**CST8912 – Cloud Solution Architecture**

**Graded Lab Activity #9**

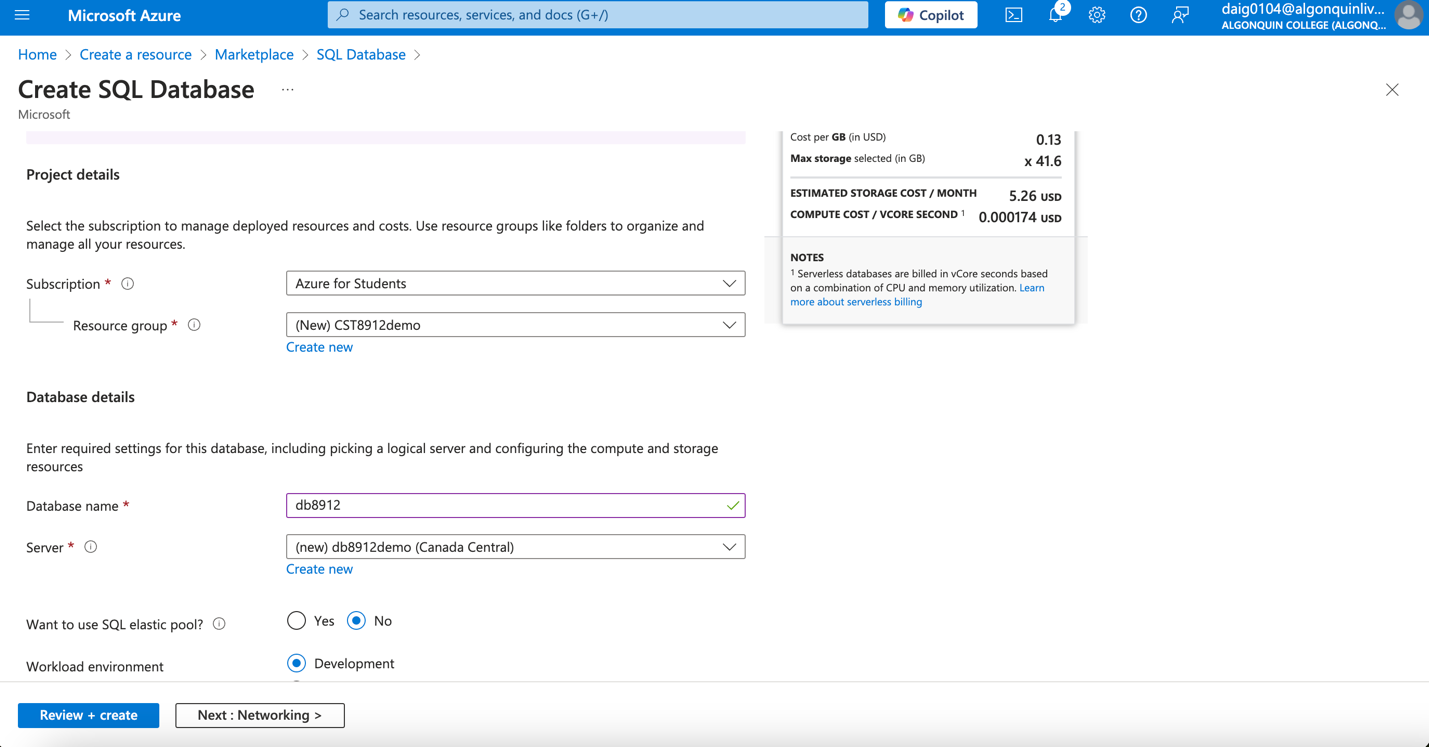
# Introduction:

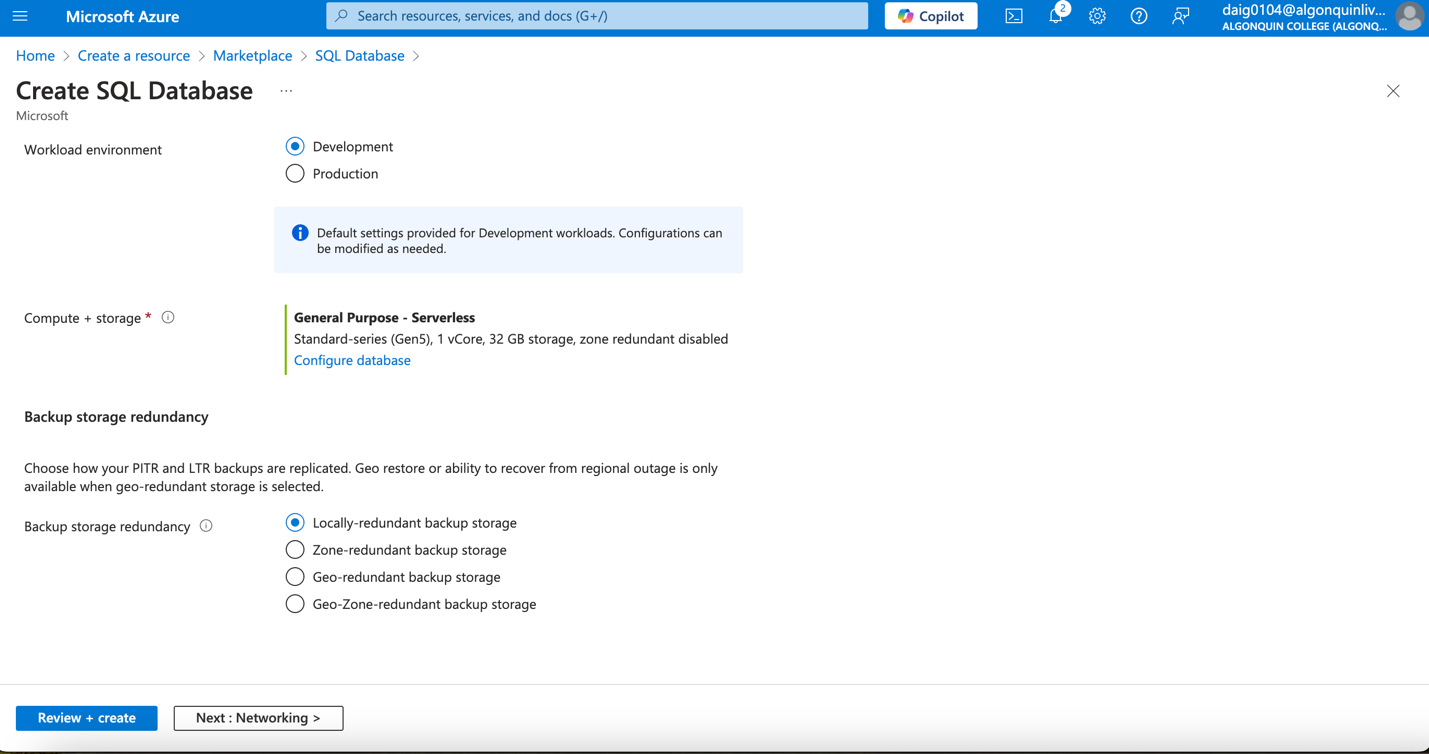
In this lab, we will review security services azure offers to protect data within an SQL database, such as Microsoft Defender, Auditing & classification as well as firewall rules.

# Screenshots:

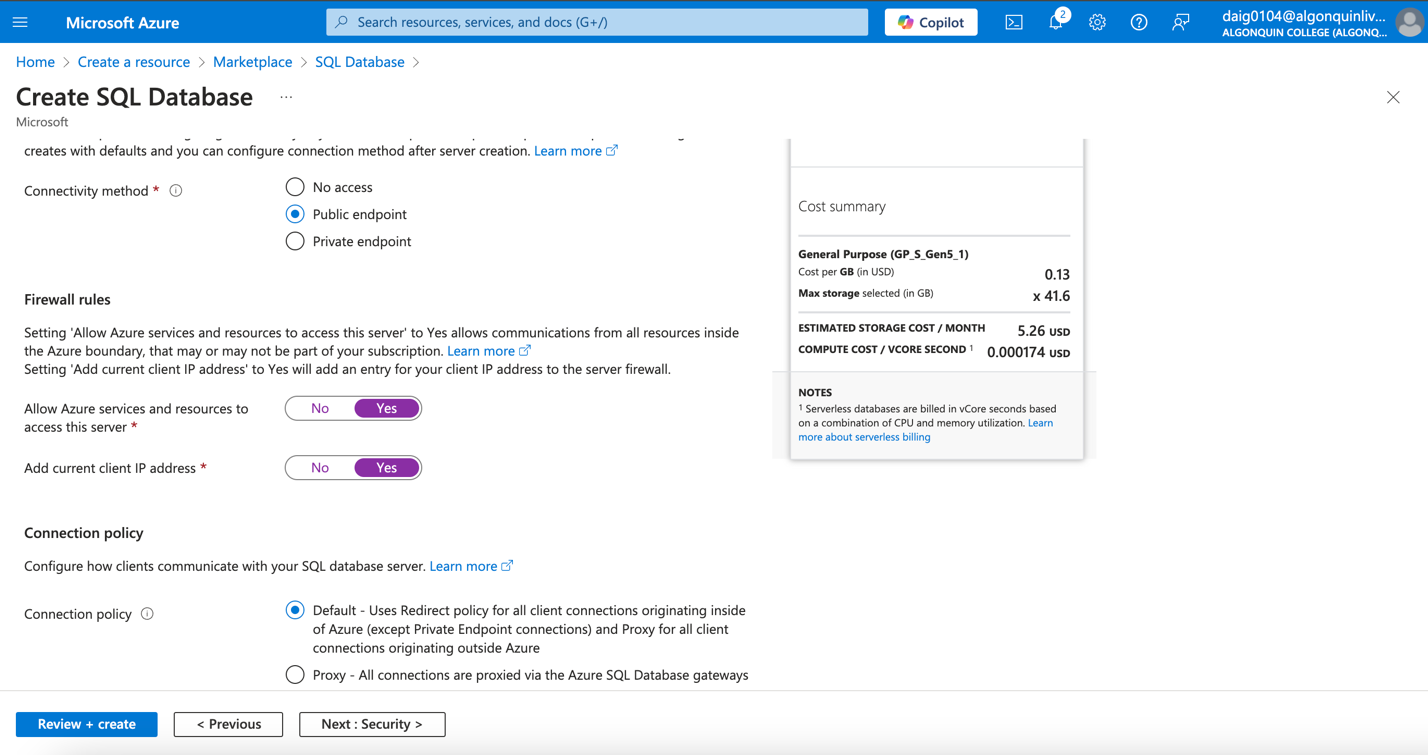
Task 1: Deploy an Azure SQL Database  
Method1:

### Below is Method 1, picking CST8912demo as the resource group and database name. In the end, I opted for Method two due to not being able to specify single database deployment.

