Contact Info	Confidential
<input type="checkbox"/>	SalesLT	Address	AddressLine2	Contact Info	Confidential
<input type="checkbox"/>	SalesLT	Address	City	Contact Info	Confidential
<input type="checkbox"/>	SalesLT	Address	PostalCode	Contact Info	Confidential
<input type="checkbox"/>	SalesLT	CustomerAddress	AddressType	Contact Info	Confidential
<input type="checkbox"/>	SalesLT	SalesOrderHeader	AccountNumber	Financial	Confidential
<input type="checkbox"/>	SalesLT	SalesOrderHeader	CreditCardApprovalCode	Credit Card	Confidential
<input type="checkbox"/>	SalesLT	SalesOrderHeader	TaxAmt	Financial	Confidential

https://portal.azure.com/#

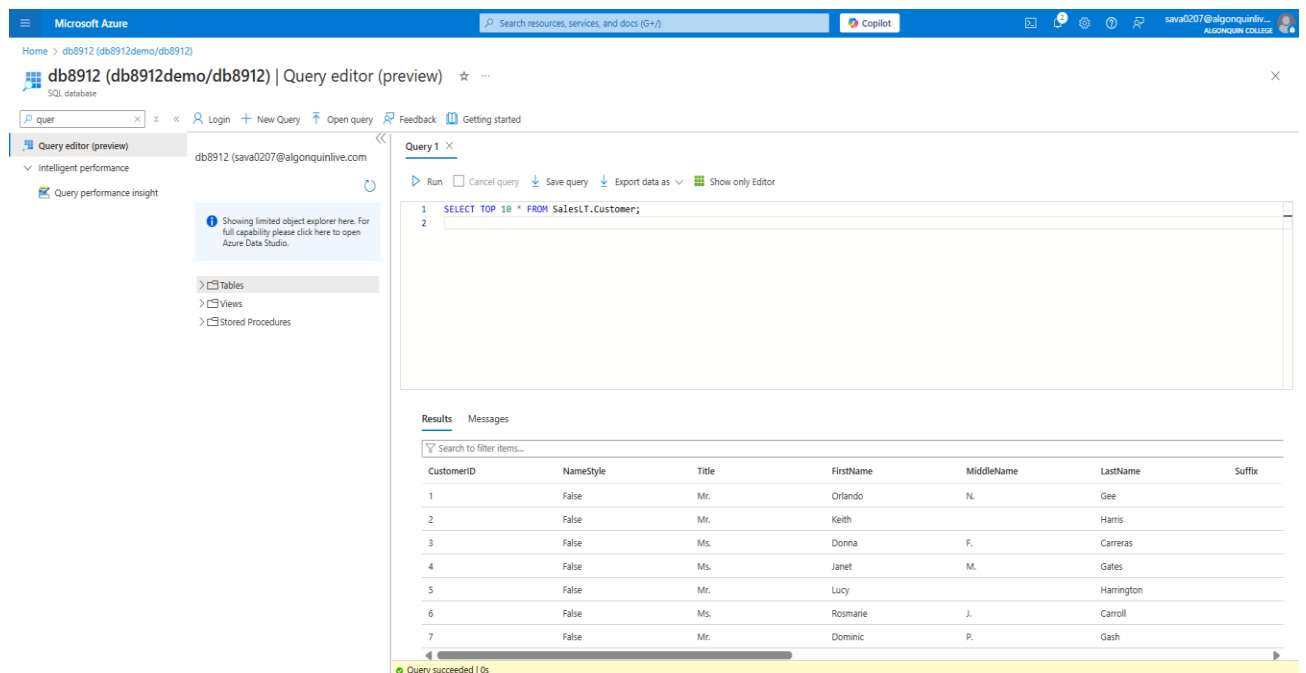
3.1 Showing Data Discovery & Classification with 15 columns



3.2 Overview of Classification



4.1 showing server level auditing is on



4.2 Run the query in query editor

Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

Home > db8912 (db8912demo/db8912) | Auditing >

Audit records

Refresh Filter Log Analytics View dashboard

This blade provides a sample of audit logs with limited fields within 1 hour 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 Mon, 24 Mar 2025 18:35:20 UTC.

