

## CST8912 – Cloud Solution Architecture

---

### Graded Lab Activity #9

#### 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:

#### 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

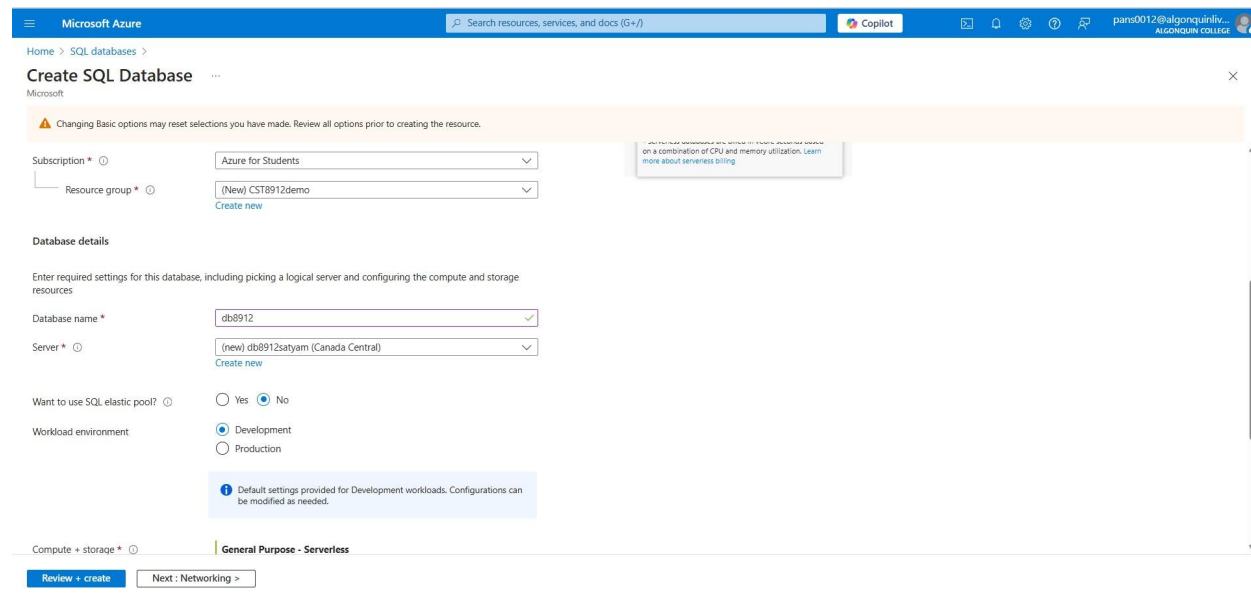
Username:db8912yourname

Password: dfguyt@234!

Want to use SQL elastic pool?: No

Workload environment: Development

Compute + storage: Leave unchanged



Microsoft Azure

Home > SQL databases >

### Create SQL Database

Microsoft

Changing Basic options may reset selections you have made. Review all options prior to creating the resource.

Subscription \* Azure for Students

Resource group \* (New) CST8912demo

[Create new](#)

and further optimize your server on a combination of CPU and memory utilization. Learn more about serverless billing.

#### 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) db8912satyam (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.

Compute + storage \* General Purpose - Serverless

[Review + create](#) [Next: Networking >](#)

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > SQL databases >

## Create SQL Database

Microsoft

⚠ Changing Basic options may reset selections you have made. Review all options prior to creating the resource.

Want to use SQL elastic pool? ☐ Yes ☒ No

Workload environment ☒ Development ☐ Production

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

Compute + storage \* ☐ **General Purpose - Serverless**  
Standard-series (Gen5), 1 vCore, 32 GB storage, zone redundant disabled  
[Configure database](#)

Backup storage redundancy

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]

[Review + create](#) [Next: Networking >](#)

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > SQL databases > 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 \*  ✓  
database.windows.net

