Lab 9

CST8912_011

Yuntian Du

du000086

March 12, 2025

Submitted to :

Prof. **Ragini Madaan**

Evaluate the security and data privacy implications

# of various cloud solutions

Introduction & Purpose

Introduction:

Microsoft Azure includes tools to safeguard data according to your company's security and compliance needs.
Encryption at Rest is a common security requirement. In Azure, organizations can encrypt data at rest without the risk or cost of a custom key management solution. Organizations have the option of letting Azure completely manage Encryption at Rest. Additionally, organizations have various options to closely manage encryption or encryption keys.

Encryption is the secure encoding of data used to protect confidentiality of data. The Encryption at Rest designs in Azure use symmetric encryption to encrypt and decrypt large amounts of data quickly according to a simple conceptual model:

A symmetric encryption key is used to encrypt data as it is written to storage.
The same encryption key is used to decrypt that data as it is readied for use in memory.
Data may be partitioned, and different keys may be used for each partition.
Keys must be stored in a secure location with identity-based access control and audit policies. Data encryption keys which are stored outside of secure locations are encrypted with a key encryption key kept in a secure location.

Encryption at rest provides data protection for stored data (at rest). Attacks against data at-rest include attempts to obtain physical access to the hardware on which the data is stored, and then compromise the contained data. In such an attack, a server's hard drive may have been mishandled during maintenance allowing an attacker to remove the hard drive. Later the attacker would put the hard drive into a computer under their control to attempt to access the data.

Encryption at rest may also be required by an organization's need for data governance and compliance efforts. Industry and government regulations such as HIPAA, PCI and FedRAMP, lay out specific safeguards regarding data protection and encryption requirements.

How azure sql database encrypts data at rest: https://www.youtube.com/watch?v=oMmKIUZQL5Q

Purpose:

In this lab you will explore the security features offered by Microsoft for azure sql database.

- Protection against attacks such as SQL injection and data exfiltration.
- Ability to discover and classify database information into categories such as Confidential.
- Ability to audit database server and database queries and log events.

In this exercise, you will complete the following tasks:
Task 1: Deploy an Azure SQL Database
Task 2: Configure Advanced Data Protection
Task 3: Configure Data Classification
Task 4: Configure Auditing
Task 5: Clean resources created during lab

Steps covered in the lab

Task 1: Deploy an Azure SQL Database

Method1:

1. Configure Azure SQL database for Canada central region under your

resource group cst8912-demo, choose single database under sql databases in sql deployment option

2. Enter the following values in create database page and keep other properties with their default settings

    Subscription: Select your Azure subscription

    Resource group: CST8912demo

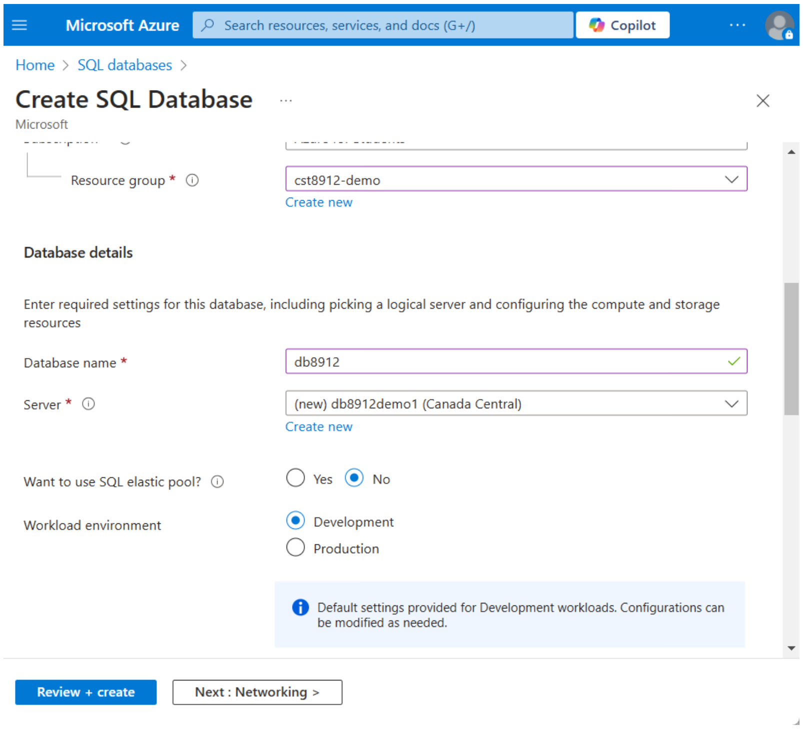
    Database name: db8912

    Server: Select Create new and create a new server with a unique name in any Canada central location. Use SQL authentication and specify your name as the server admin login and a suitably complex password (remember the password - you'll need it later!)

    Server : db8912demo

    Username:db8912yourname

    Password: dfguyt@234!



Create SQL Database

Microsoft

Resource group * : cst8912-demo
Create new

Database details

Enter required settings for this database, including picking a logical server and configuring the compute and storage resources

Database name * : db8912

Server * : (new) db8912demo1 (Canada Central)
Create new

Want to use SQL elastic pool? ○ Yes ● No

Workload environment ● Development ○ Production

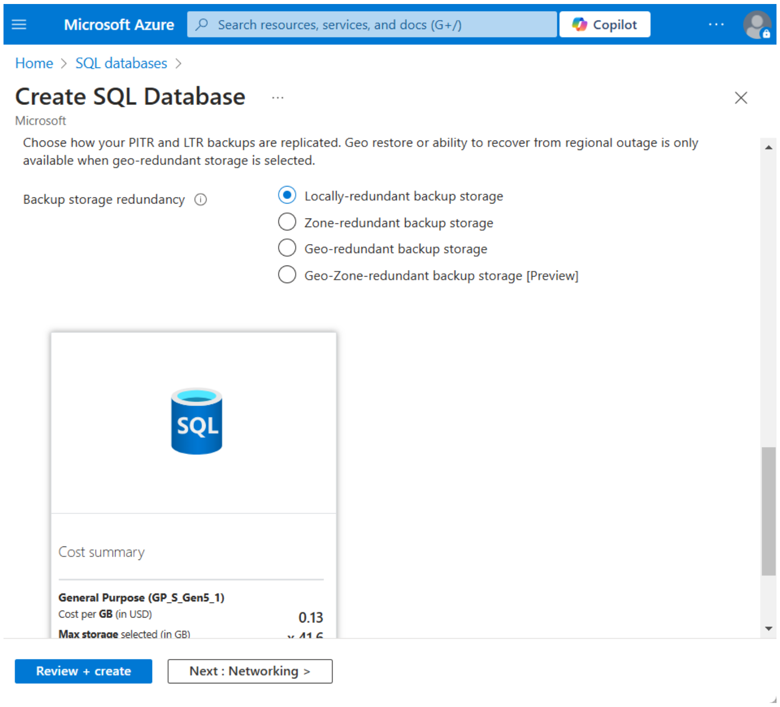
Default settings provided for Development workloads. Configurations can be modified as needed.

Want to use SQL elastic pool?: No

Workload environment: Development

Compute + storage: Leave unchanged

Backup storage redundancy: Locally-redundant backup storage



Create SQL Database

Microsoft

Choose how your PITR and LTR backups are replicated. Geo restore or ability to recover from regional outage is only available when geo-redundant storage is selected.