Run in Query Editor

Event time (UTC)	Principal name	Event type	Action status
3/24/2025 6:32:11 PM	db8912tarang	BATCH COMPLETED	Succeeded
3/24/2025 6:32:11 PM	db8912tarang	DATABASE AUTHENTICATION SUCCEEDED	Succeeded
3/24/2025 6:31:53 PM	db8912tarang	BATCH COMPLETED	Succeeded
3/24/2025 6:31:53 PM	db8912tarang	DATABASE AUTHENTICATION SUCCEEDED	Succeeded
3/24/2025 6:31:52 PM	db8912tarang	DATABASE AUTHENTICATION SUCCEEDED	Succeeded
3/24/2025 6:31:52 PM	db8912tarang	BATCH COMPLETED	Succeeded

[Load more](#)

4.3 Showing audit records of Database audit

Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

Home > db8912 (db8912demo/db8912) | Auditing >

Audit records

Refresh Filter Log Analytics View dashboard

This blade provides a sample of audit logs with limited fields within 1 hour 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

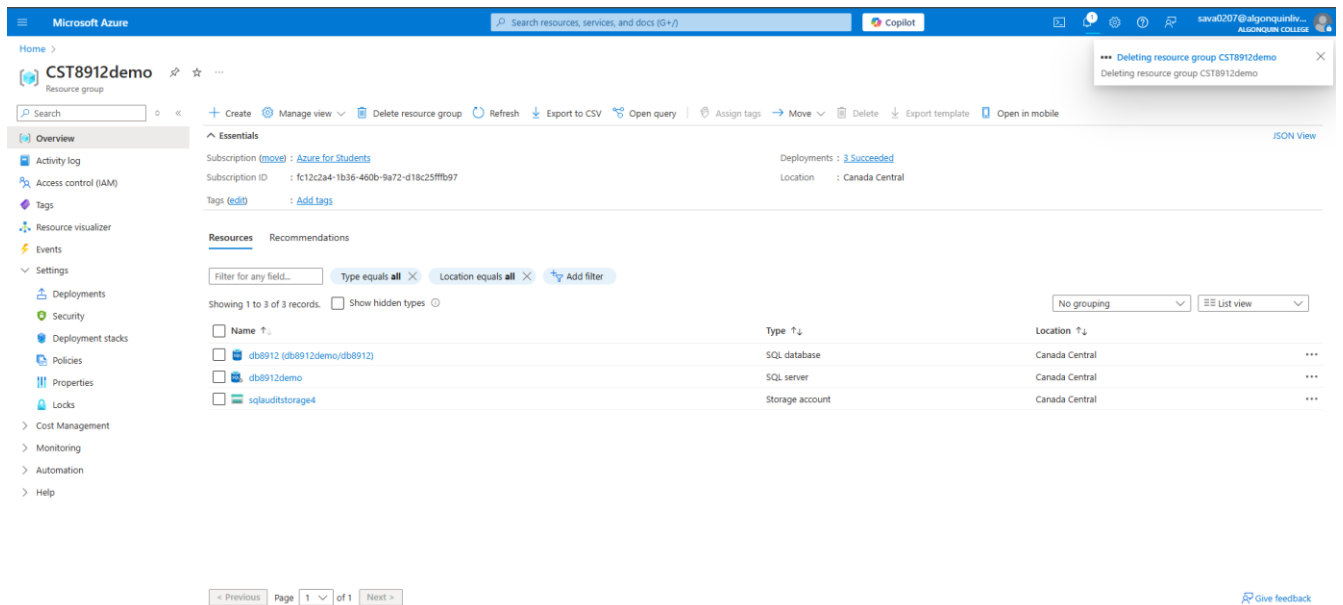
Showing audit records up to Mon, 24 Mar 2025 18:35:20 UTC.

Run in Query Editor

Event time (UTC)	Principal name	Event type	Action status
3/24/2025 6:32:11 PM	db8912tarang	BATCH COMPLETED	Succeeded
3/24/2025 6:32:11 PM	db8912tarang	DATABASE AUTHENTICATION SUCCEEDED	Succeeded
3/24/2025 6:31:53 PM	db8912tarang	BATCH COMPLETED	Succeeded
3/24/2025 6:31:53 PM	db8912tarang	DATABASE AUTHENTICATION SUCCEEDED	Succeeded
3/24/2025 6:31:52 PM	db8912tarang	DATABASE AUTHENTICATION SUCCEEDED	Succeeded
3/24/2025 6:31:52 PM	db8912tarang	BATCH COMPLETED	Succeeded

[Load more](#)

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.