Location \*  ✓

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

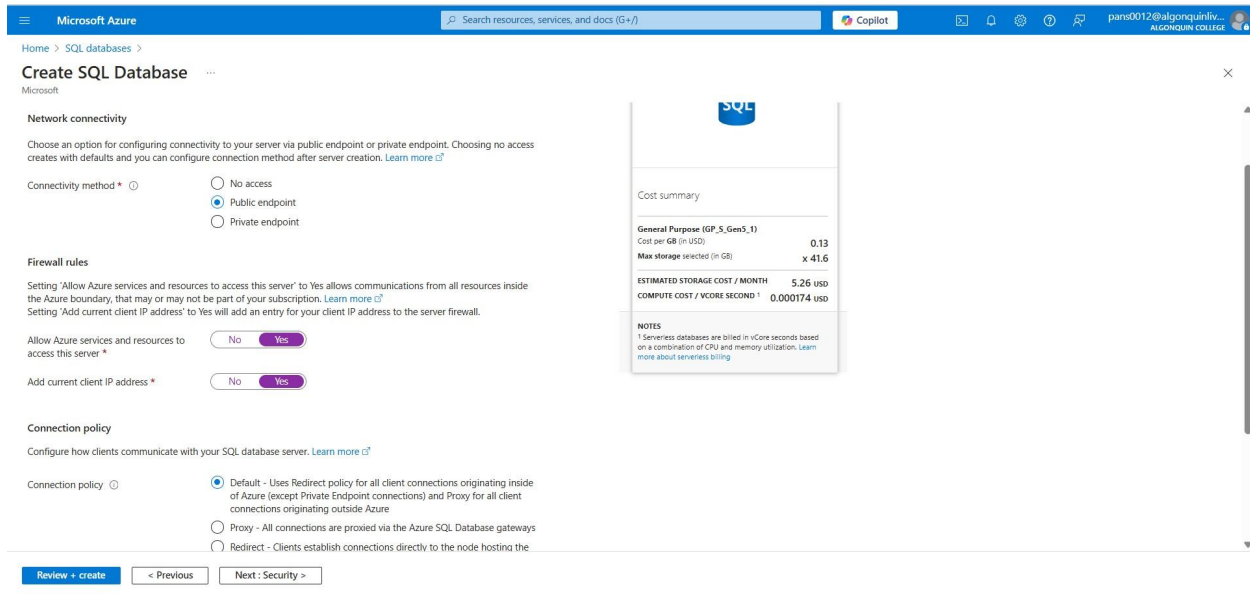
Server admin login \*  ✓

Password \*  ✓

[OK](#) ✔ Password and confirm password must match.

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.



**Microsoft Azure** | Search resources, services, and docs (G+/I) | Copilot | pans0012@algonquiniv... ALGONQUIN COLLEGE

Home > SQL databases >

### Create SQL Database

Microsoft

**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 \*

Add current client IP address \*

**Connection policy**

Configure how clients communicate with your SQL database server. [Learn more](#)

Connection policy \*

- ☒ Default - Uses Redirect policy for all client connections originating inside of Azure (except Private Endpoint connections) and Proxy for all client connections originating outside Azure
- ☐ Proxy - All connections are proxied via the Azure SQL Database gateways
- ☐ Redirect - Clients establish connections directly to the node hosting the

[Review + create](#) [< Previous](#) [Next: Security >](#)

**Cost summary**

**General Purpose (GP\_S\_Gen5\_1)**

Cost per GB (in USD) 0.13

Max storage selected (in GB) x 41.6

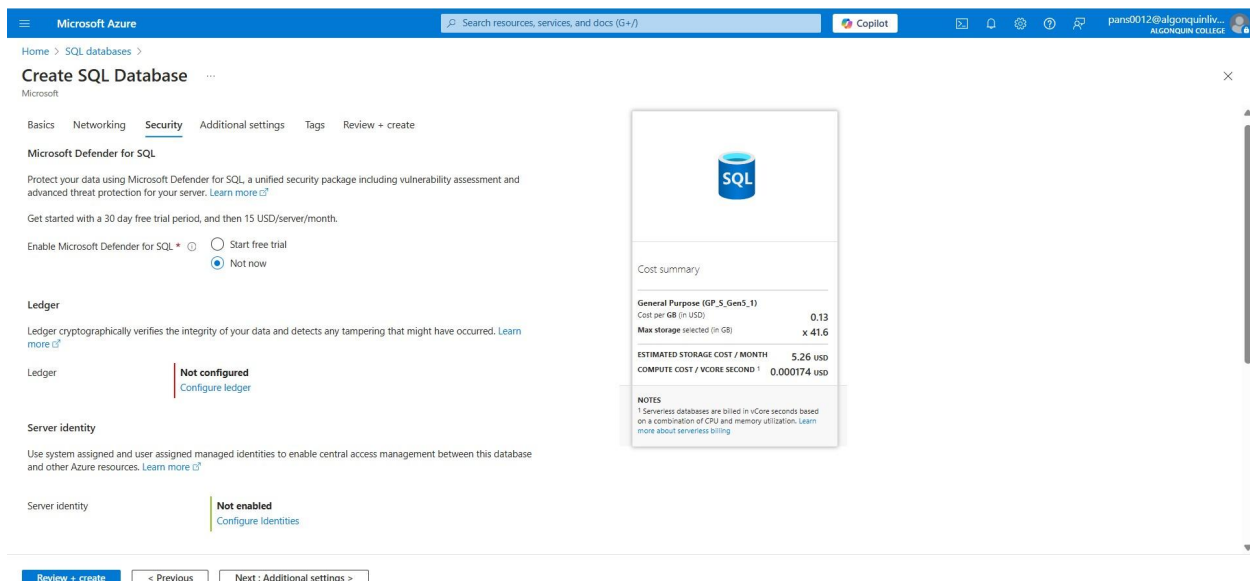
ESTIMATED STORAGE COST / MONTH 5.26 USD

COMPUTE COST / VCORE SECOND <sup>1</sup> 0.000174 USD

**NOTES**

<sup>1</sup> Serverless databases are billed in vCore seconds based on a combination of CPU and memory utilization. [Learn more about serverless billing](#)

4. Select Next: Security > and set the Enable Microsoft Defender for SQL option to Notnow.



**Microsoft Azure** | Search resources, services, and docs (G+/I) | Copilot | pans0012@algonquiniv... ALGONQUIN COLLEGE

Home > SQL databases >

### 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 and other Azure resources. [Learn more](#)

Server identity **Not enabled**  
[Configure identities](#)

[Review + create](#) [< Previous](#) [Next: Additional settings >](#)