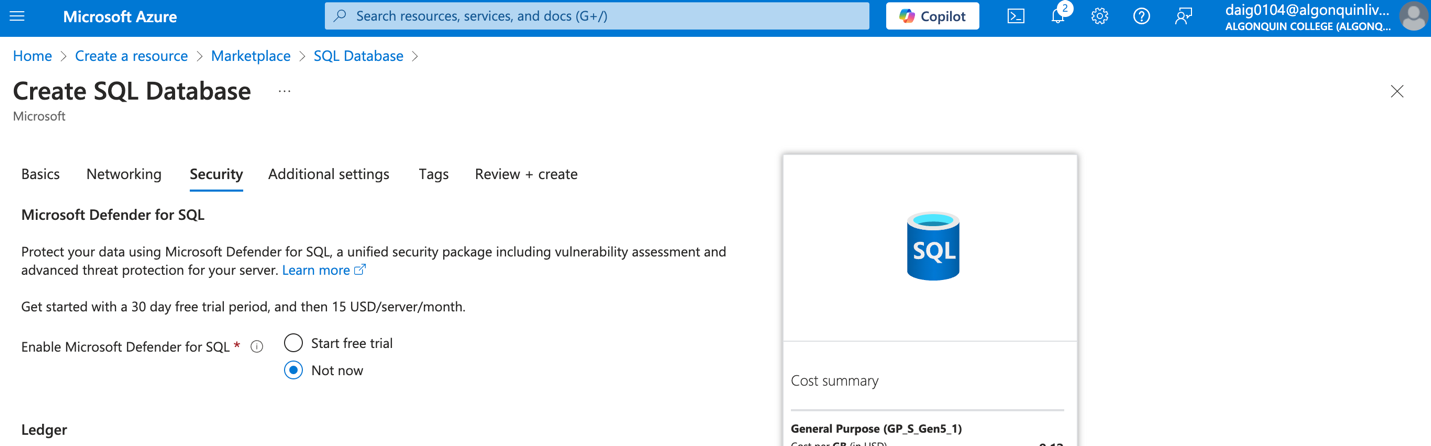




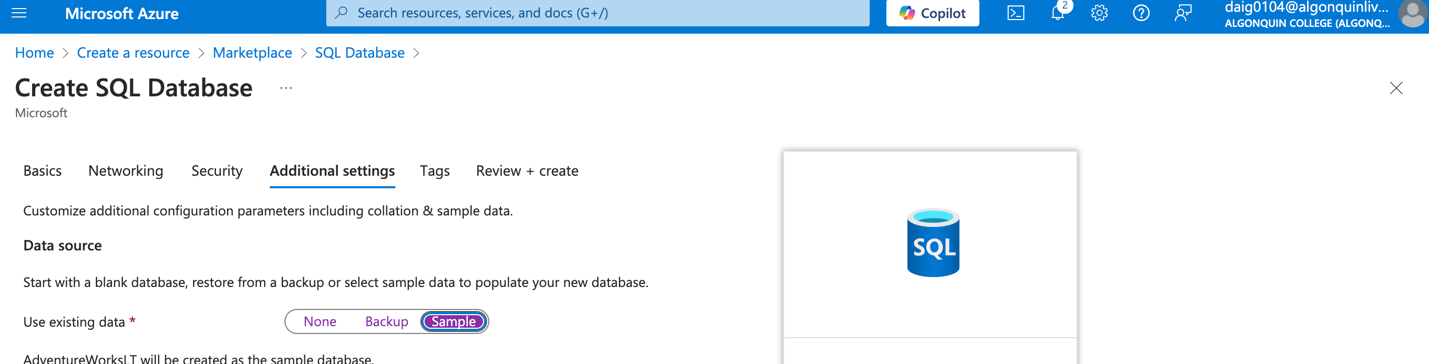
### Selecting yes for both options

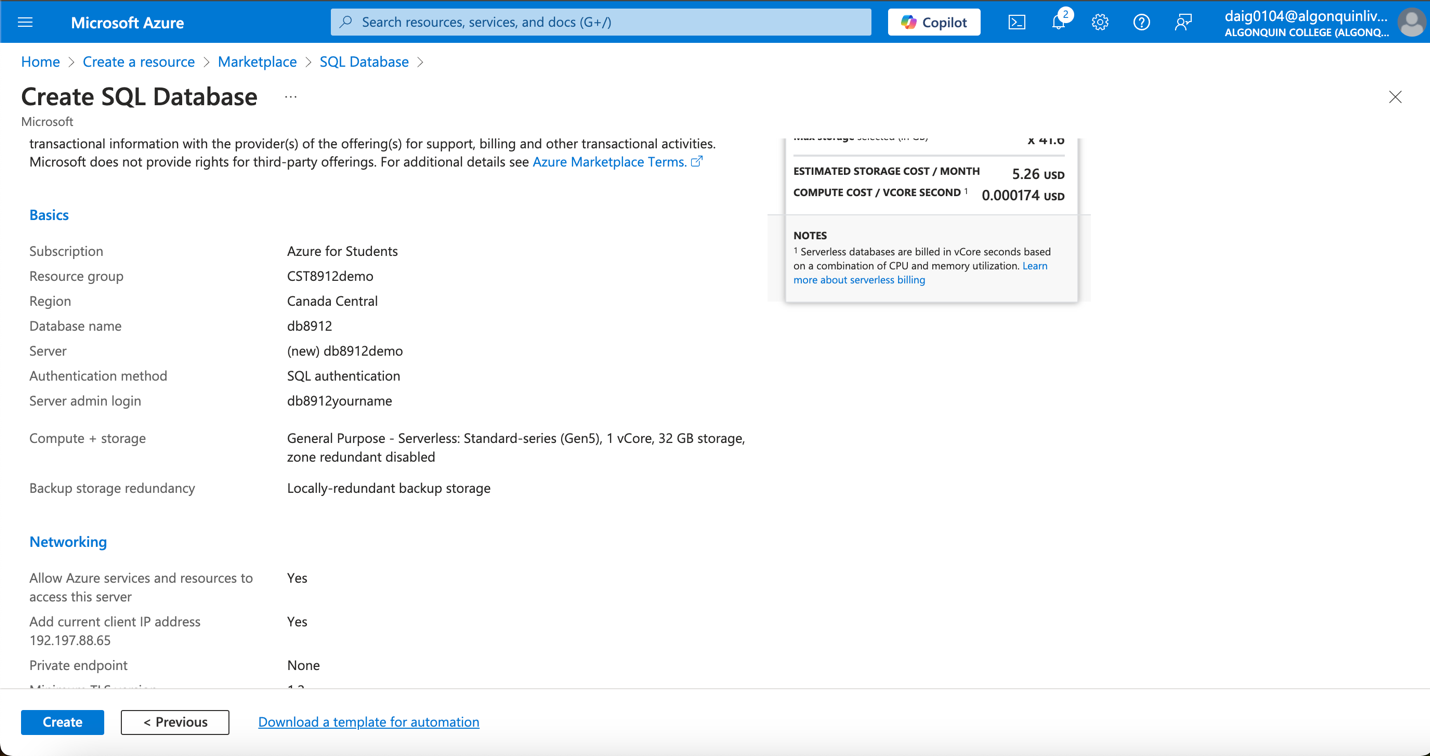


Defender to Not Now.



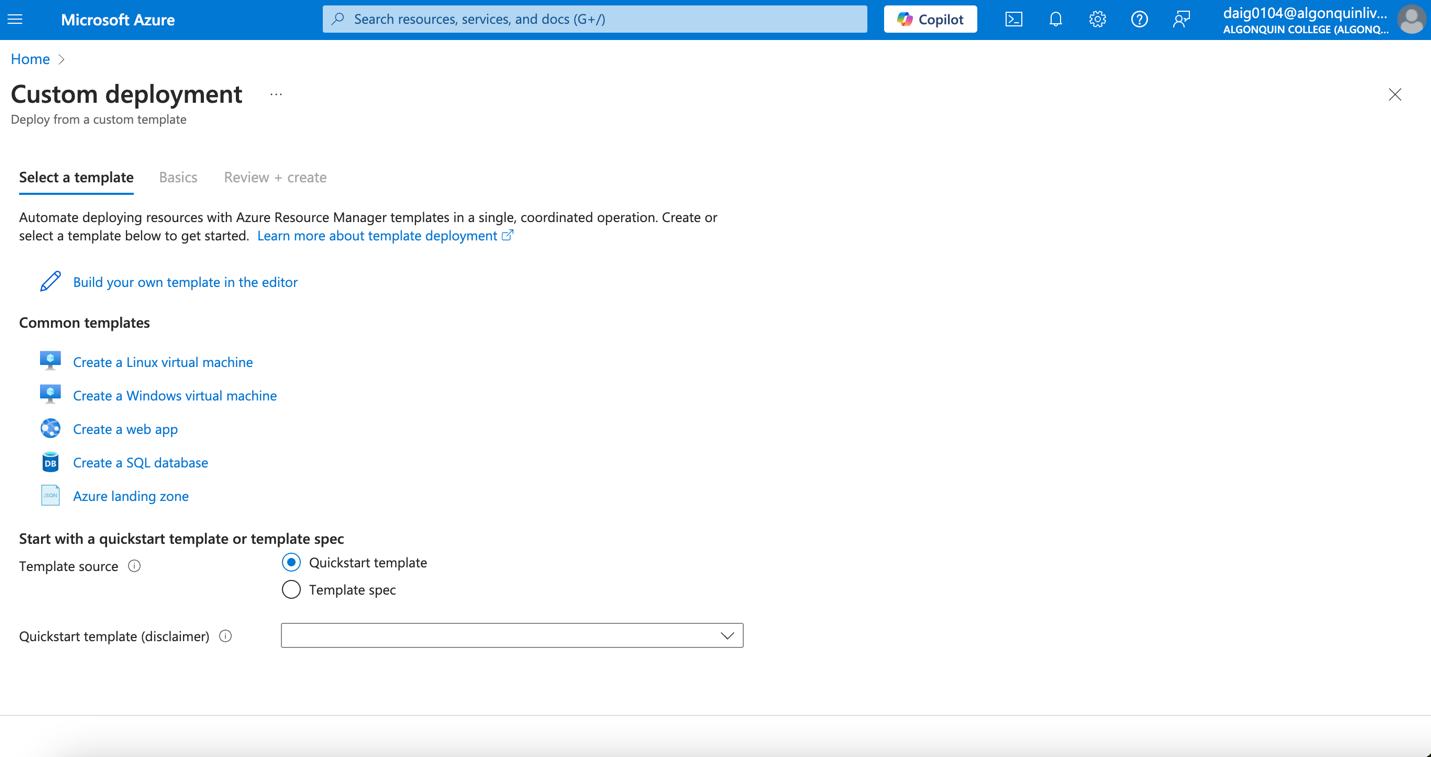
Use Existing Sample Set

Creating Database.