Backup storage redundancy ⓘ

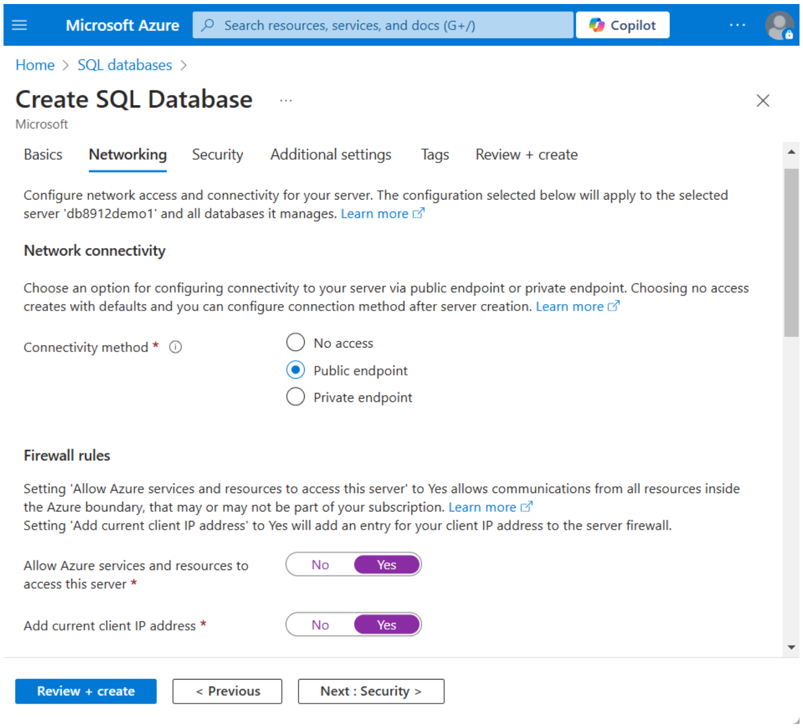
● Locally-redundant backup storage
○ Zone-redundant backup storage
○ Geo-redundant backup storage
○ Geo-Zone-redundant backup storage [Preview]

Cost summary

General Purpose (GP_S_Gen5_1)

Cost per **GB** (in USD)	0.13
Max storage selected (in GB)	x 41.6

3. On the Create SQL Database page, select Next :Networking >, and on the Networking page, in the Network connectivity section, select Public endpoint. Then select Yes for both options in the Firewall rules section to allow access to your database server from Azure services and your current client IP address.



Create SQL Database

Microsoft

Basics | **Networking** | Security | Additional settings | Tags | Review + create

Configure network access and connectivity for your server. The configuration selected below will apply to the selected server 'db8912demo1' and all databases it manages. Learn more

Network connectivity

Choose an option for configuring connectivity to your server via public endpoint or private endpoint. Choosing no access creates with defaults and you can configure connection method after server creation. Learn more

Connectivity method *
○ No access
● Public endpoint
○ Private endpoint

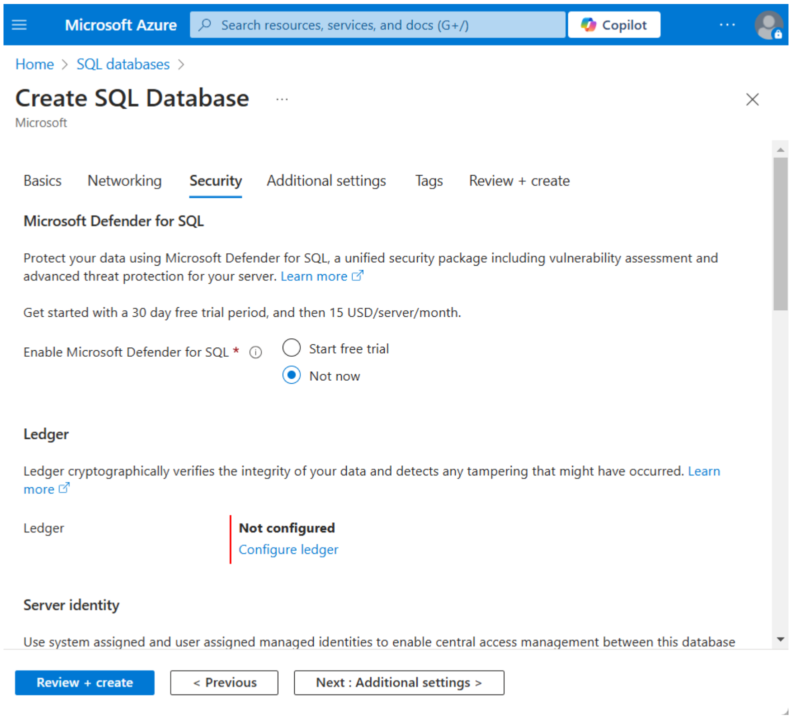
Firewall rules

Setting 'Allow Azure services and resources to access this server' to Yes allows communications from all resources inside the Azure boundary, that may or may not be part of your subscription. Learn more
Setting 'Add current client IP address' to Yes will add an entry for your client IP address to the server firewall.

Allow Azure services and resources to access this server * No [✓ Yes]

Add current client IP address * No [✓ Yes]

4. Select Next: Security > and set the Enable Microsoft Defender for SQL option to Not now.



Create SQL Database

Microsoft

Basics | Networking | **Security** | Additional settings | Tags | Review + create

Microsoft Defender for SQL

Protect your data using Microsoft Defender for SQL, a unified security package including vulnerability assessment and advanced threat protection for your server. Learn more

Get started with a 30 day free trial period, and then 15 USD/server/month.

Enable Microsoft Defender for SQL *
○ Start free trial
● Not now

Ledger

Ledger cryptographically verifies the integrity of your data and detects any tampering that might have occurred. Learn more

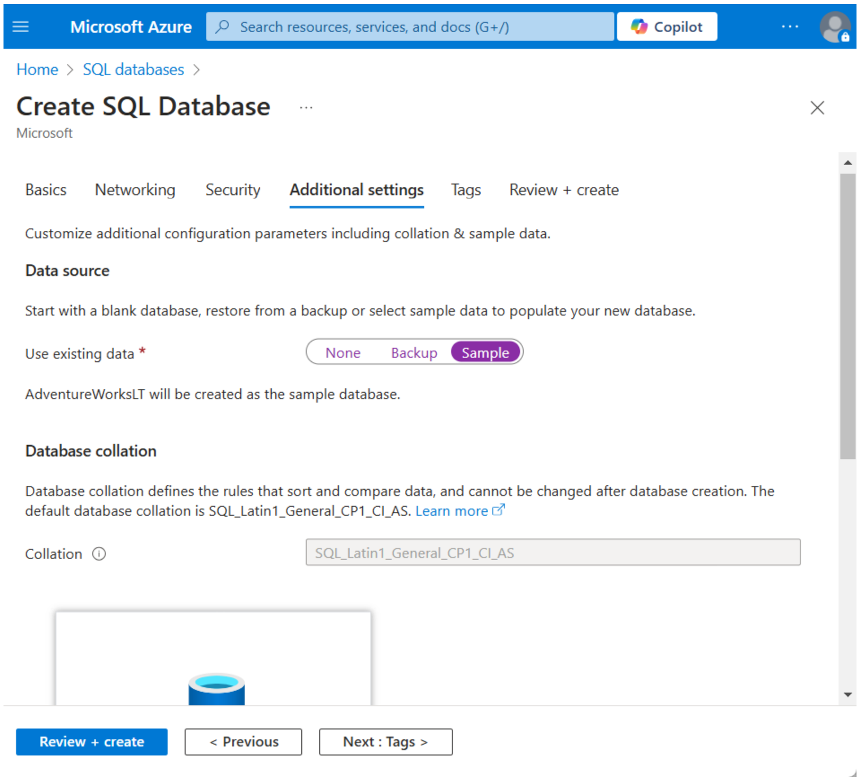
Ledger **Not configured**
Configure ledger

Server identity

Use system assigned and user assigned managed identities to enable central access management between this database

5. Select Next: Additional Settings > and on the Additional settings tab, set the Use existing data option to Sample (this will create a sample

database that you can explore later).