**Cost summary**

**General Purpose (GP\_S\_Gen5\_1)**

Cost per GB (in USD) 0.13

Max storage selected (in GB) x 41.6

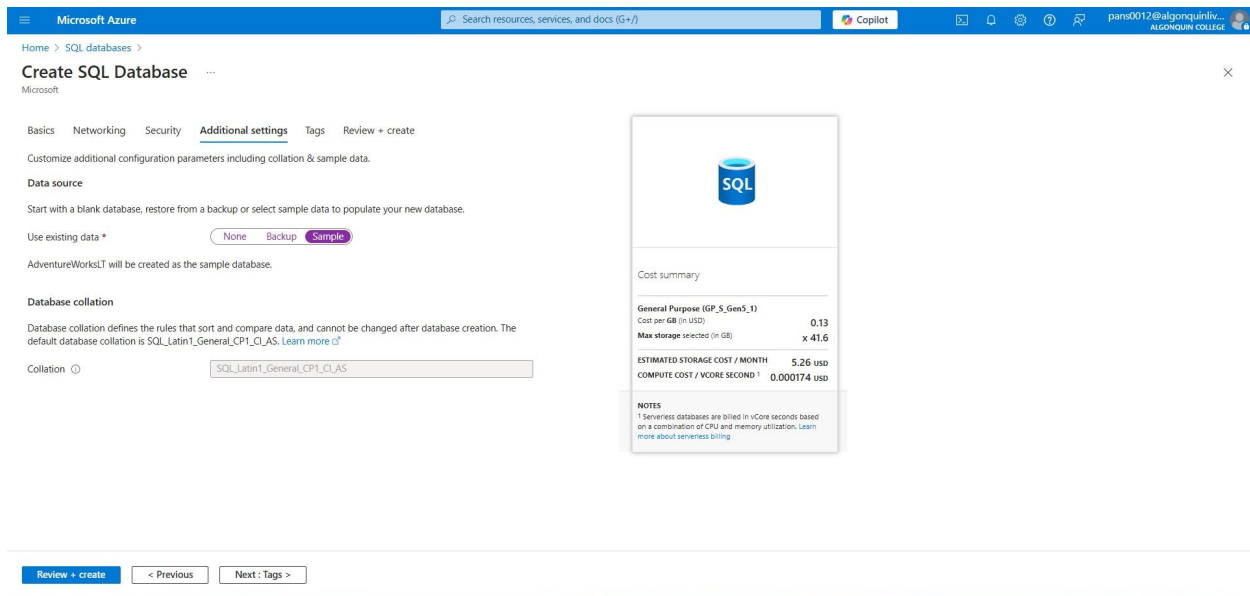
ESTIMATED STORAGE COST / MONTH 5.26 USD

COMPUTE COST / VCORE SECOND <sup>1</sup> 0.000174 USD

**NOTES**

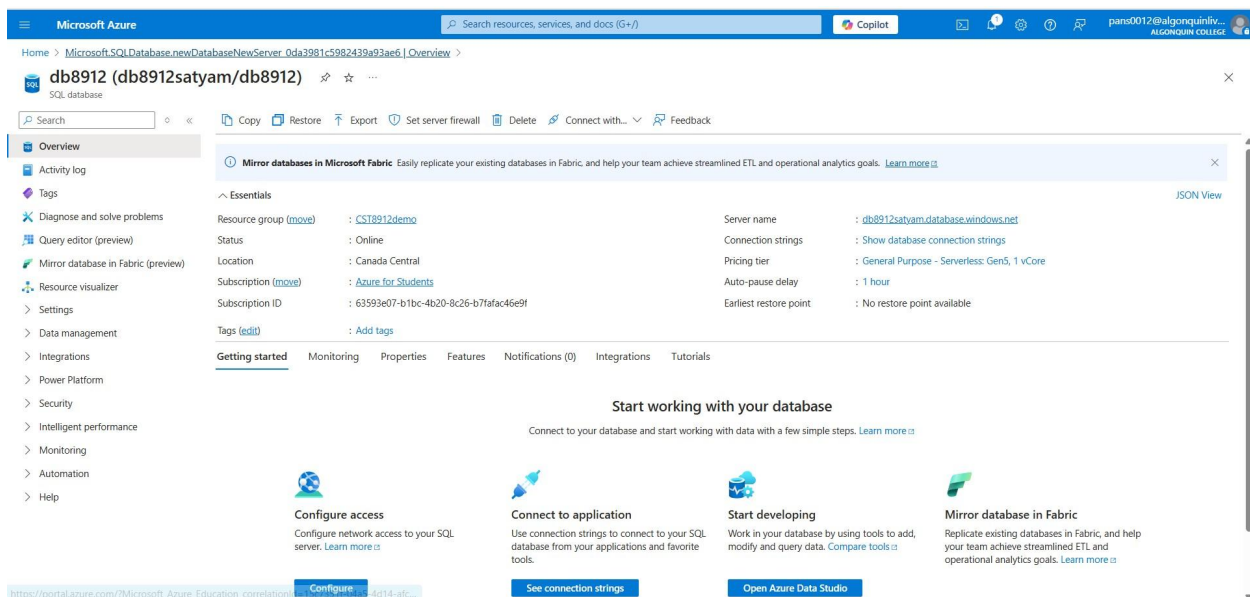
<sup>1</sup> Serverless databases are billed in vCore seconds based on a combination of CPU and memory utilization. [Learn more about serverless billing](#)

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).



The screenshot shows the 'Create SQL Database' wizard in the Microsoft Azure portal. The 'Additional settings' tab is selected. The 'Data source' section has 'Sample' selected under 'Use existing data \*'. The 'Database collation' is set to 'SQL\_Latin1\_General\_CP1\_CI\_AS'. A cost summary box on the right shows a General Purpose (GP\_S\_Gen5\_1) tier with a cost of 0.13 per GB and a max storage of 41.6 GB. The estimated storage cost is 5.26 USD per month, and the compute cost is 0.000174 USD per second. At the bottom, there are buttons for 'Review + create', '< Previous', and 'Next: Tags >'.