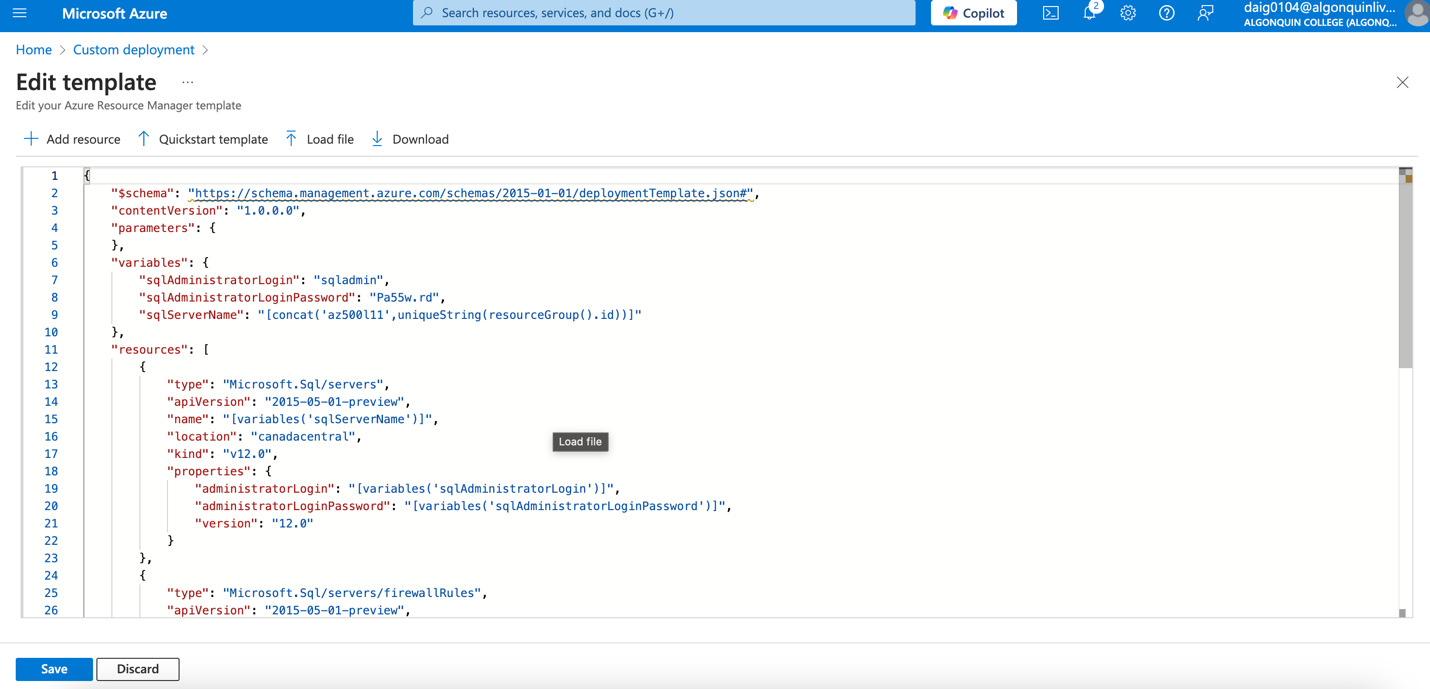


## Method 2:

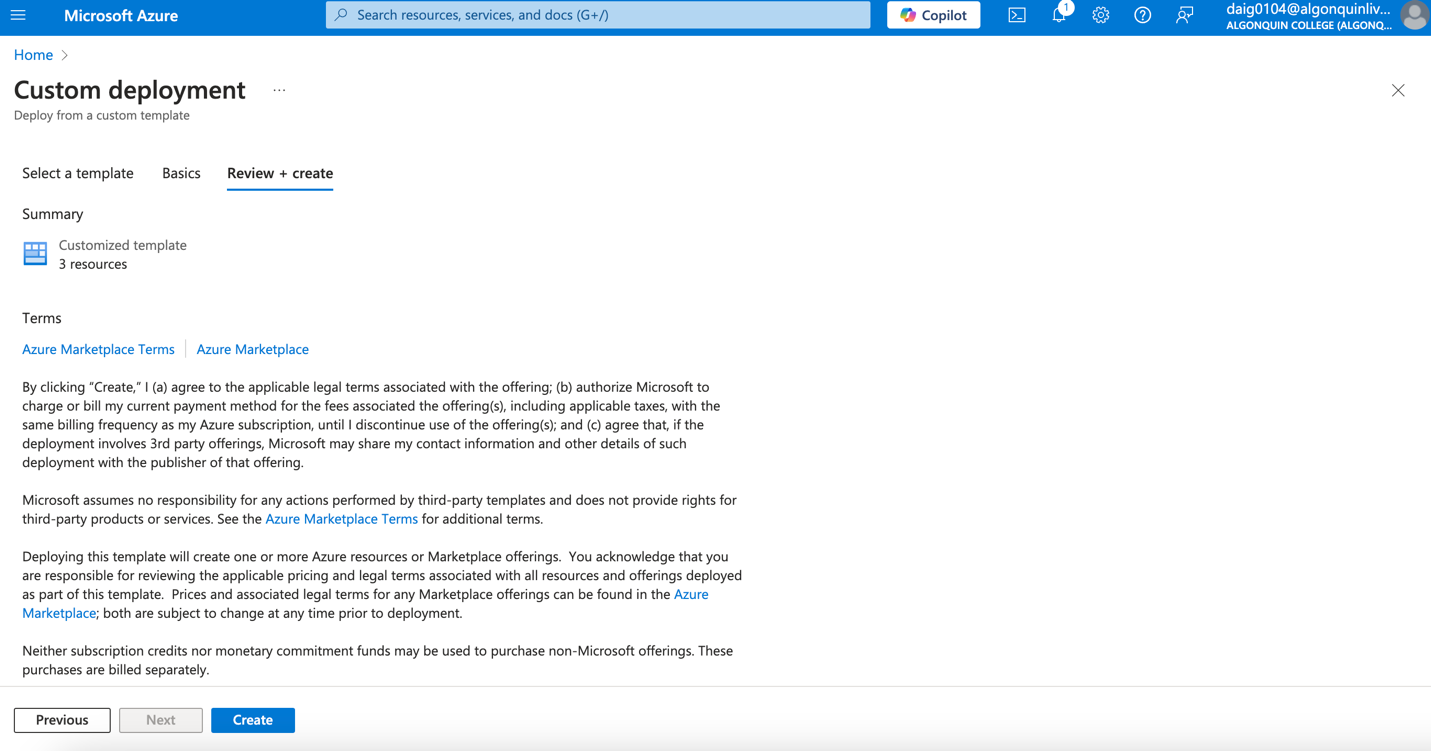
**I had chosen method two: uploading the JSON file below and saving it. There had to be a change within the JSON it originally had “eastus” as the region, but it has been changed to “centralcanada”**



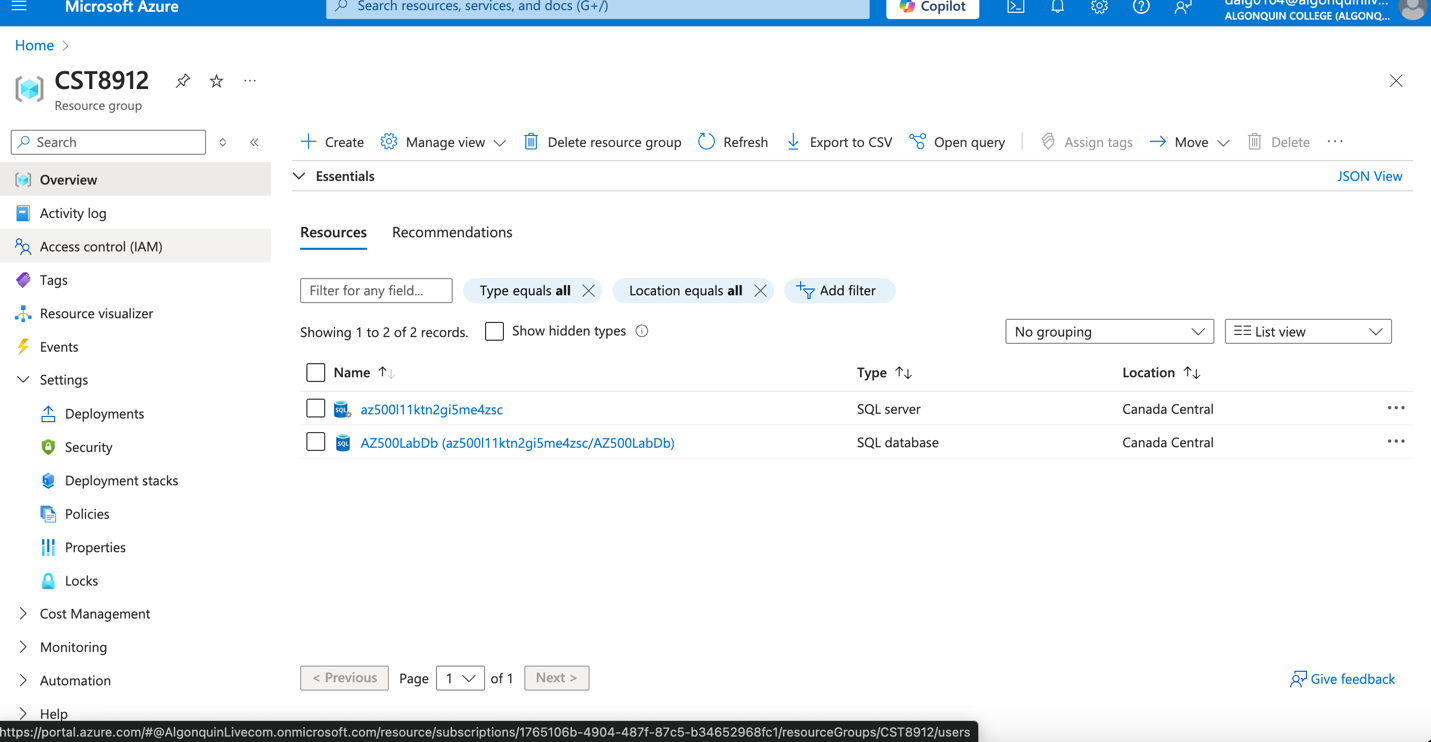
The JSON file:



Creating the deployment

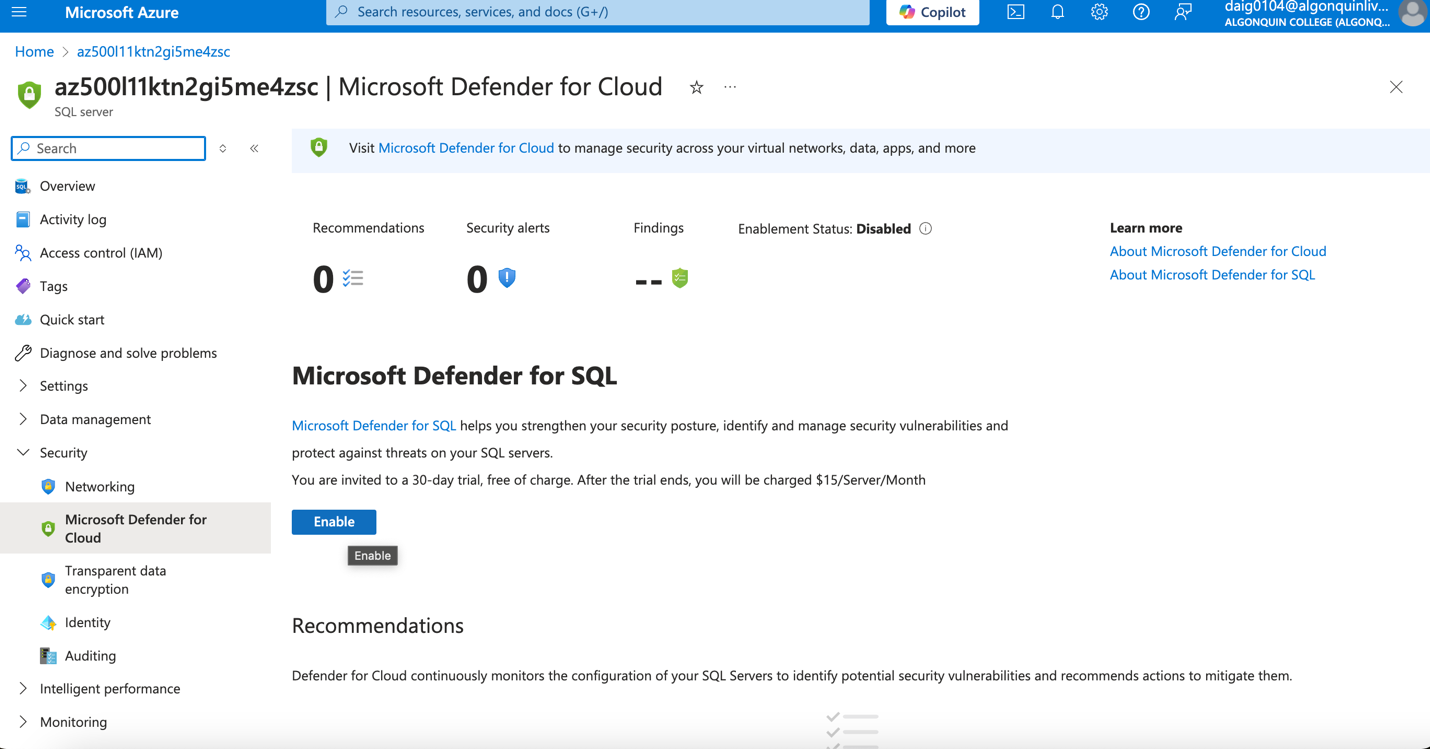


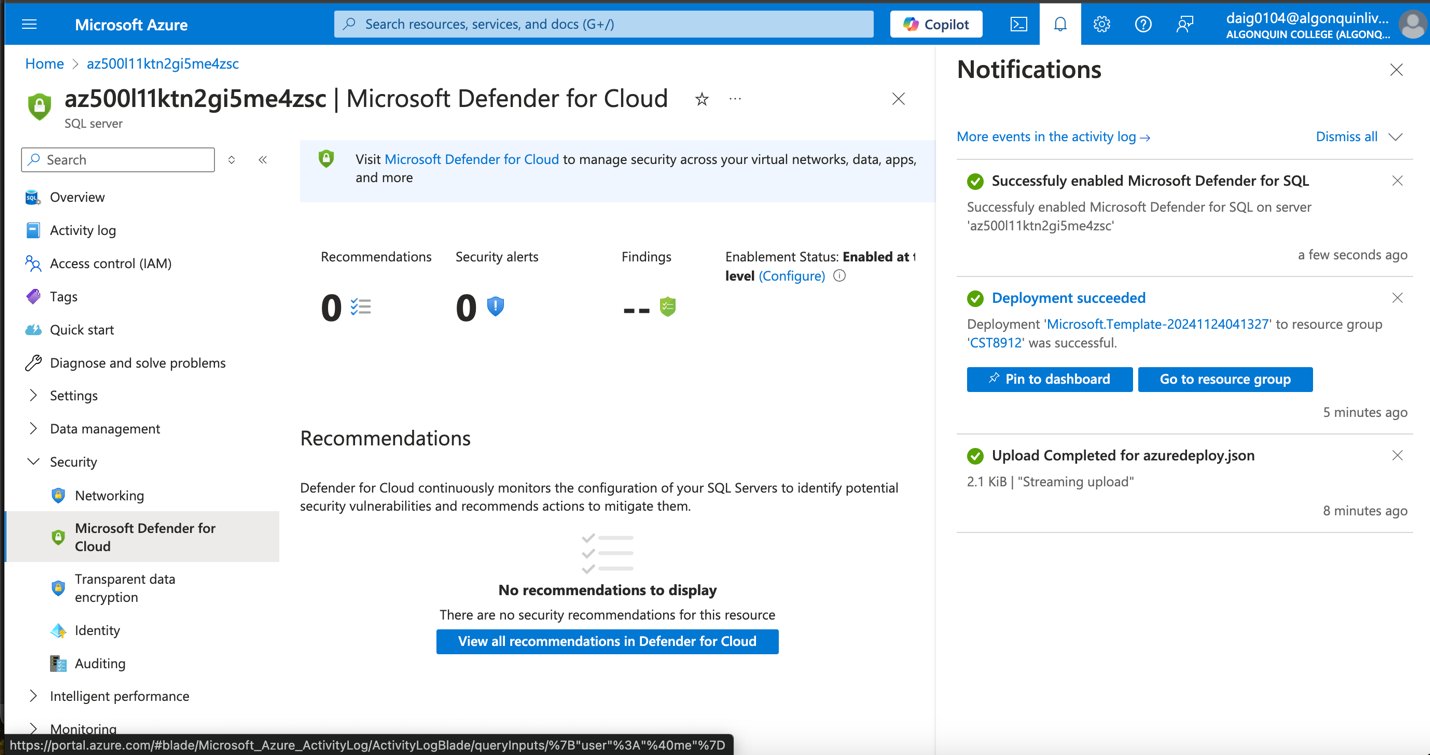
Result:



# Task 2: Configure Advanced Data Protection

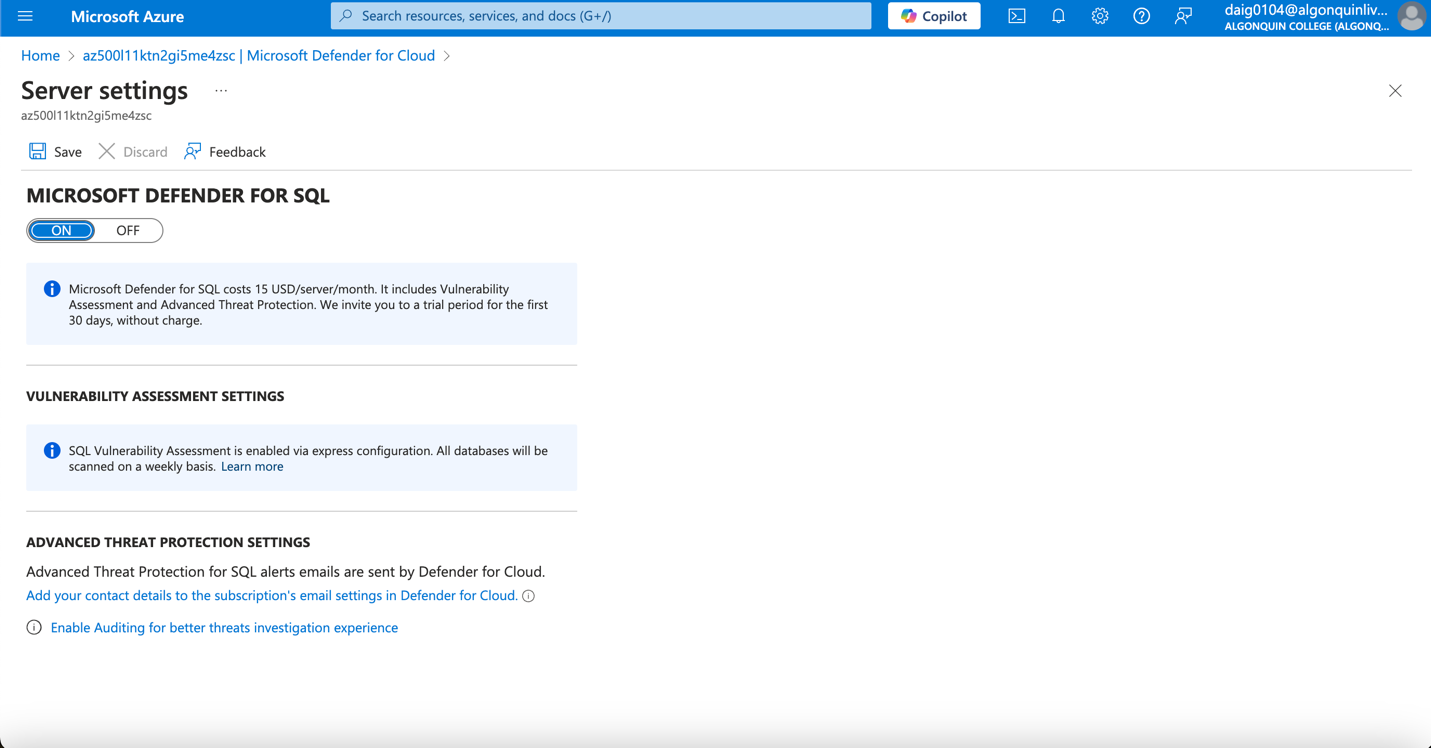
### Enabling Microsoft Defender for the SQL Server.



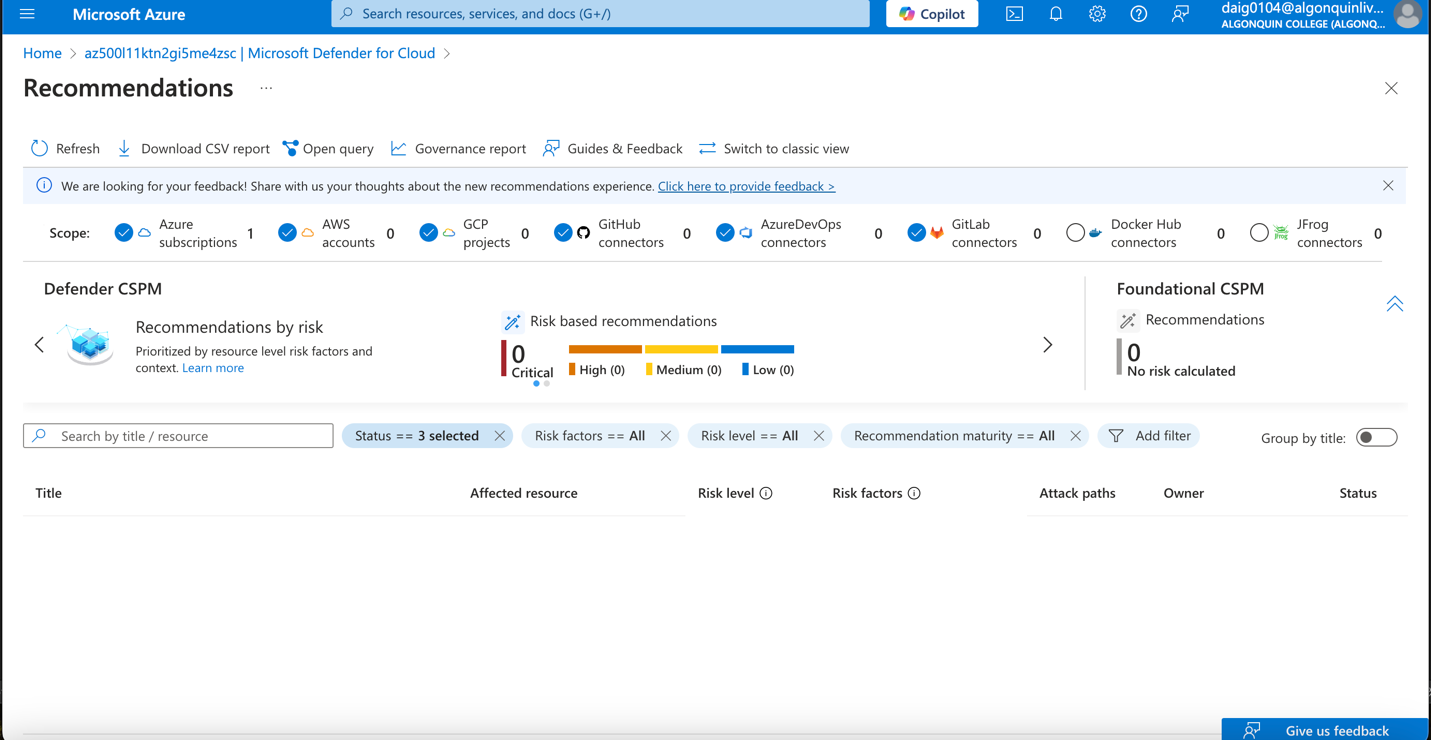


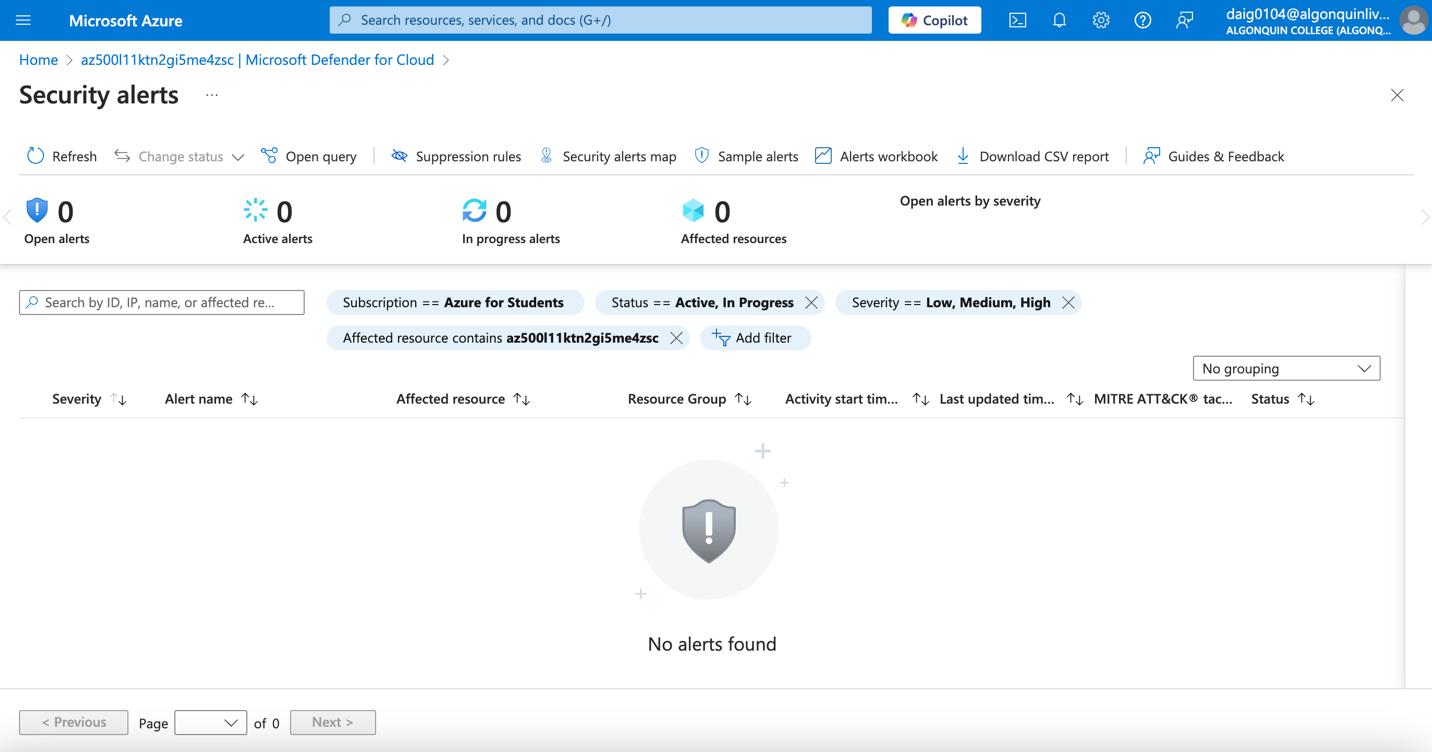
### Clicking Configure in (Enablement Status: Enabled at the server level).

### On the Server Settings blade, review pricing and the trial period, VULNERABILITY ASSESSMENT SETTINGS and ADVANCED THREAT PROTECTION SETTINGS. (The cost of Microsoft defender is 15 UST/server/month)



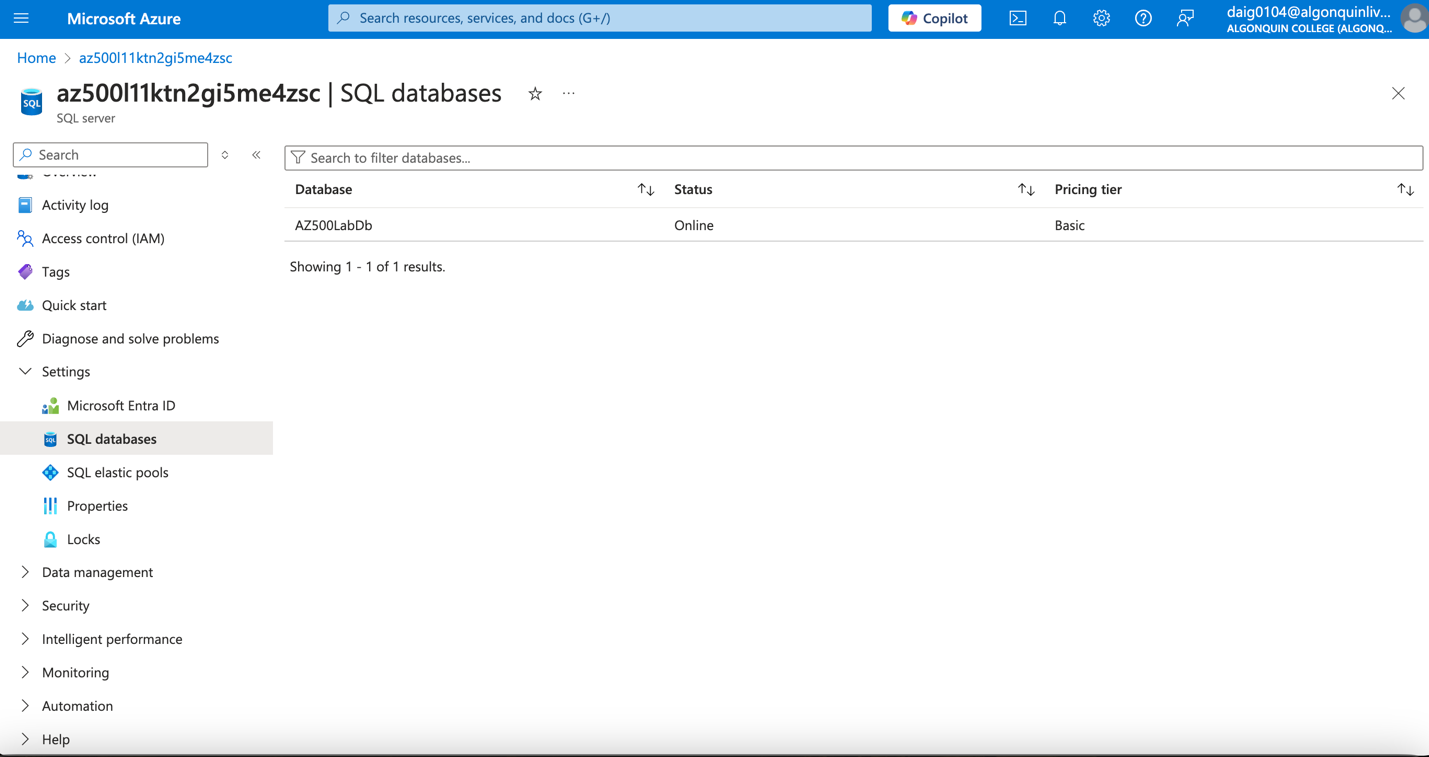
### Back to Microsoft Defender for Cloud blade, review Recommendations and security alerts.