Create SQL Database

Microsoft

Customize additional configuration parameters including collation & sample data.

Data source

Start with a blank database, restore from a backup or select sample data to populate your new database.

Use existing data * None Backup [✓ Sample]

AdventureWorksLT will be created as the sample database.

Database collation

Database collation defines the rules that sort and compare data, and cannot be changed after database creation. The default database collation is SQL_Latin1_General_CP1_CI_AS. Learn more

Collation: SQL_Latin1_General_CP1_CI_AS

6. Select Review + Create, and then select Create to create your Azure SQL database.

Method 2:

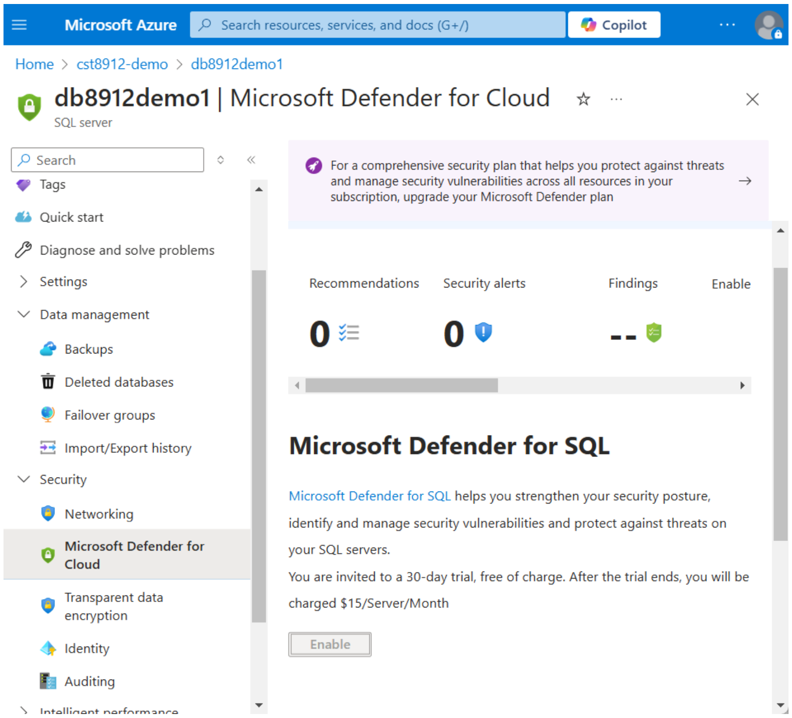
1. In the Azure portal, in the Search resources, services, and docs text box at the top of the Azure portal page, type Deploy a custom template and press the Enter key.
2. On the Custom deployment blade, click the Build your own template in the editor option.
3. On the Edit template blade, click Load file , locate the https://github.com/MicrosoftLearning/AZ500-AzureSecurityTechnologies/blob/master/Allfiles/Labs/11/azuredeploy.json file and click Open.
4. On the Edit template blade, click Save.
5. On the Custom deployment blade, ensure that the following settings are configured (leave any others with their default values):

Setting	Value
Subscription	Azure subscription
Resource group	CST8912
Location	**Canada Central**

6. Click Review + Create and then click Create.

Task 2: Configure Advanced Data Protection

1. On the SQL server blade, in the Security section, click Microsoft Defender for Cloud, select Enable Microsoft Defender for SQL.



For a comprehensive security plan that helps you protect against threats and manage security vulnerabilities across all resources in your subscription, upgrade your Microsoft Defender plan

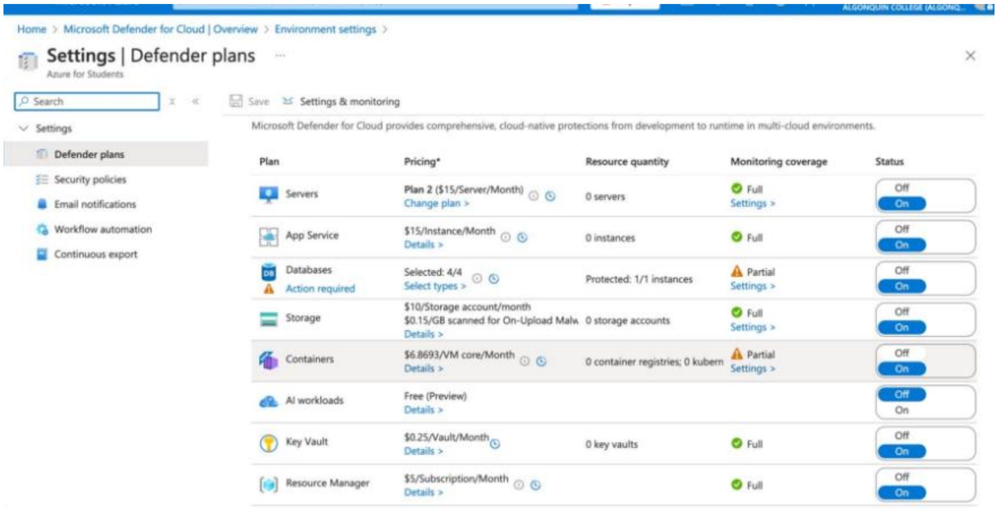
Microsoft Defender for SQL

Microsoft Defender for SQL helps you strengthen your security posture, identify and manage security vulnerabilities and protect against threats on your SQL servers.

You are invited to a 30-day trial, free of charge. After the trial ends, you will be charged $15/Server/Month

Enable

2. 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)
3. On the Server Settings blade, review the information about pricing and the trial period, VULNERABILITY ASSESSMENT SETTINGS and ADVANCED THREAT PROTECTION SETTINGS.

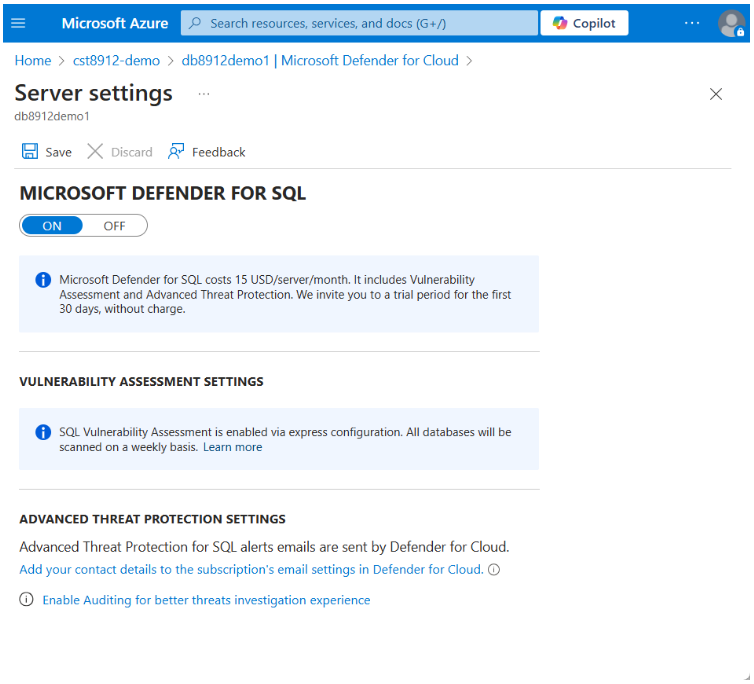


Settings | Defender plans

Azure for Students

Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments.