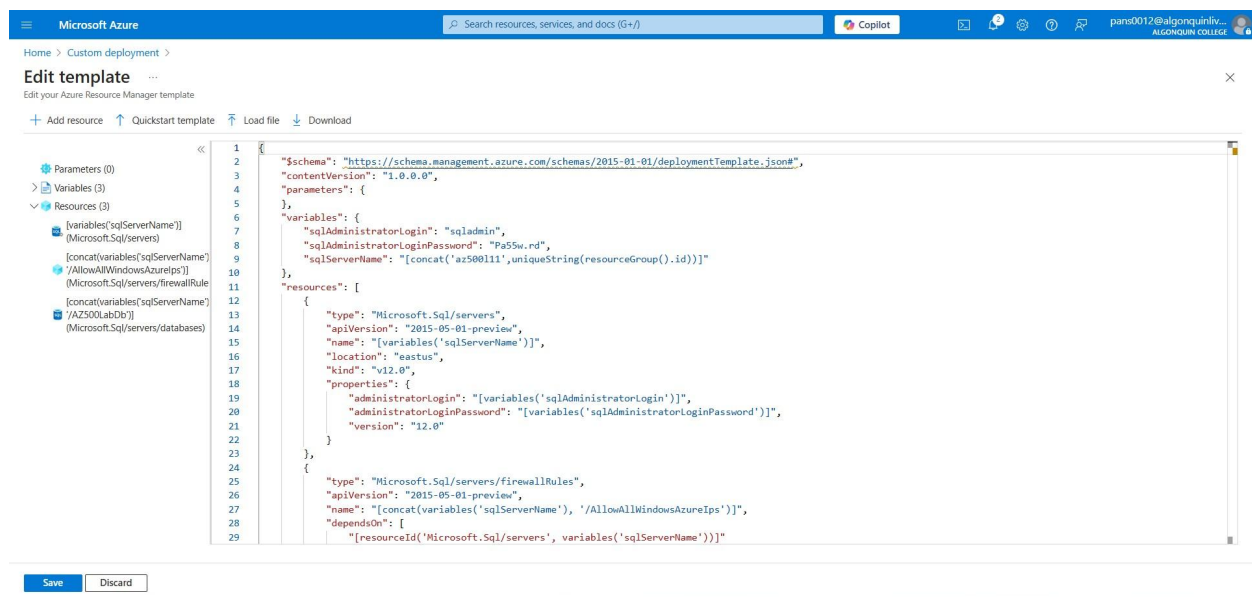
6. Select Review + Create, and then select Create to create your Azure SQL database.



The screenshot shows the 'Overview' page for the SQL database 'db8912 (db8912satyam/db8912)'. The 'Essentials' section displays key information: Resource group (CST8912demo), Status (Online), Location (Canada Central), Subscription ID (63593e07-b1bc-4b20-8c26-b71afac46e9f), and Tags (Add tags). The 'Getting started' section provides instructions on how to connect to the database, including options for 'Configure access', 'Connect to application', 'Start developing', and 'Mirror database in Fabric'. The 'Start working with your database' section offers a guide on how to connect to the database and start working with data.

## 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.js> on file and click **Open**.
4. On the **Edit template** blade, click **Save**.



The screenshot shows the 'Edit template' blade in the Azure portal. The left sidebar contains a tree view with 'Parameters (0)', 'Variables (3)', and 'Resources (3)'. The main area displays a JSON ARM template with the following content:

```

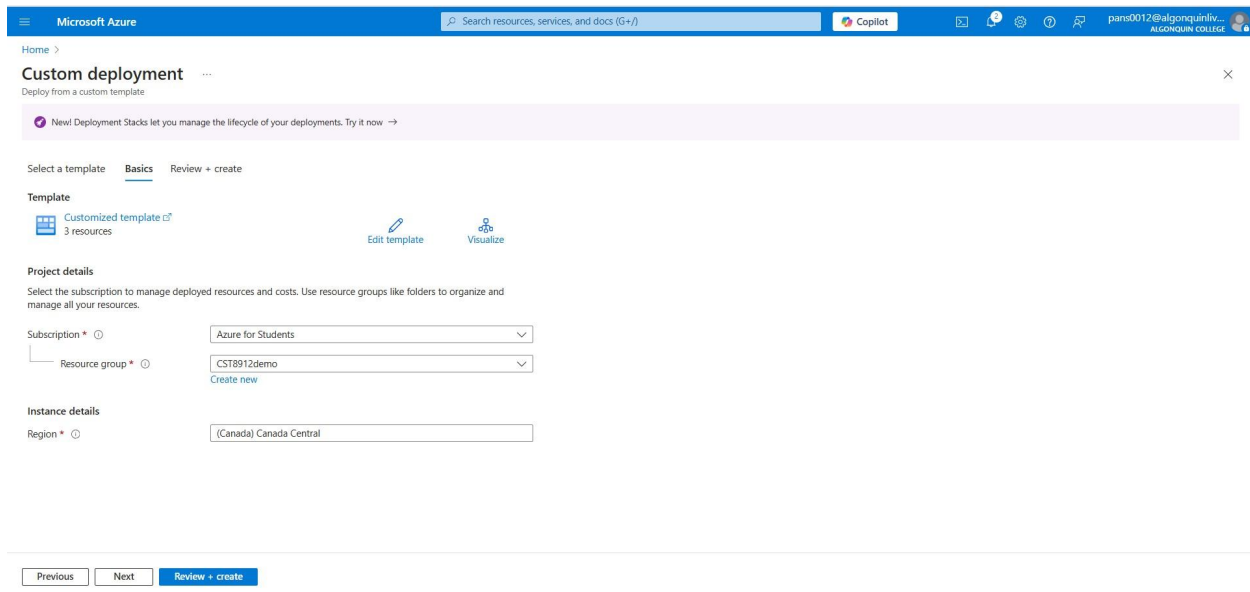
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {
5   },
6   "variables": {
7     "sqlAdministratorLogin": "sqladmin",
8     "sqlAdministratorLoginPassword": "Pa55w.rd",
9     "sqlServerName": "[concat('az500111',uniqueString(resourceGroup().id))]"
10  },
11  "resources": [
12    {
13      "type": "Microsoft.Sql/servers",
14      "apiVersion": "2015-05-01-preview",
15      "name": "[variables('sqlServerName')]",
16      "location": "eastus",
17      "kind": "v12.0",
18      "properties": {
19        "administratorLogin": "[variables('sqlAdministratorLogin')]",
20        "administratorLoginPassword": "[variables('sqlAdministratorLoginPassword')]",
21        "version": "12.0"
22      }
23    },
24    {
25      "type": "Microsoft.Sql/servers/firewallRules",
26      "apiVersion": "2015-05-01-preview",
27      "name": "[concat(variables('sqlServerName'), '/AllowAllWindowsAzureIps')]",
28      "dependsOn": [
29        "[resourceId('Microsoft.Sql/servers', variables('sqlServerName'))]"
30      ]
31    }
32  ]
33 }
```