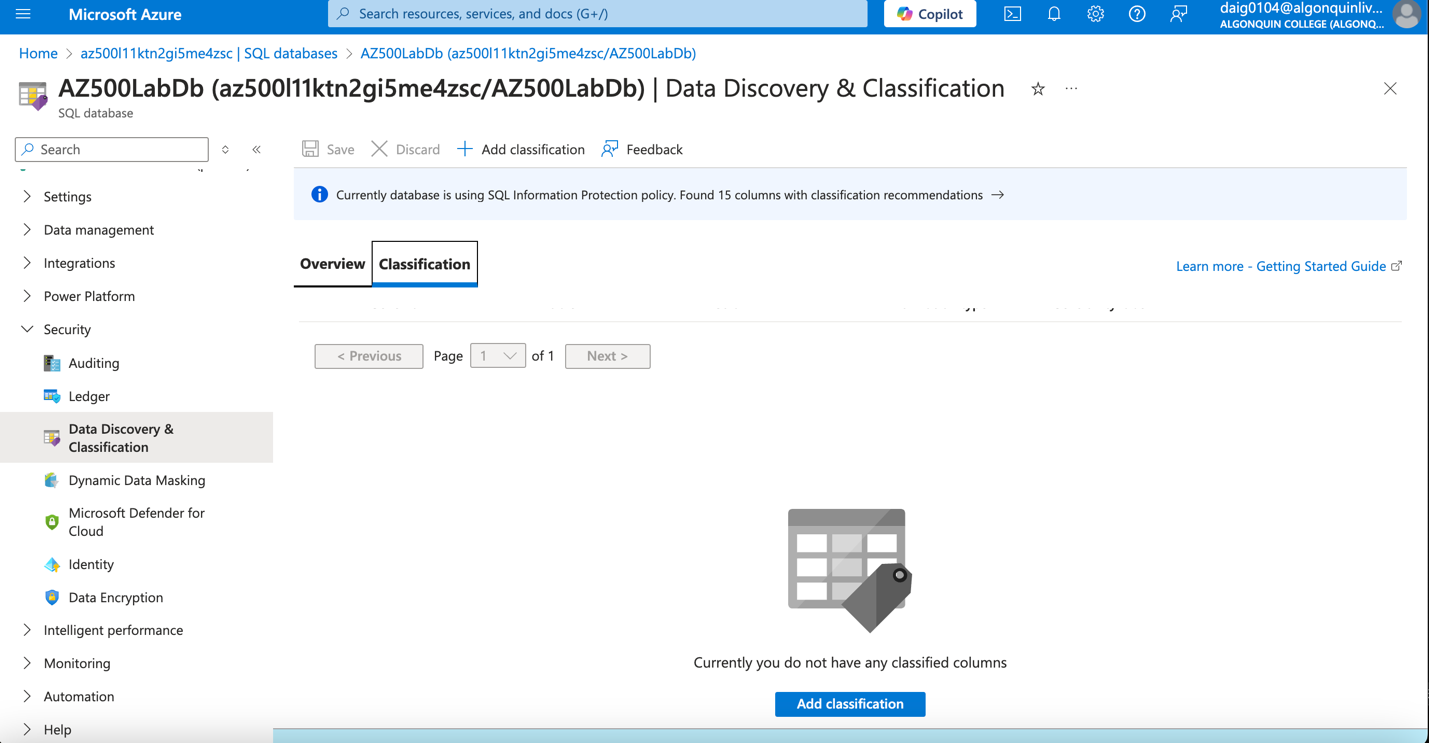


Task 3: Configure Data Classification

### On the SQL server blade, in the Settings section, clicking SQL Databases.

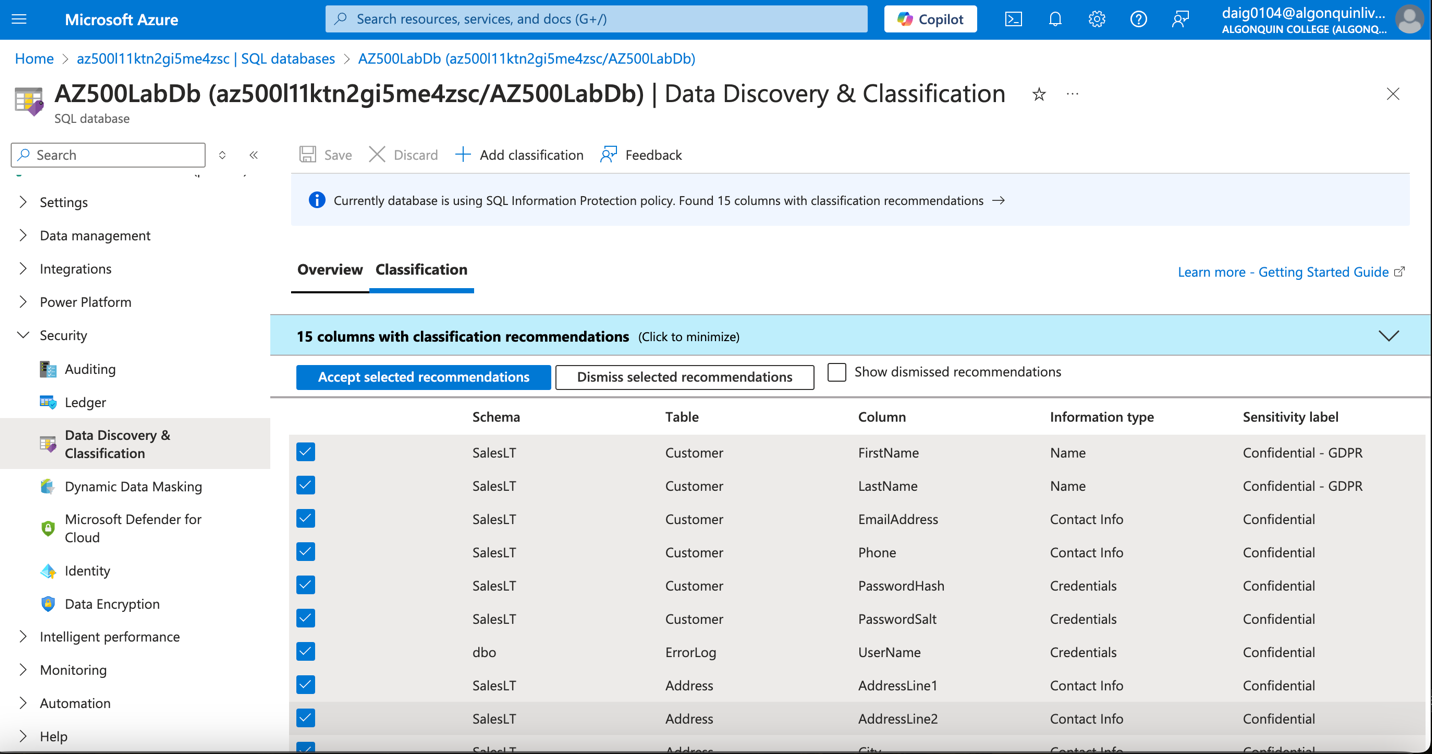


### On the SQL database blade, in the Security section, clicking Data Discovery & Classification.

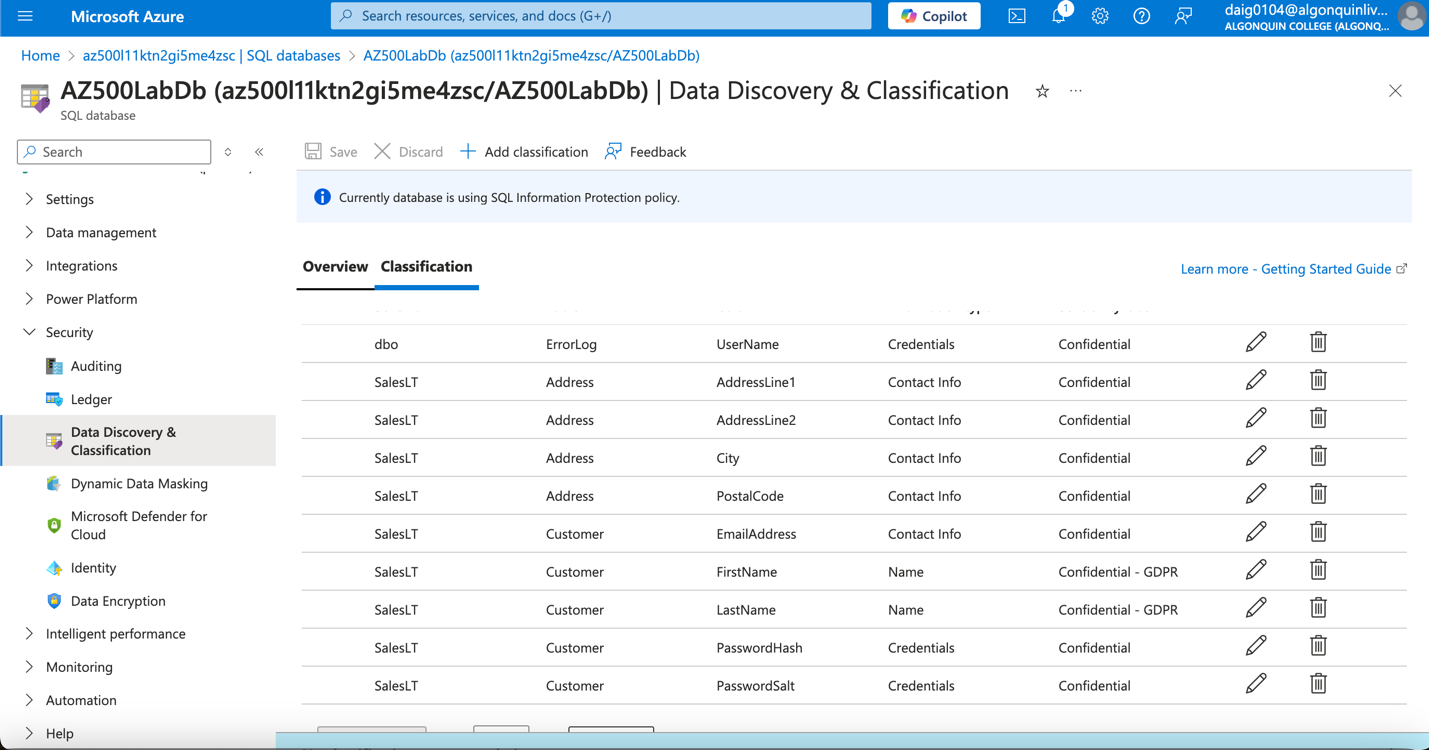


### On the Data Discovery & Classification blade, the Classification tab. Reviewing the columns and recommended sensitivity labels. (mostly confidential)