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Servers	Plan 2 ($15/Server/Month) Change plan >	0 servers	✓ Full Settings >	Off [✓ On]
App Service	$15/Instance/Month Details >	0 instances	✓ Full	Off [✓ On]
Databases ⚠ Action required	Selected: 4/4 Select types >	Protected: 1/1 instances	⚠ Partial Settings >	Off [✓ On]
Storage	$10/Storage account/month $0.15/GB scanned for On-Upload Malw Details >	0 storage accounts	✓ Full Settings >	Off [✓ On]
Containers	$6.8693/VM core/Month Details >	0 container registries; 0 kubern	⚠ Partial Settings >	Off [✓ On]
AI workloads	Free (Preview) Details >			[✓ Off] On
Key Vault	$0.25/Vault/Month Details >	0 key vaults	✓ Full	Off [✓ On]
Resource Manager	$5/Subscription/Month Details >		✓ Full	Off [✓ On]



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > cst8912-demo > db8912demo1 | Microsoft Defender for Cloud >
Save
Discard
Feedback

Server settings

db8912demo1

MICROSOFT DEFENDER FOR SQL

[✓ ON] OFF

Microsoft Defender for SQL costs 15 USD/server/month. It includes Vulnerability Assessment and Advanced Threat Protection. We invite you to a trial period for the first 30 days, without charge.

VULNERABILITY ASSESSMENT SETTINGS

SQL Vulnerability Assessment is enabled via express configuration. All databases will be scanned on a weekly basis. Learn more

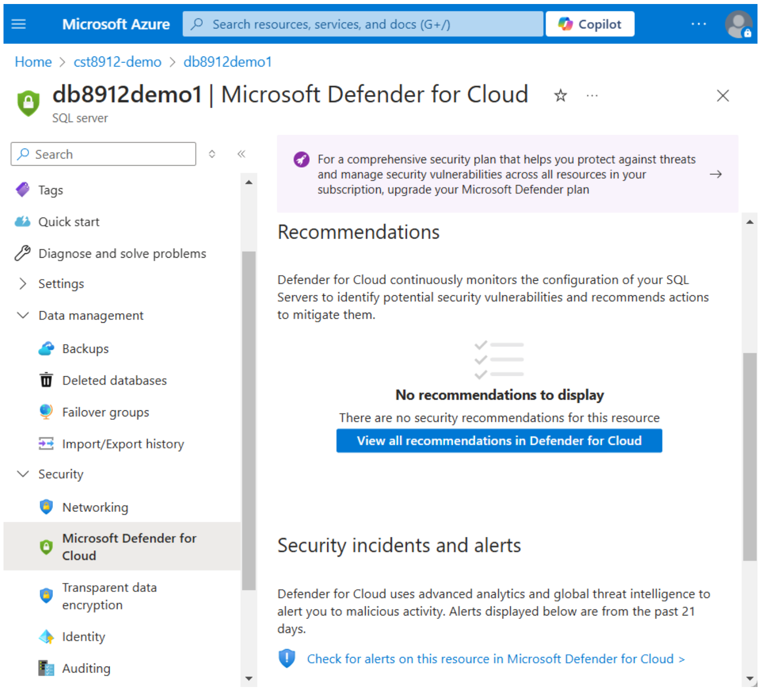
ADVANCED THREAT PROTECTION SETTINGS

Advanced Threat Protection for SQL alerts emails are sent by Defender for Cloud.

Add your contact details to the subscription's email settings in Defender for Cloud.

Enable Auditing for better threats investigation experience

4. Back to Microsoft Defender for Cloud blade, review Recommendations and Security alerts.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > cst8912-demo > db8912demo1
db8912demo1 | Microsoft Defender for Cloud
SQL server
Search
Tags
Quick start
Diagnose and solve problems
Settings
Data management
Backups
Deleted databases
Failover groups
Import/Export history
Security
Networking
Microsoft Defender for Cloud
Transparent data encryption
Identity
Auditing
View all recommendations in Defender for Cloud
Check for alerts on this resource in Microsoft Defender for Cloud >

For a comprehensive security plan that helps you protect against threats and manage security vulnerabilities across all resources in your subscription, upgrade your Microsoft Defender plan

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

There are no security recommendations for this resource

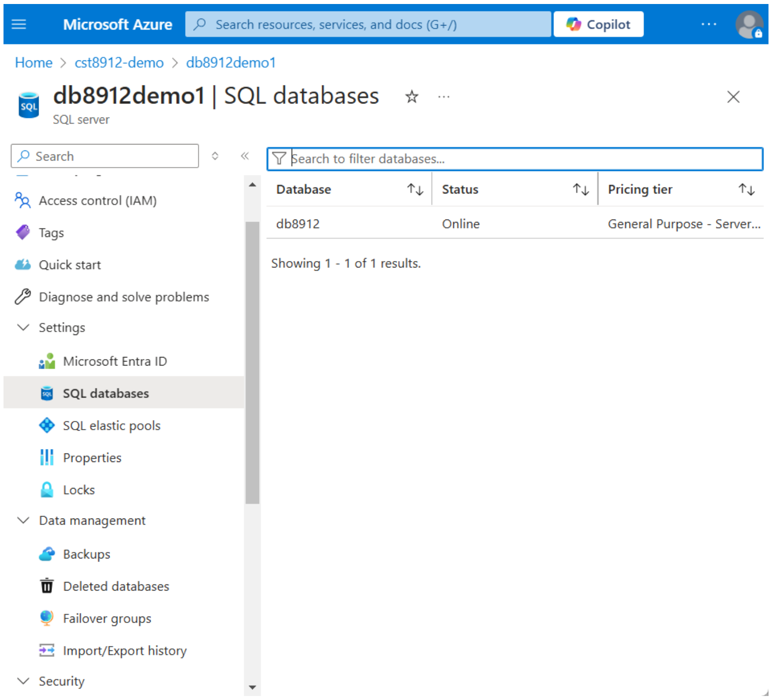
Security incidents and alerts

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.

Task 3: Configure Data Classification

In this task, you will explore and classify data in SQL database for GPDR and data protection compliance.