At the bottom of the blade, there are 'Save' and 'Discard' buttons.

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

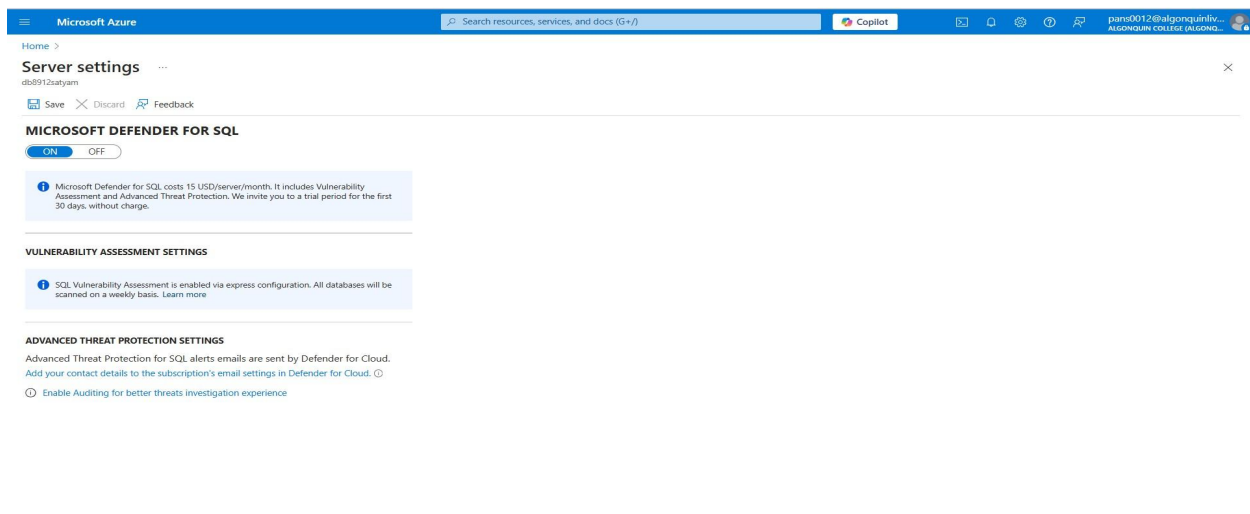
6. Click **Review + Create** and then click **Create**.



The screenshot shows the 'Custom deployment' page in the Microsoft Azure portal, specifically the 'Review + create' step. The page has a blue header with the Microsoft Azure logo and a search bar. Below the header, there's a 'Home' link and a 'Custom deployment' title. A purple banner at the top says 'New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now ->'. The main content area is divided into sections: 'Select a template' (with 'Basics' and 'Review + create' tabs), 'Template' (showing a 'Customized template' with 3 resources and links to 'Edit template' and 'Visualize'), 'Project details' (with instructions to select subscription and resource group), 'Subscription' (dropdown menu showing 'Azure for Students'), 'Resource group' (dropdown menu showing 'CST8912demo' with a 'Create new' link), and 'Instance details' (dropdown menu showing '(Canada) Canada Central'). At the bottom, there are three buttons: 'Previous', 'Next', and 'Review + create' (which is highlighted in blue).