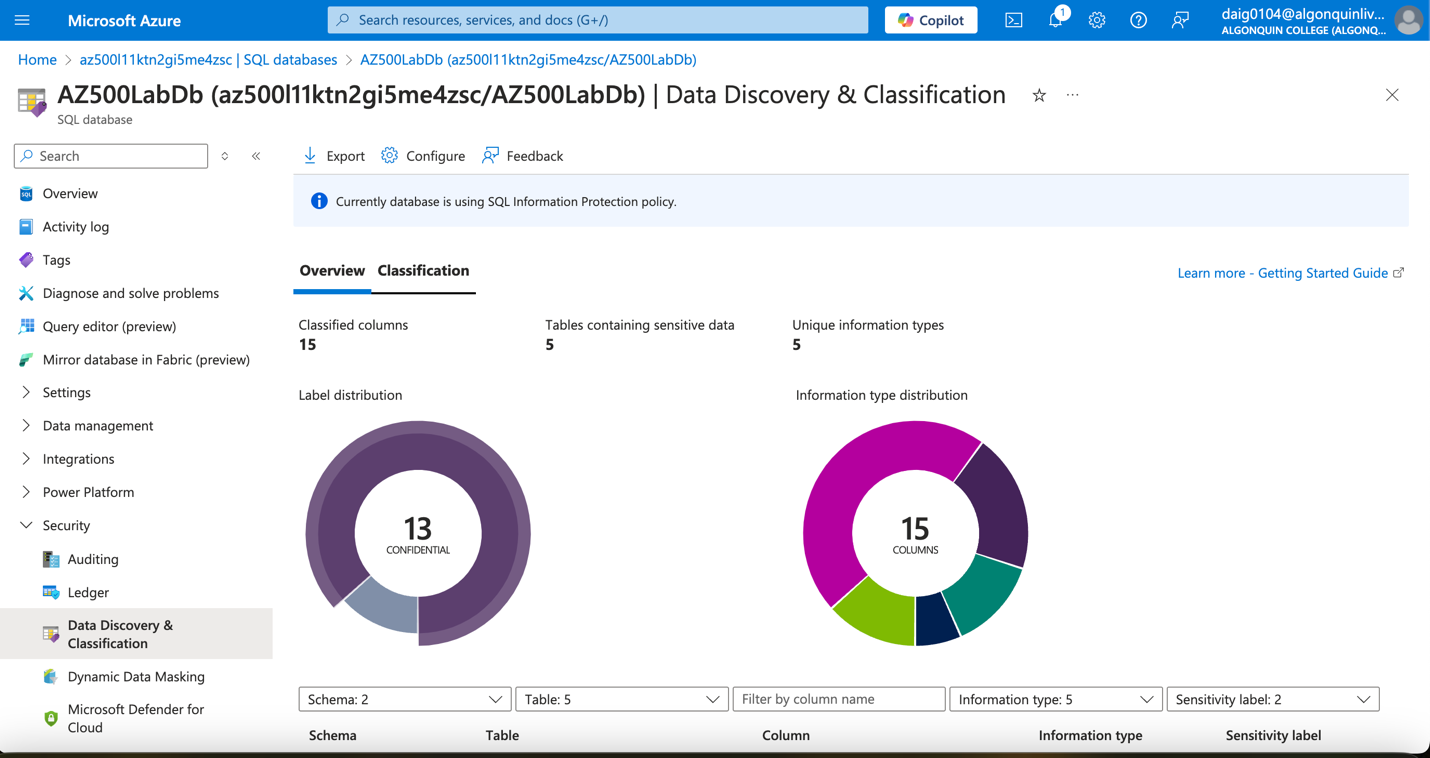
### Selected all checkboxes



Saving and Accepting

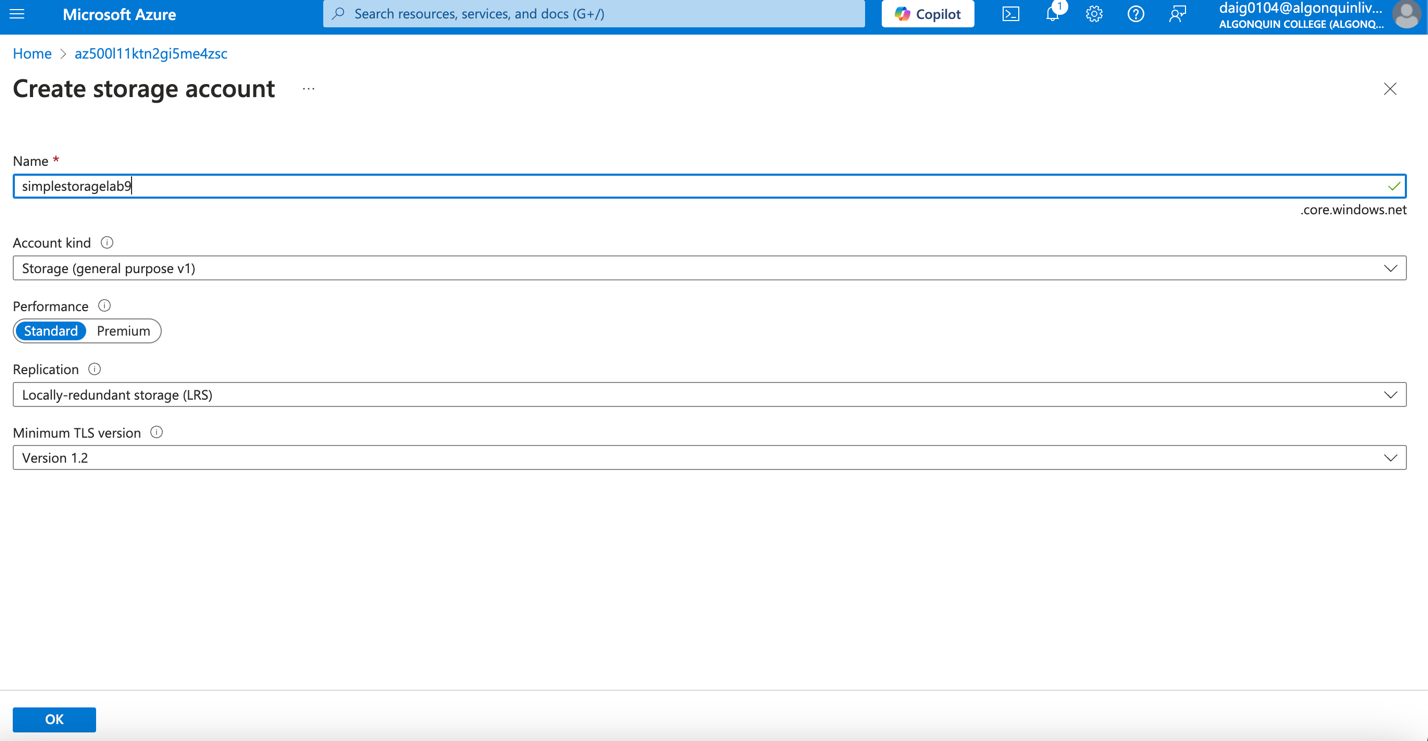


### On the Data Discovery & Classification blade Overview tab, it has been updated to reflect the latest classification information. Of 15 columns, 13 confidential.

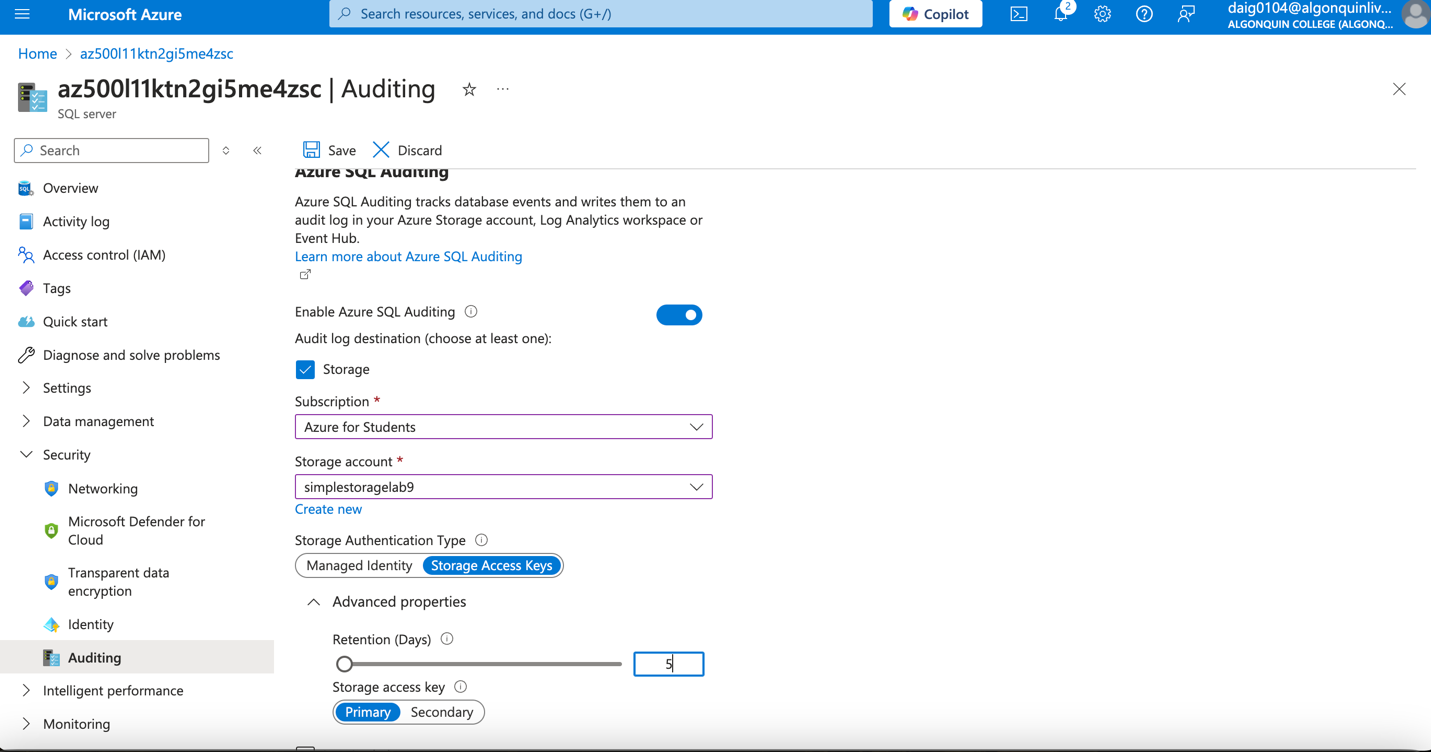


# Task 4: Configure Auditing

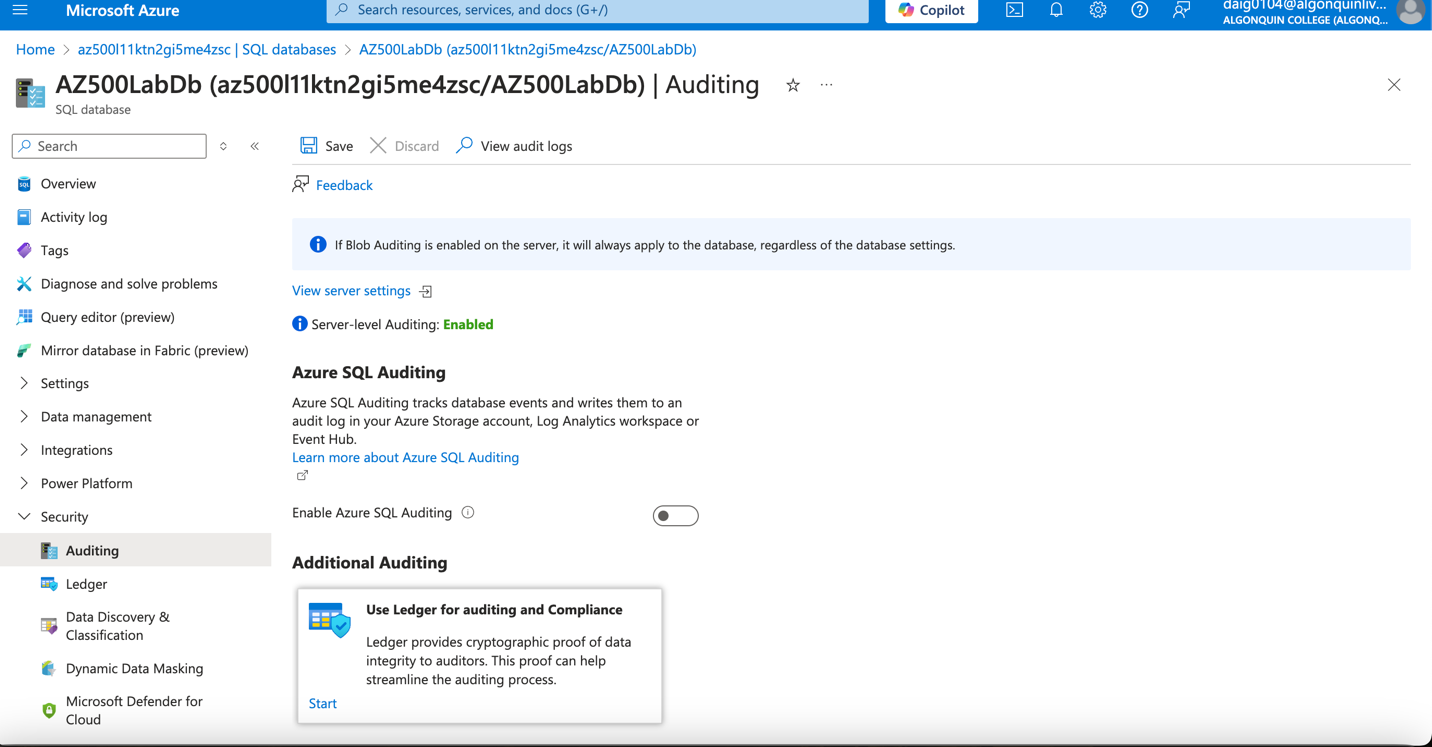
### Creating the storage account when enabling auditing:



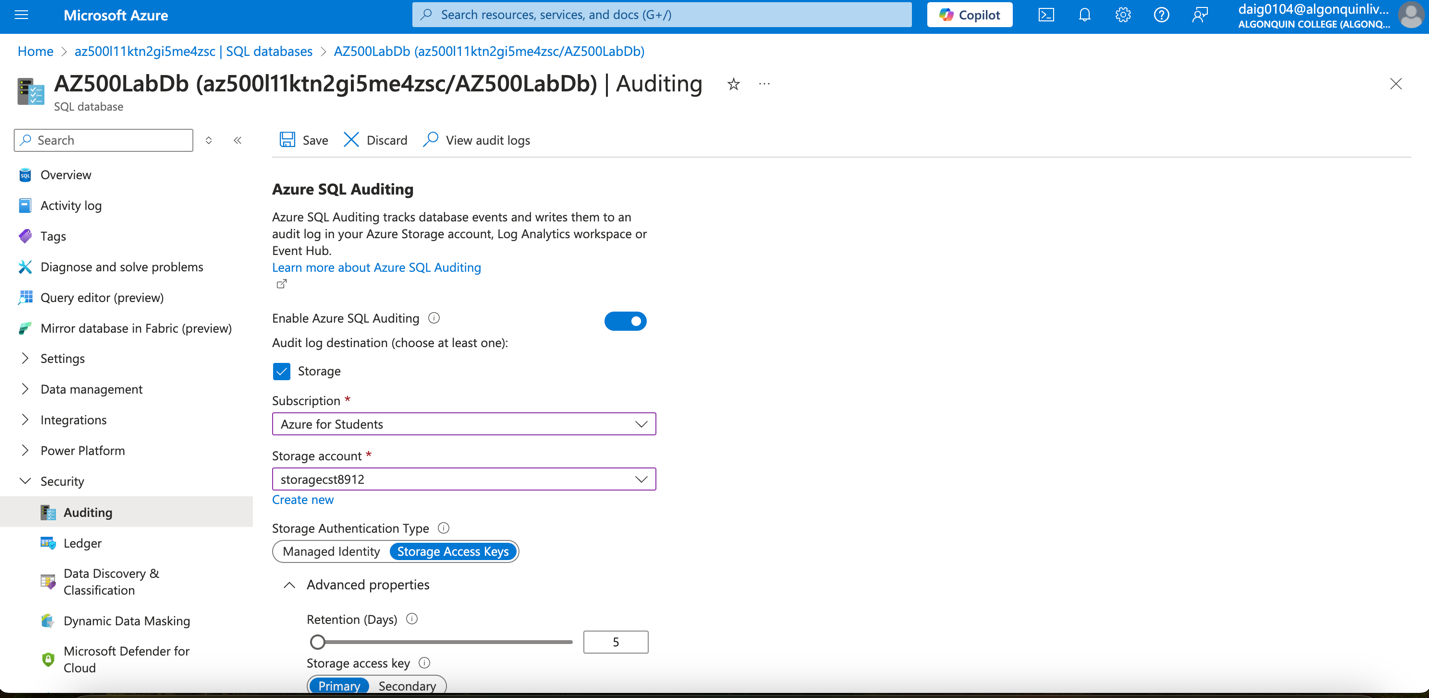
### Enabled Auditing, with subscription, storage account and Retention (days) to 5.



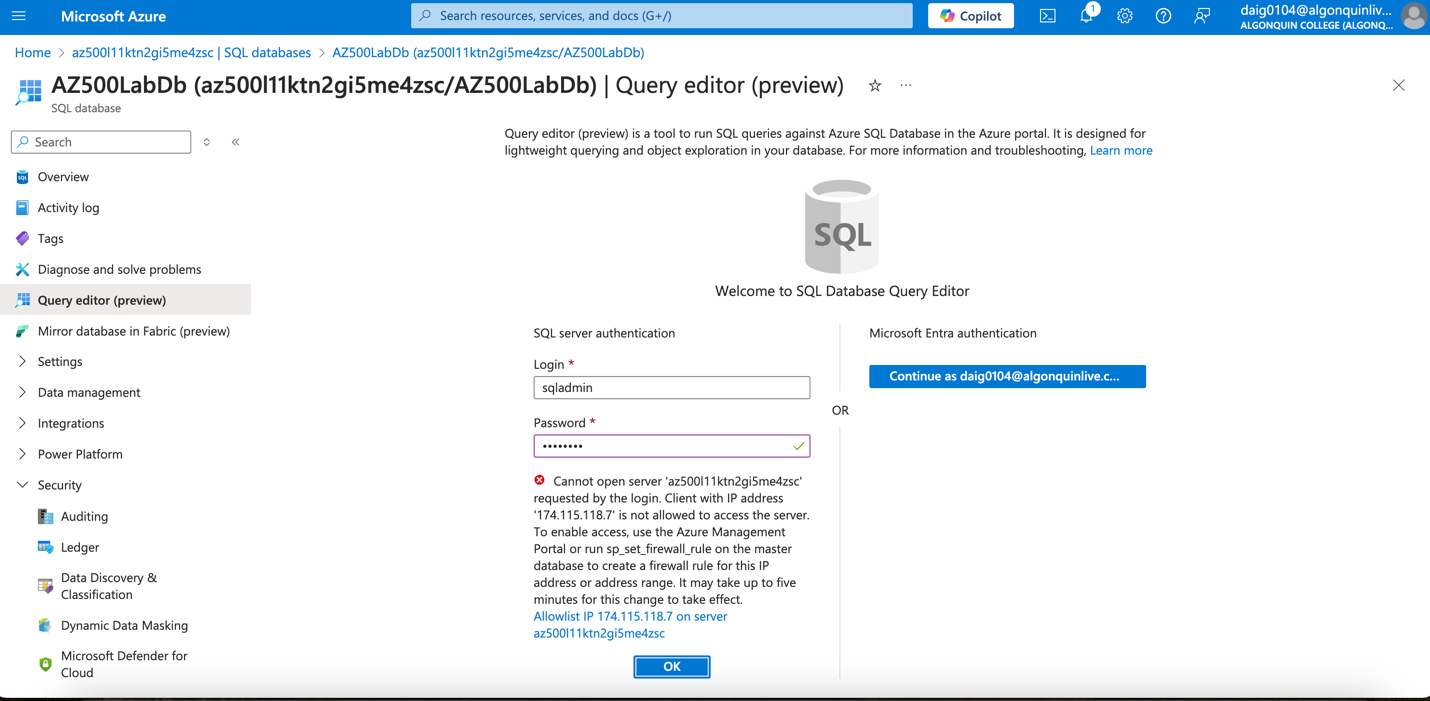
### Within the database level auditing. Server-level auditing is already enabled, (I actually tried one with enabling database auditing and without)



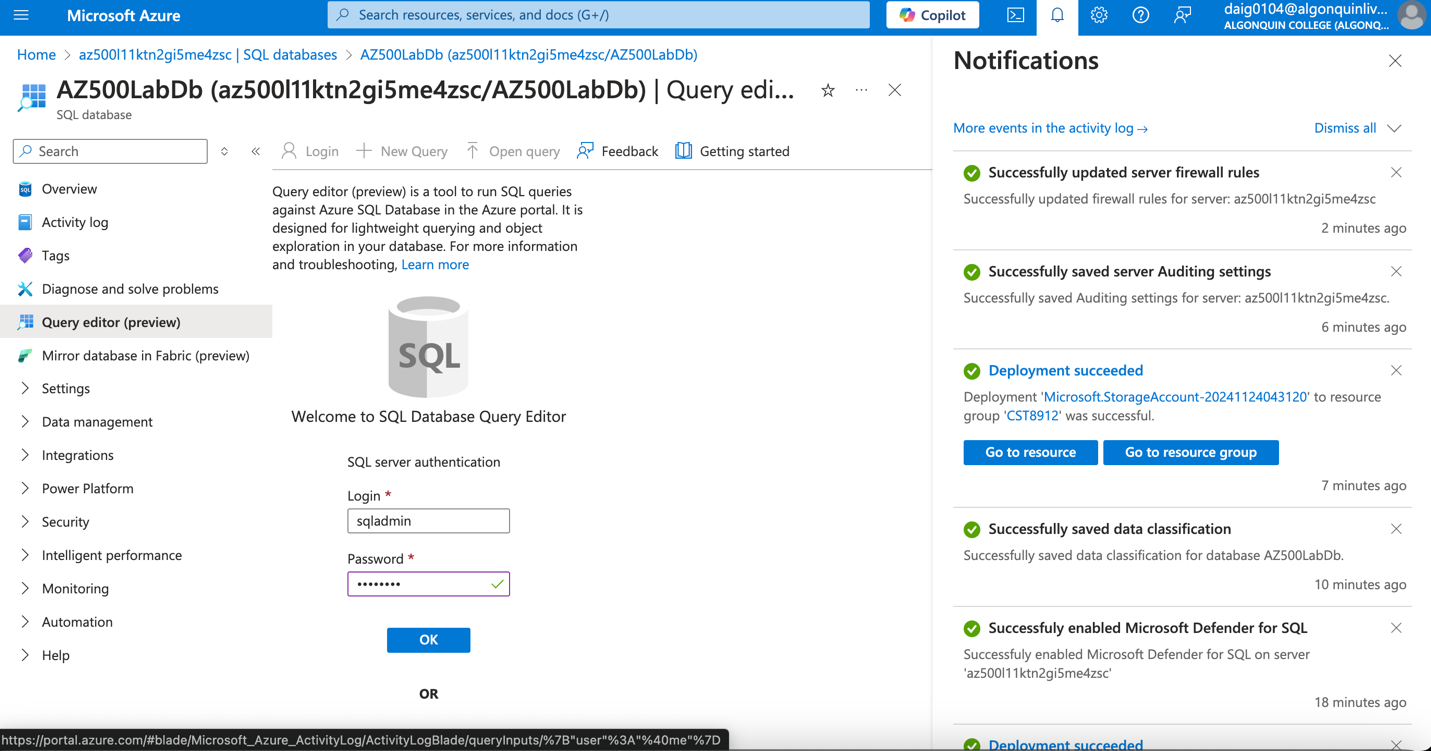
### With database auditing enabled (I picked the same configurations as the server auditing)



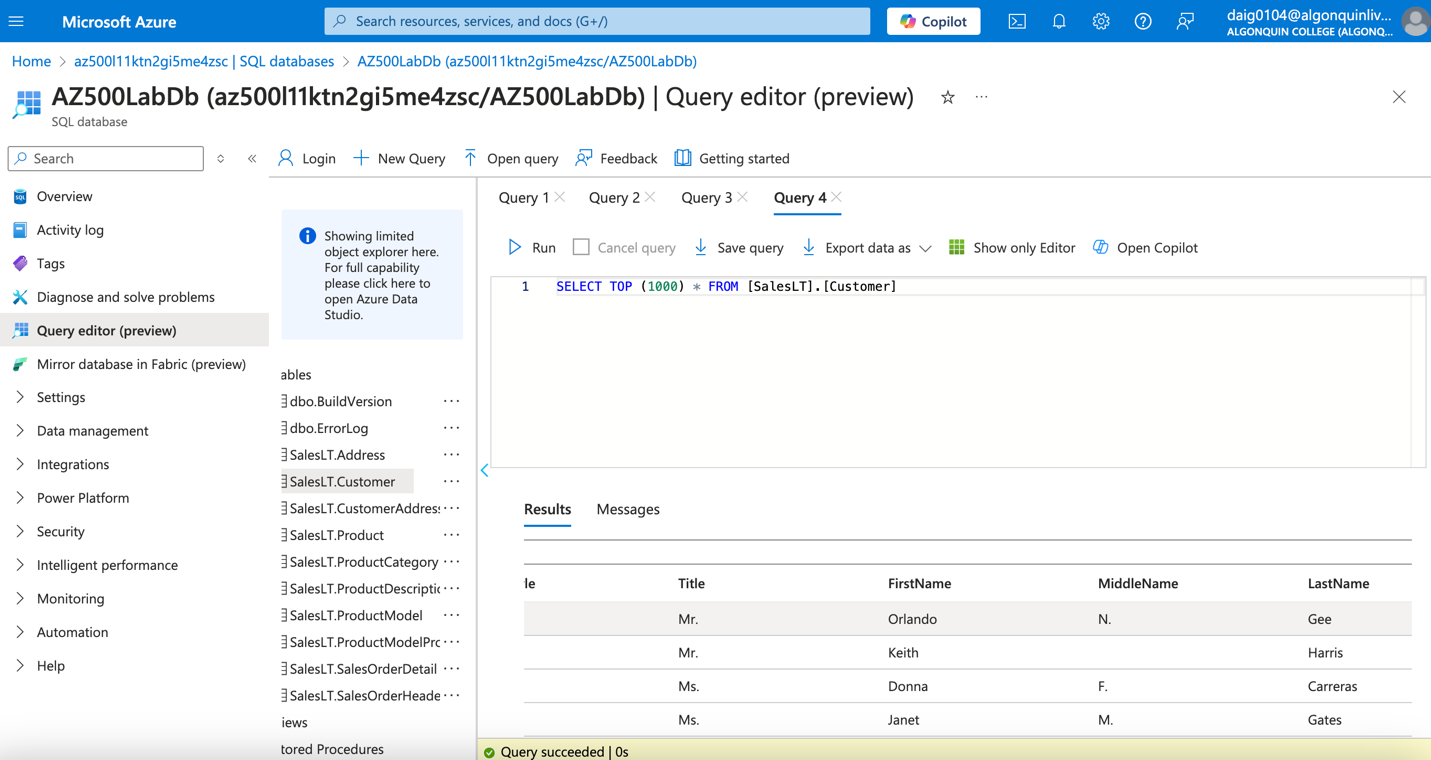
### Signing in select Query editor (preview). Here, there is an error stating the firewall is blocking access to the Query editor, by clicking the allowlist IP it fixes the error.