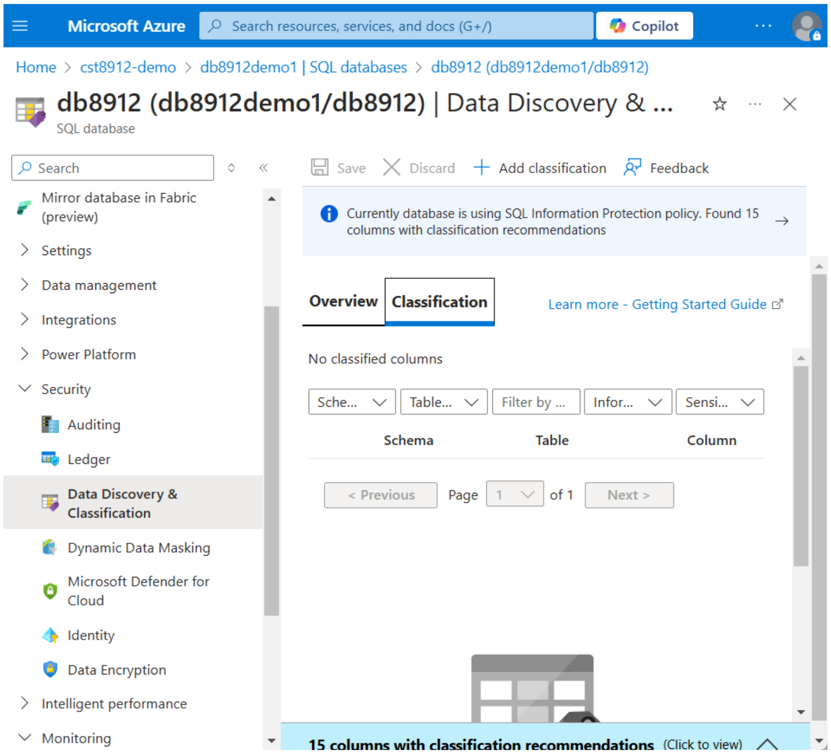
1. On the SQL server blade, in the Settings section, click SQL Databases.



Database	Status	Pricing tier
db8912	Online	General Purpose - Server...

Showing 1 - 1 of 1 results.

2. On the SQL database blade, in the Security section, click Data Discovery & Classification.
3. On the Data Discovery & Classification blade, click the Classification tab.

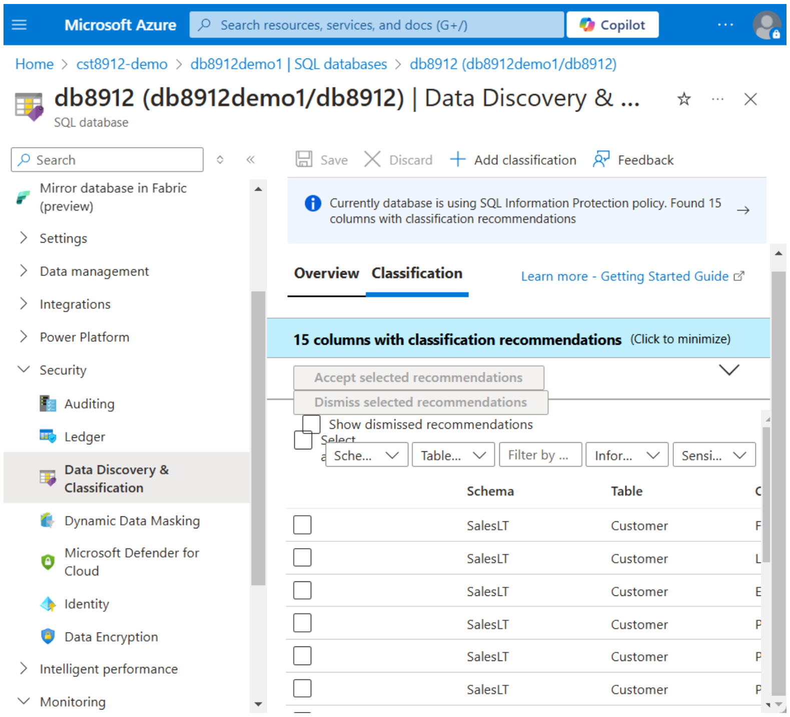


Currently database is using SQL Information Protection policy. Found 15 columns with classification recommendations

No classified columns

15 columns with classification recommendations (Click to view)

4. Click the text message We have found 15 columns with classification recommendations displayed on blue bar at the top of the blade.

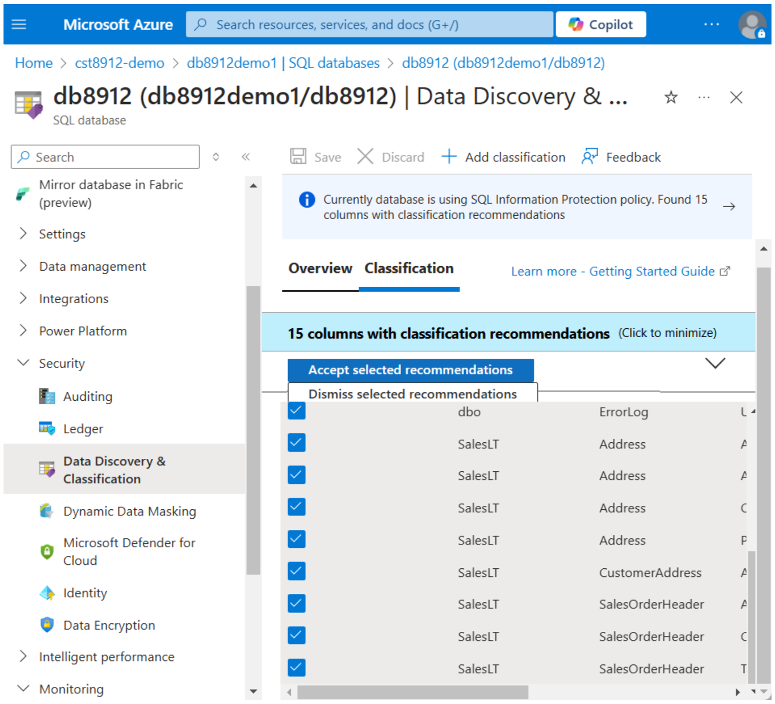

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > cst8912-demo > db8912demo1 | SQL databases > db8912 (db8912demo1/db8912)
db8912 (db8912demo1/db8912) | Data Discovery & ...
SQL database
Search
Mirror database in Fabric (preview)
Settings
Data management
Integrations
Power Platform
Security
Auditing
Ledger
Data Discovery & Classification
Dynamic Data Masking
Microsoft Defender for Cloud
Identity
Data Encryption
Intelligent performance
Monitoring
Save
Discard
Add classification
Feedback
Overview
Classification
Learn more - Getting Started Guide
Accept selected recommendations
Dismiss selected recommendations
Show dismissed recommendations
Select a
Sche...
Table...
Filter by ...
Infor...
Sensi...

Currently database is using SQL Information Protection policy. Found 15 columns with classification recommendations

15 columns with classification recommendations (Click to minimize)

	Schema	Table	C
□	SalesLT	Customer	F
□	SalesLT	Customer	L
□	SalesLT	Customer	E
□	SalesLT	Customer	P
□	SalesLT	Customer	P
□	SalesLT	Customer	P

5. Review the listed columns and the recommended sensitivity label.
6. Enable the Select all checkbox and then click Accept Selected Recommendations.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > cst8912-demo > db8912demo1 | SQL databases > db8912 (db8912demo1/db8912)
Search
Mirror database in Fabric (preview)
Settings
Data management
Integrations
Power Platform
Security
Auditing
Ledger
Data Discovery & Classification
Dynamic Data Masking
Microsoft Defender for Cloud
Identity
Data Encryption
Intelligent performance
Monitoring
Save
Discard
Add classification
Feedback
Overview
Classification
Learn more - Getting Started Guide
Accept selected recommendations
Dismiss selected recommendations

db8912 (db8912demo1/db8912) | Data Discovery & ...