## 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.
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)



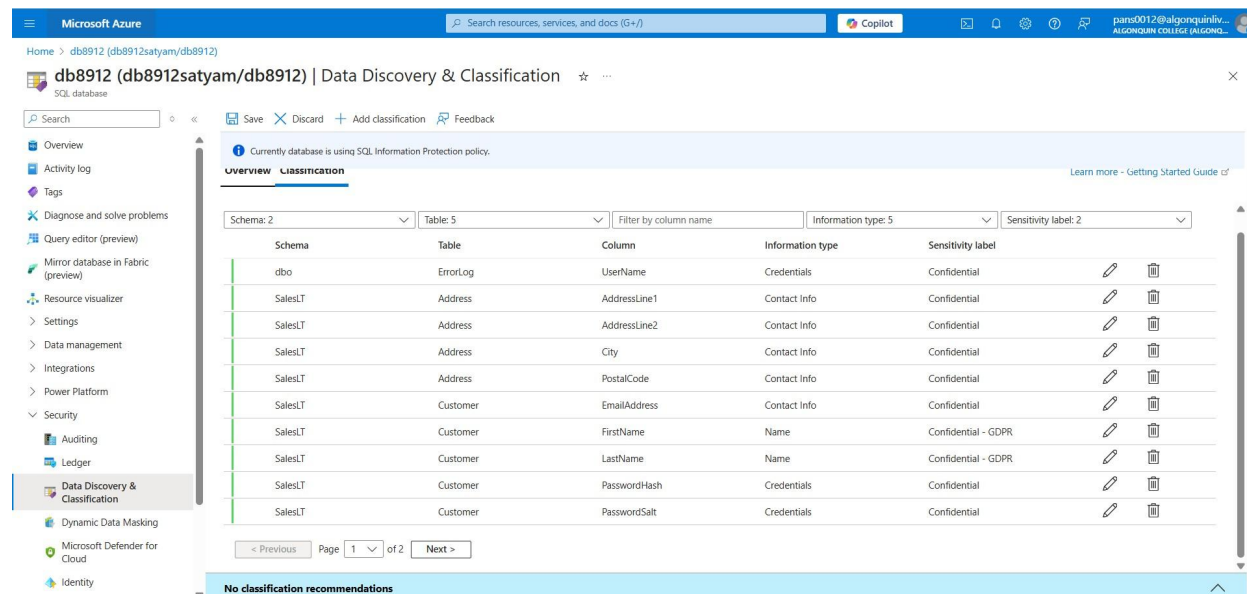
The screenshot shows the 'Server settings' page in the Microsoft Azure portal, specifically the 'Microsoft Defender for SQL' section. The page has a blue header with the Microsoft Azure logo and a search bar. Below the header, there's a 'Home' link and a 'Server settings' title. A purple banner at the top says 'New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now ->'. The main content area is divided into sections: 'Microsoft Defender for SQL' (with a toggle switch set to 'ON'), 'Vulnerability Assessment Settings' (with a link to 'SQL Vulnerability Assessment'), and 'Advanced Threat Protection Settings' (with a link to 'Enable Auditing for better threats investigation experience').

3. On the Server Settings blade, review the information about pricing and the trial period, VULNERABILITY ASSESSMENT SETTINGS and ADVANCED THREAT PROTECTION SETTINGS.
4. Back to Microsoft Defender for Cloud blade, review Recommendations and Security alerts.

### 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.
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.
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

Home > db8912 (db8912satyam/db8912)

db8912 (db8912satyam/db8912) | Data Discovery & Classification

SQL database

Search

Save Discard Add classification Feedback

Currently database is using SQL Information Protection policy.

Overview Classification

Schema: 2 Table: 5 Filter by column name Information type: 5 Sensitivity label: 2

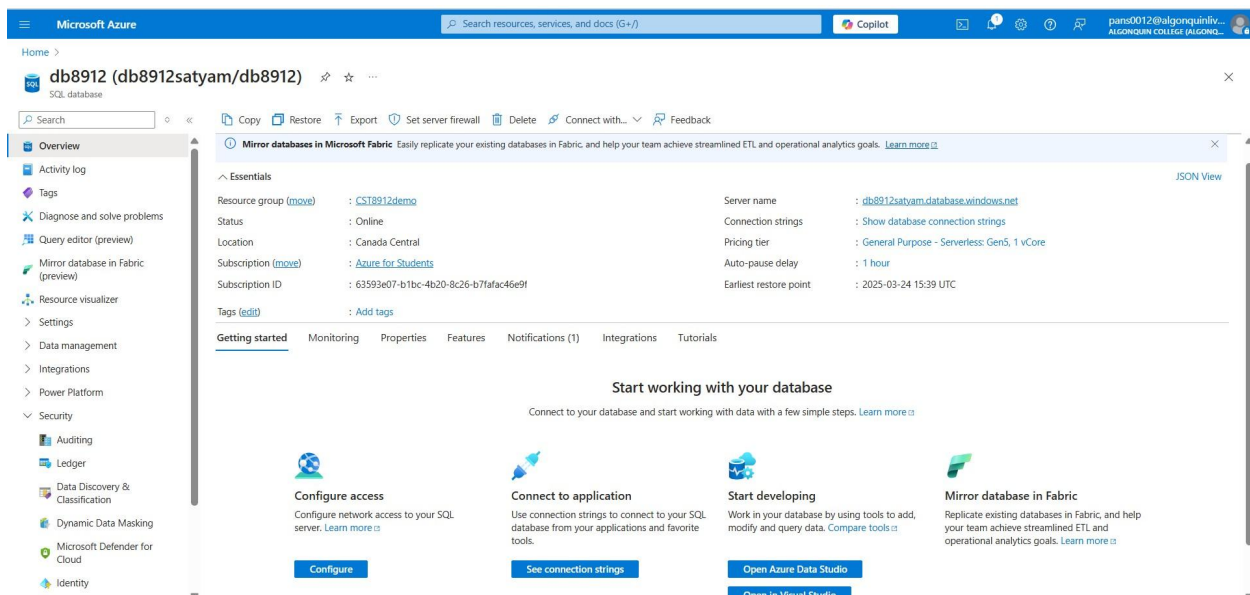
Schema	Table	Column	Information type	Sensitivity label
dbo	ErrorLog	UserName	Credentials	Confidential
SalesLT	Address	AddressLine1	Contact Info	Confidential
SalesLT	Address	AddressLine2	Contact Info	Confidential
SalesLT	Address	City	Contact Info	Confidential
SalesLT	Address	PostalCode	Contact Info	Confidential
SalesLT	Customer	EmailAddress	Contact Info	Confidential
SalesLT	Customer	FirstName	Name	Confidential - GDPR
SalesLT	Customer	LastName	Name	Confidential - GDPR
SalesLT	Customer	PasswordHash	Credentials	Confidential
SalesLT	Customer	PasswordSalt	Credentials	Confidential