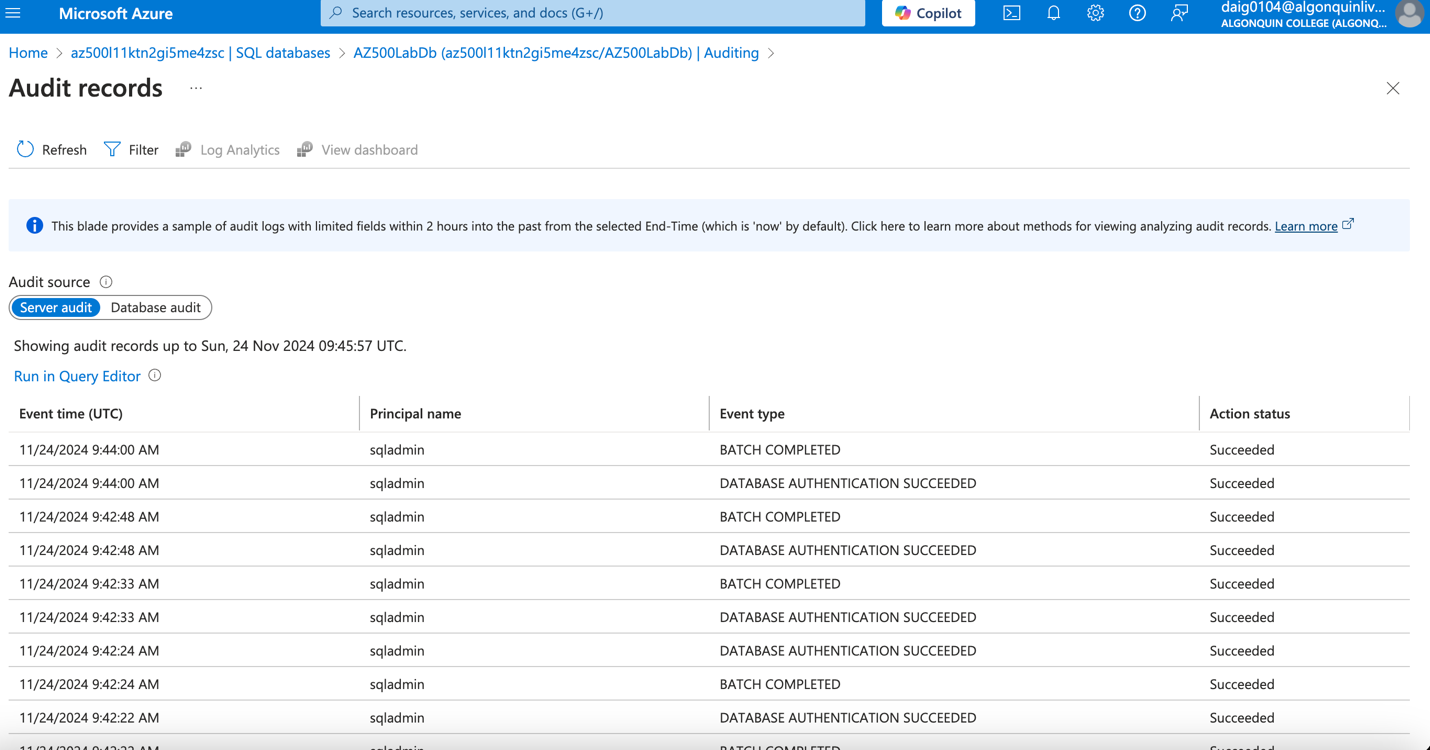
### The fixed firewall rules



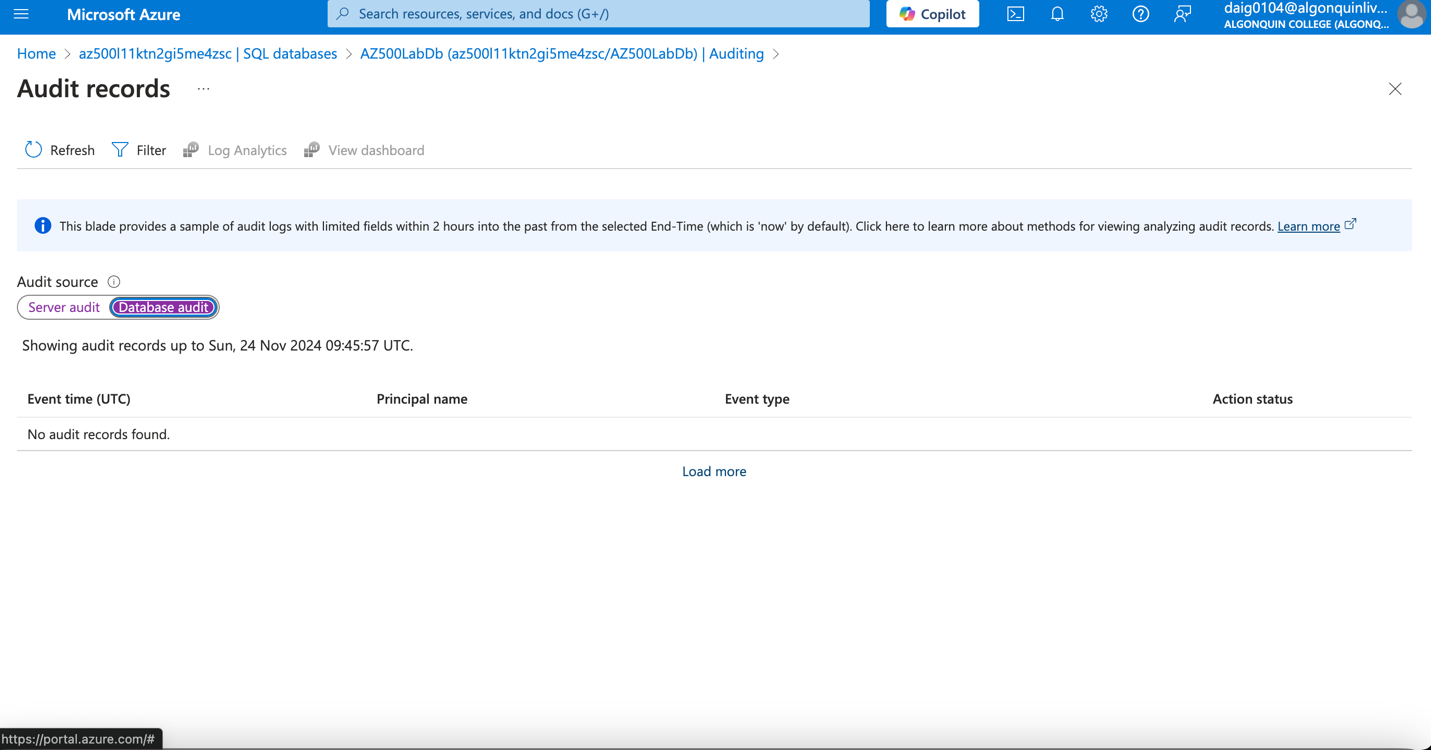
### The query editor, here I selected top 1000 customers from the database.



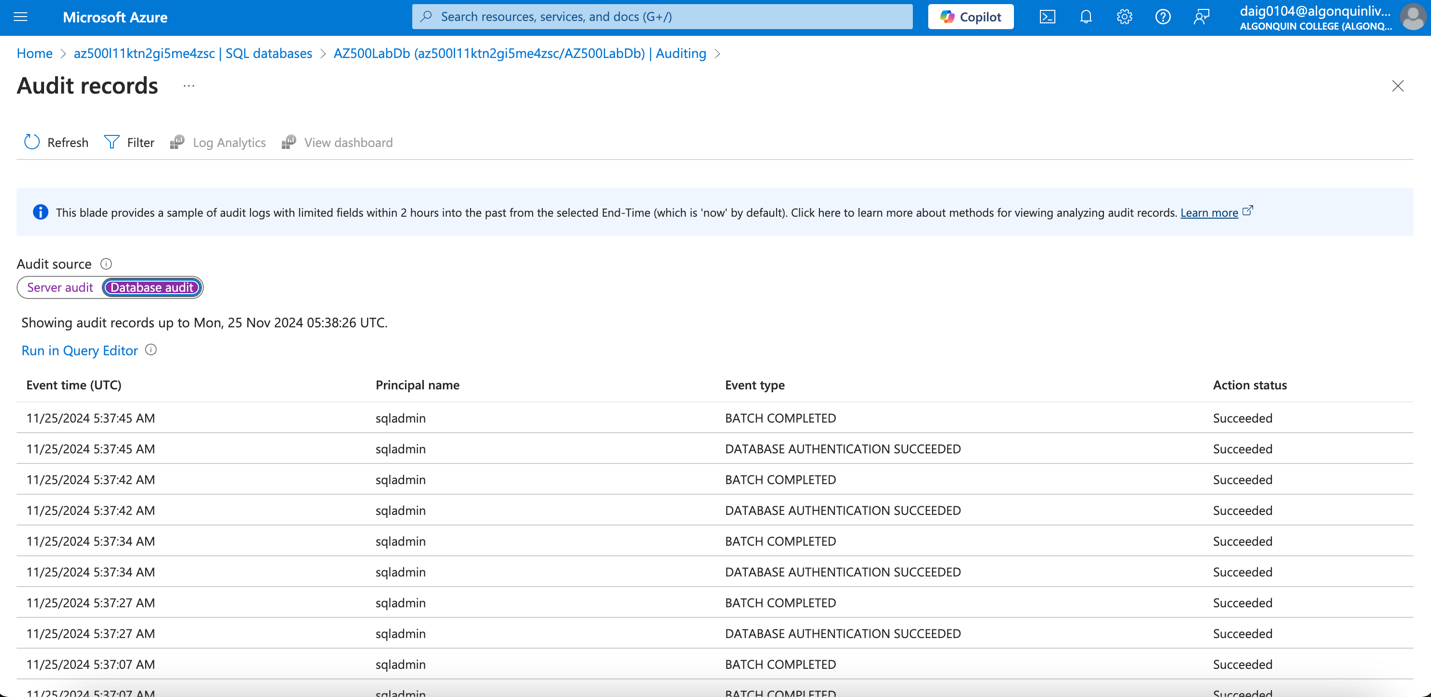
### Viewing Audit Logs and audit records this is the Server Audit:



### This is the database audit if the database auditing was disabled.



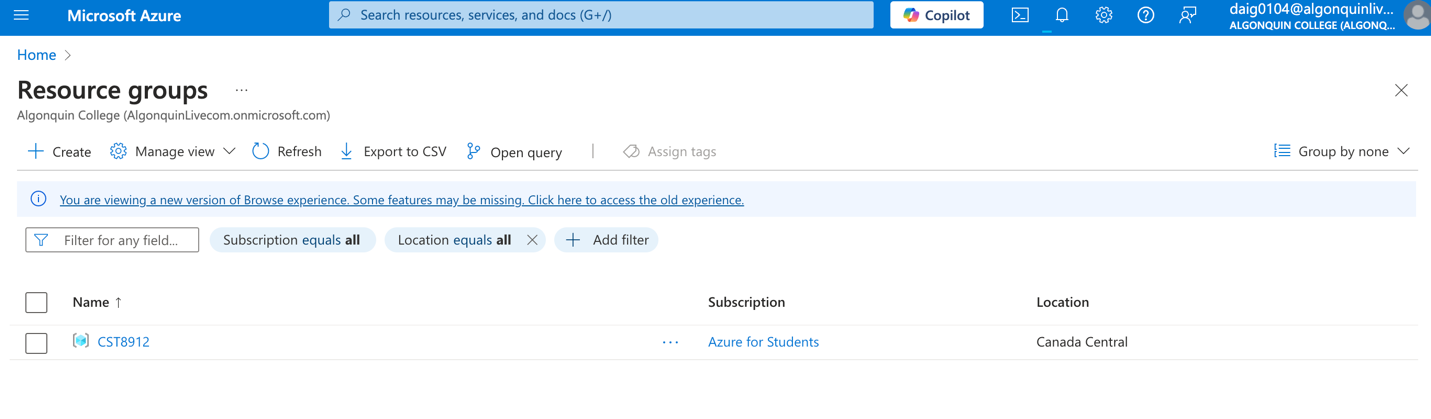
### This is the database audit if the database auditing was enabled.



### Cleaning up resources created during this lab, deleting the resource group



Before:



After:



# Conclusion:

In this lab, I learned about the different tools used in Azure to safeguard data from harmful attacks. Microsoft Defender is enabled for advanced data protection with its advanced vulnerability assessments, scanning the database for vulnerabilities weekly. Advanced threat protection also will send alerts to your email by Microsoft Defender. I also learned about auditing and the difference between server-level and database-level auditing to audit and review the classification of data within the database. Lastly, I learned a bit about firewalls and how you must allow specific IPs to enter, as the firewall will deny any other.