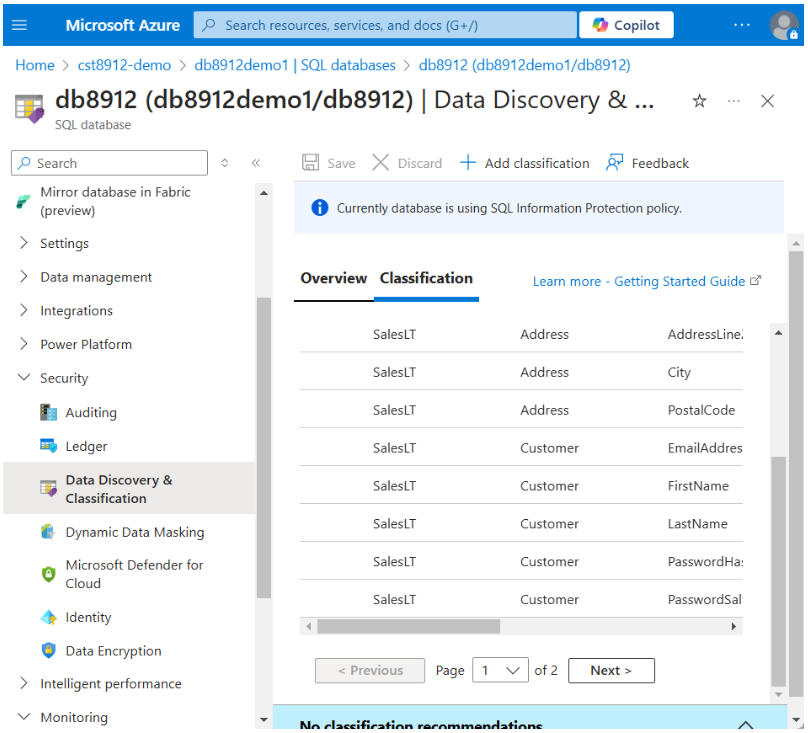
SQL database

Currently database is using SQL Information Protection policy. Found 15 columns with classification recommendations

15 columns with classification recommendations (Click to minimize)

☑	dbo	ErrorLog	L
☑	SalesLT	Address	A
☑	SalesLT	Address	A
☑	SalesLT	Address	C
☑	SalesLT	Address	P
☑	SalesLT	CustomerAddress	A
☑	SalesLT	SalesOrderHeader	A
☑	SalesLT	SalesOrderHeader	C
☑	SalesLT	SalesOrderHeader	T

7. Once you have completed your review click Save.
8. Back on the Data Discovery & Classification blade Overview tab, note that it has been updated to account for the latest classification information.



db8912 (db8912demo1/db8912) | Data Discovery & ...

SQL database

Currently database is using SQL Information Protection policy.

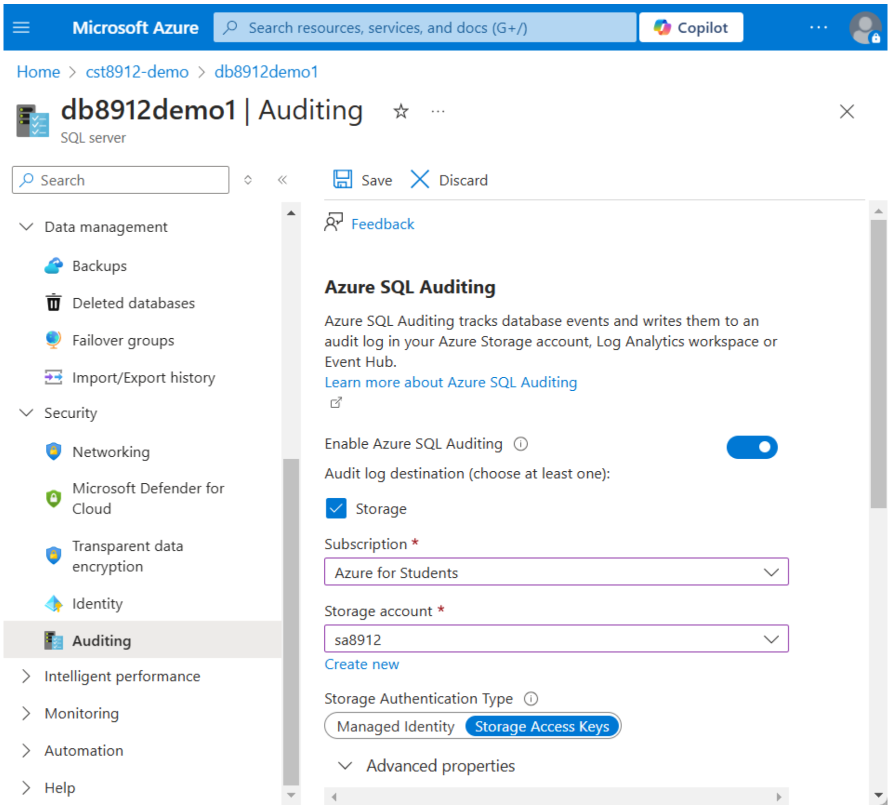
SalesLT	Address	AddressLine
SalesLT	Address	City
SalesLT	Address	PostalCode
SalesLT	Customer	EmailAddres
SalesLT	Customer	FirstName
SalesLT	Customer	LastName
SalesLT	Customer	PasswordHa
SalesLT	Customer	PasswordSal

No classification recommendations

Task 4: Configure Auditing

In this task, you will first configure server level auditing and then configure database level auditing.

1. In the Azure portal, navigate back to the SQL Server blade.
2. On the SQL Server blade, in the Security section, click Auditing.
3. Set the Enable Azure SQL Auditing switch to ON to enable auditing
4. Select the Storage checkbox and entry boxes for Subscription and Storage Account will display (create new storage account if not selected)
5. Choose your Subscription from the dropdown list.
6. Click Storage account and choose Create new.