< Previous Page 1 of 2 Next >

No classification recommendations



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



The screenshot shows the Microsoft Azure portal interface for an SQL database. The top navigation bar includes the Microsoft Azure logo, a search bar, and a Copilot button. The main content area is titled 'db8912 (db8912satyam/db8912)' and shows the 'Overview' tab selected. The left sidebar contains a list of navigation options including Activity log, Tags, Diagnose and solve problems, Query editor (preview), Mirror database in Fabric (preview), Resource visualizer, Settings, Data management, Integrations, Power Platform, Security, Auditing, Ledger, Data Discovery & Classification, Dynamic Data Masking, Microsoft Defender for Cloud, and Identity. The main content area displays the 'Essentials' section with details about the database, including Resource group (CS18912demo), Status (Online), Location (Canada Central), Subscription (Azure for Students), and Subscription ID (63593e07-b1bc-4b20-8c26-b71afac46e9f). Below this, there are tabs for Getting started, Monitoring, Properties, Features, Notifications (1), Integrations, and Tutorials. The 'Getting started' tab is active, showing a section titled 'Start working with your database' with four main actions: Configure access, Connect to application, Start developing, and Mirror database in Fabric. Each action has a brief description and a 'Learn more' link.

## 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)

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > SQL servers > db8912satyam

### Create storage account

Name \*

satyamlabstorage

Account kind

Storage (general purpose v1)

Performance

Standard Premium

Replication

Locally-redundant storage (LRS)

Minimum TLS version

Version 1.2

OK

5. Choose your Subscription from the dropdown list.
6. Click Storage account and choose Create new.
7. Back on the Auditing blade, under Advanced properties set Retention (days) to 5.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > SQL servers > db8912satyam

### SQL servers

Algonquin College (AlgonquinLivecom.onmicrosoft...)

+ Create Manage view

Filter for any field...

Name ↑

db8912satyam

db8912satyam | Auditing

Overview

Activity log

Access control (IAM)

Tags

Quick start

Diagnose and solve problems

Resource visualizer

Settings

Data management

Security

Networking

Microsoft Defender for Cloud

Transparent data encryption

Identity

Auditing

Intelligent performance

Monitoring

Automation

Help

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 \*

satyamlabstorage

Create new

Storage Authentication Type

Managed Identity Storage Access Keys

Advanced properties

Retention (Days)