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

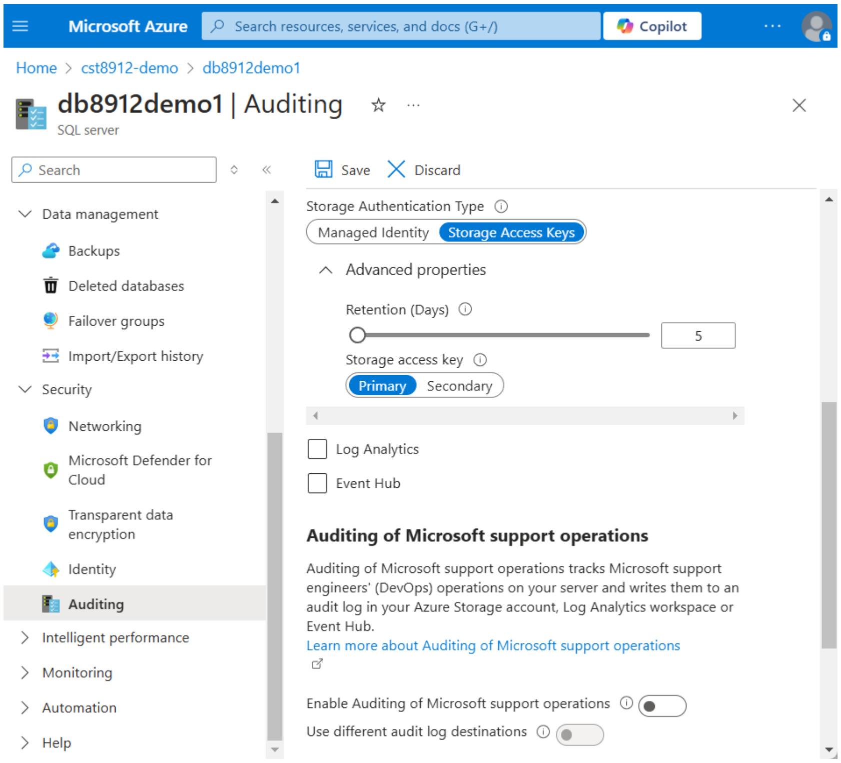
Subscription *
Azure for Students

Storage account *
sa8912
Create new

Storage Authentication Type ⓘ
Managed Identity | Storage Access Keys

Advanced properties

7. Back on the Auditing blade, under Advanced properties set Retention (days) to 5.



db8912demo1 | Auditing

SQL server

Storage Authentication Type: Managed Identity | Storage Access Keys

Advanced properties

Retention (Days): 5

Storage access key: Primary | Secondary

☐ Log Analytics

☐ Event Hub

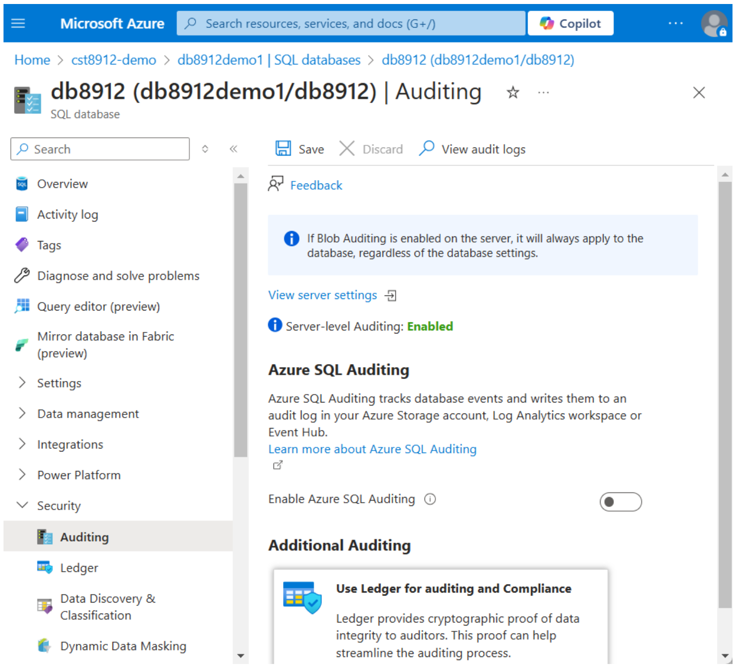
Auditing of Microsoft support operations

Auditing of Microsoft support operations tracks Microsoft support engineers' (DevOps) operations on your server and writes them to an audit log in your Azure Storage account, Log Analytics workspace or Event Hub.
Learn more about Auditing of Microsoft support operations

Enable Auditing of Microsoft support operations ○

Use different audit log destinations ○

8. On the Auditing blade, click Save to save the auditing settings
9. On the server blade, in the Settings section, click SQL Databases.
10. On the SQL database blade, in the Security section, click Auditing.
    Note: This is database level auditing. Server-level auditing is already enabled.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > cst8912-demo > db8912demo1 | SQL databases > db8912 (db8912demo1/db8912)
Search
Overview
Activity log
Tags
Diagnose and solve problems
Query editor (preview)
Mirror database in Fabric (preview)
Settings
Data management
Integrations
Power Platform
Security
Auditing
Ledger
Data Discovery & Classification
Dynamic Data Masking
Save
Discard
View audit logs
Feedback

db8912 (db8912demo1/db8912) | Auditing

SQL database

If Blob Auditing is enabled on the server, it will always apply to the database, regardless of the database settings.

View server settings

Server-level Auditing: **Enabled**

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

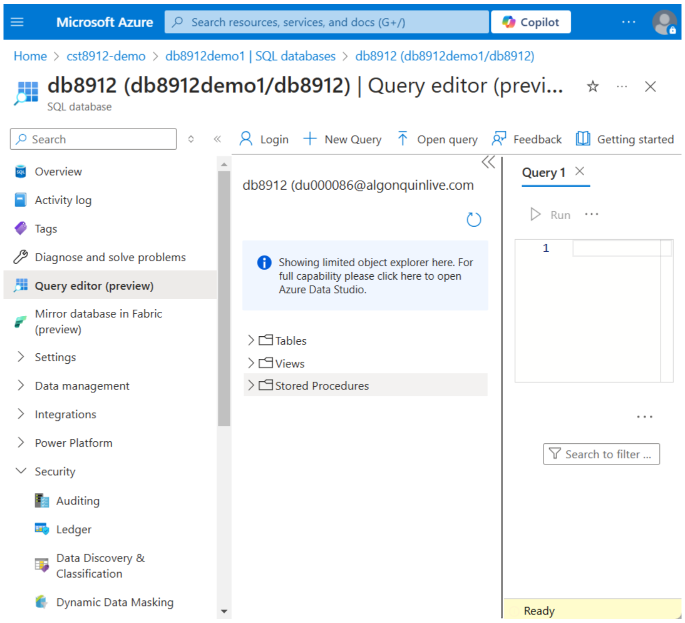
Enable Azure SQL Auditing ○

Additional Auditing

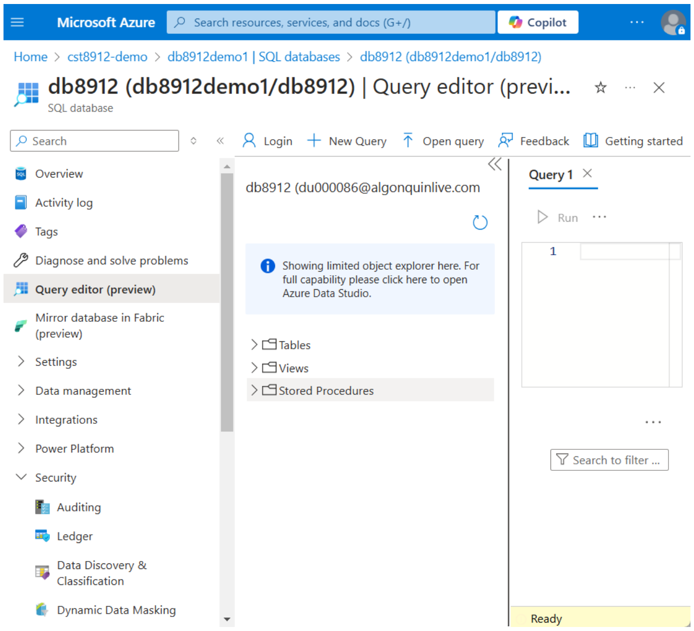
Use Ledger for auditing and Compliance

Ledger provides cryptographic proof of data integrity to auditors. This proof can help streamline the auditing process.

11. On your SQL database Overview page in the Azure portal, select Query editor (preview) from the left menu. Try to sign in, you might fail on password, firewall rule for your IP address, everything gets audited. Try successful login as well, run query and you might find more details in audit logs

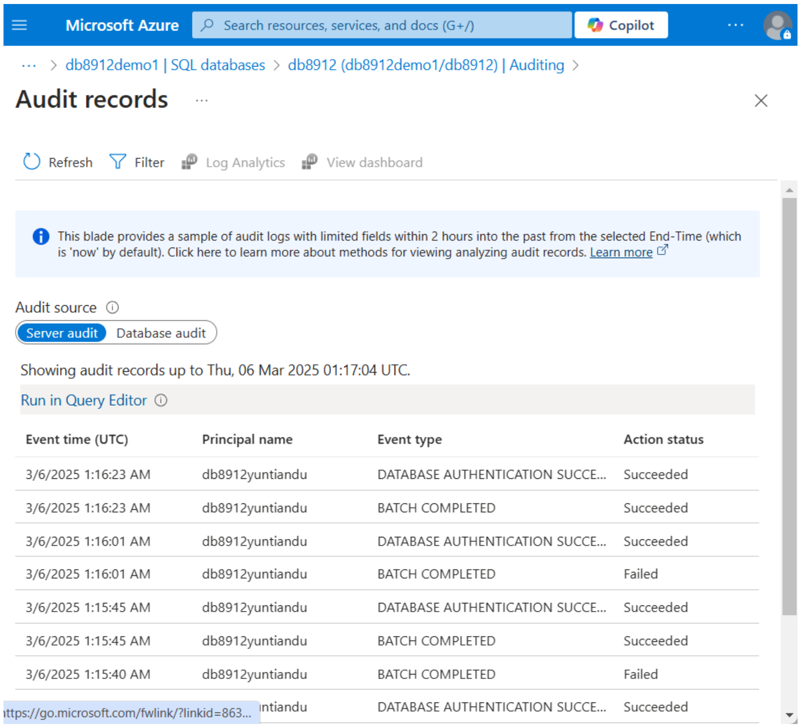

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > cst8912-demo > db8912demo1 | SQL databases > db8912 (db8912demo1/db8912)
db8912 (db8912demo1/db8912) | Query editor (previ...
SQL database
Search
Login
New Query
Open query
Feedback
Getting started
Overview
Activity log
Tags
Diagnose and solve problems
Query editor (preview)
Mirror database in Fabric (preview)
Settings
Data management
Integrations
Power Platform
Security
Auditing
Ledger
Data Discovery & Classification
Dynamic Data Masking
db8912 (du000086@algonquinlive.com
Tables
Views
Stored Procedures
Query 1
Run
Search to filter ...
Ready

Showing limited object explorer here. For full capability please click here to open Azure Data Studio.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > cst8912-demo > db8912demo1 | SQL databases > db8912 (db8912demo1/db8912)
db8912 (db8912demo1/db8912) | Query editor (previ...
SQL database
Search
Login
New Query
Open query
Feedback
Getting started
Overview
Activity log
Tags
Diagnose and solve problems
Query editor (preview)
Mirror database in Fabric (preview)
Settings
Data management
Integrations
Power Platform
Security
Auditing
Ledger
Data Discovery & Classification
Dynamic Data Masking
db8912 (du000086@algonquinlive.com
Tables
Views
Stored Procedures
Query 1
Run
Search to filter ...
Ready

Showing limited object explorer here. For full capability please click here to open Azure Data Studio.

12. switch back to DB, Auditing and Click View Audit Logs.



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
··· > db8912demo1 | SQL databases > db8912 (db8912demo1/db8912) | Auditing >
Audit records
Refresh
Filter
Log Analytics
View dashboard

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 Thu, 06 Mar 2025 01:17:04 UTC.

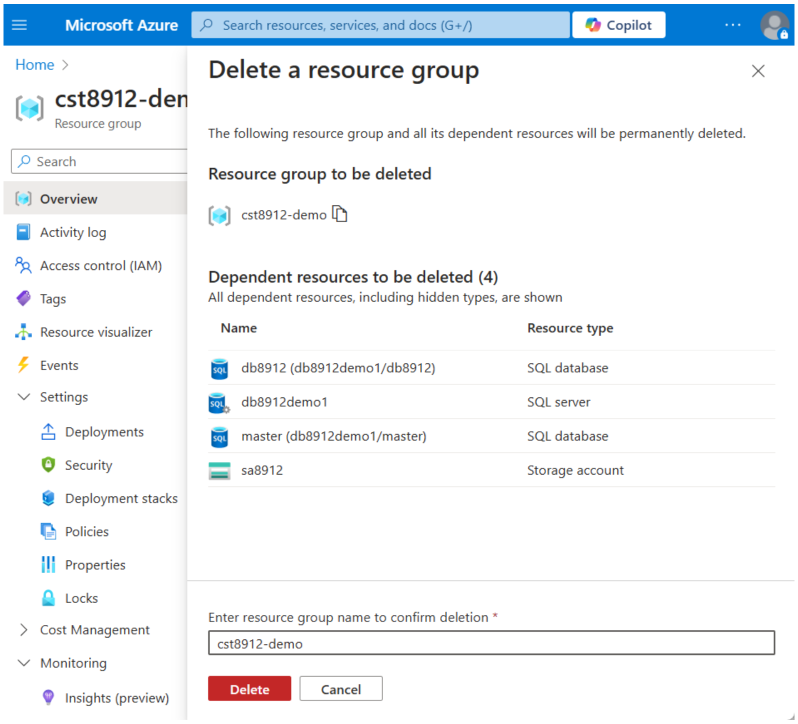
Run in Query Editor

Event time (UTC)	Principal name	Event type	Action status
3/6/2025 1:16:23 AM	db8912yuntiandu	DATABASE AUTHENTICATION SUCCE...	Succeeded
3/6/2025 1:16:23 AM	db8912yuntiandu	BATCH COMPLETED	Succeeded
3/6/2025 1:16:01 AM	db8912yuntiandu	DATABASE AUTHENTICATION SUCCE...	Succeeded
3/6/2025 1:16:01 AM	db8912yuntiandu	BATCH COMPLETED	Failed
3/6/2025 1:15:45 AM	db8912yuntiandu	DATABASE AUTHENTICATION SUCCE...	Succeeded
3/6/2025 1:15:45 AM	db8912yuntiandu	BATCH COMPLETED	Succeeded
3/6/2025 1:15:40 AM	db8912yuntiandu	BATCH COMPLETED	Failed
ittps://go.microsoft.com/fwlink/?linkid=863...	ıntiandu	DATABASE AUTHENTICATION SUCCE...	Succeeded

13. On the Audit records blade, note that you can switch between Server audit and Database audit.

Task 5: Clean up resources created during this lab

Deliverable: Delete all the resources created during this lab and document all the steps with screenshots in lab report.



Delete a resource group

The following resource group and all its dependent resources will be permanently deleted.

Resource group to be deleted

cst8912-demo

Dependent resources to be deleted (4)

All dependent resources, including hidden types, are shown

Name	Resource type
db8912 (db8912demo1/db8912)	SQL database
db8912demo1	SQL server
master (db8912demo1/master)	SQL database
sa8912	Storage account

Enter resource group name to confirm deletion *

cst8912-demo

References

None.