5

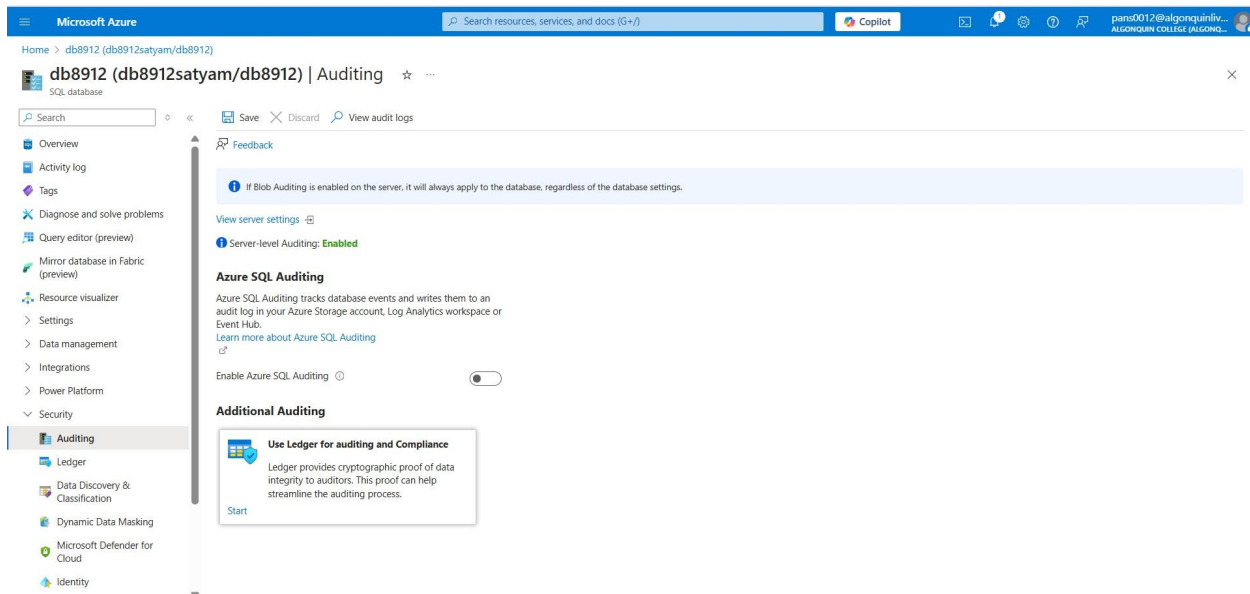
Storage access key

Primary Secondary

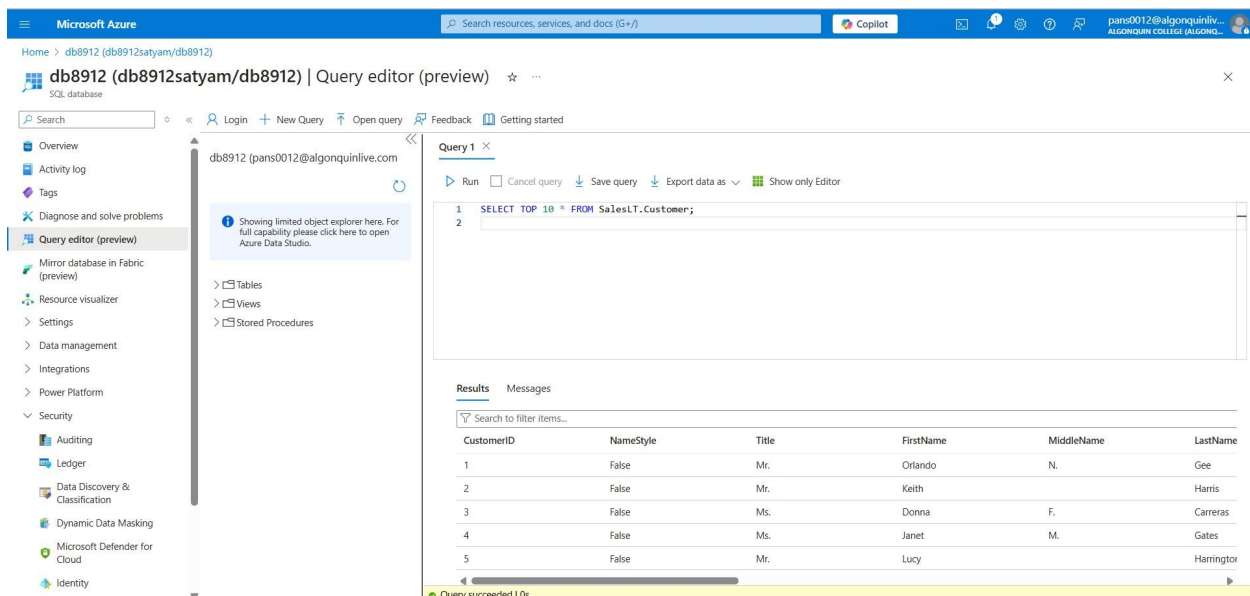
Page 1 of 1

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.



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



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

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

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 17:47:21 UTC.

Run in Query Editor

Event time (UTC)	Principal name	Event type	Action status
3/24/2025 5:46:45 PM	db8912satyam	DATABASE AUTHENTICATION SUCCEEDED	Succeeded
3/24/2025 5:46:45 PM	db8912satyam	BATCH COMPLETED	Succeeded
3/24/2025 5:46:07 PM	db8912satyam	BATCH COMPLETED	Succeeded
3/24/2025 5:46:07 PM	db8912satyam	DATABASE AUTHENTICATION SUCCEEDED	Succeeded
3/24/2025 5:44:17 PM	db8912satyam	BATCH COMPLETED	Succeeded
3/24/2025 5:44:17 PM	db8912satyam	DATABASE AUTHENTICATION SUCCEEDED	Succeeded
3/24/2025 5:44:16 PM	db8912satyam	DATABASE AUTHENTICATION SUCCEEDED	Succeeded
3/24/2025 5:44:16 PM	db8912satyam	BATCH COMPLETED	Succeeded

[Load more](#)

[https://portal.azure.com/?Microsoft\\_Azure\\_Education\\_correlationId=15c7351f-04a5-4d14-afc...](https://portal.azure.com/?Microsoft_Azure_Education_correlationId=15c7351f-04a5-4d14-afc...)

## Task 5: Clean up resources created during this lab

**Delete a resource group**

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

**Resource group to be deleted**

CST8912demo

**Dependent resources to be deleted (4)**  
All dependent resources, including hidden types, are shown

Name	Resource type
db8912 (db8912satyam/db8912)	SQL database
db8912satyam	
master (db8912)	
satyamlabstorage	

**Delete confirmation**

Deleting this resource group and its dependent resources is a permanent action and cannot be undone.

[Delete](#) [Go back](#)

Enter resource group name to confirm deletion \*

CST8912demo

[Delete](#) [Cancel](#)

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

para0012@algonquiniv...  
ALGONQUIN COLLEGE (ALGONO...

Home > Resource groups >

## Resource groups

Algonquin College (AlgonquinLivecom.onmicrosof...

+ Create

...

Group by none

❗ You are viewing a new version of browse experience. Some features may be missing. Click here to access the old experience.

☐ Name ↑

☐ CST8912

☐ CST8912demo

☐ DefaultResourceGroup-CCAN

☐ DefaultResourceGroup-EUS

☐ NetworkWatcherRG

Showing 1 - 5 of 5. Display count: auto

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Deployments

Security

Deployment stacks

Policies

Properties

Locks

Cost Management

Monitoring

Insights (preview)

Alerts

Metrics

Diagnostic settings

Logs

CST8912

Resource group

Search

...

+ Create

Manage view

Delete resource group

Refresh

Export

Essentials

Subscription (move) : Azure for Students

Subscription ID : 63593e07-b1bc-4b20-8c26-b7afac46e9f

Tags (edit) : Add tags

Resources

Recommendations (1)

Filter for any field...

Type equals all

Location equals all

Showing 0 to 0 of 0 records.

Show hidden types

Name ↑

No resources

Try changing o

+ Create resou

Delete a resource group

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

Resource group to be deleted

CST8912

Delete confirmation

Deleting this resource group and its dependent resources is a permanent action and cannot be undone.

Delete

Go back

Enter resource group name to confirm deletion \*

CST8912

Delete

Cancel