Azure SQL Diagnostics and Audit Logs

Auditing in Azure SQL Database is a security feature that helps track and monitor database activities. It logs database events to provide insight into database access, operations, and changes. This is crucial for regulatory compliance, security, and troubleshooting. Azure SQL Database auditing can be configured to store logs in various destinations, such as an Azure Storage Account, Log Analytics Workspace, or an Event Hub.

Key features of auditing in Azure SQL Database include:

Activity Monitoring: Tracks database reads, updates, deletes, and administrative actions.

Compliance: Helps meet organizational and regulatory requirements by providing an audit trail.

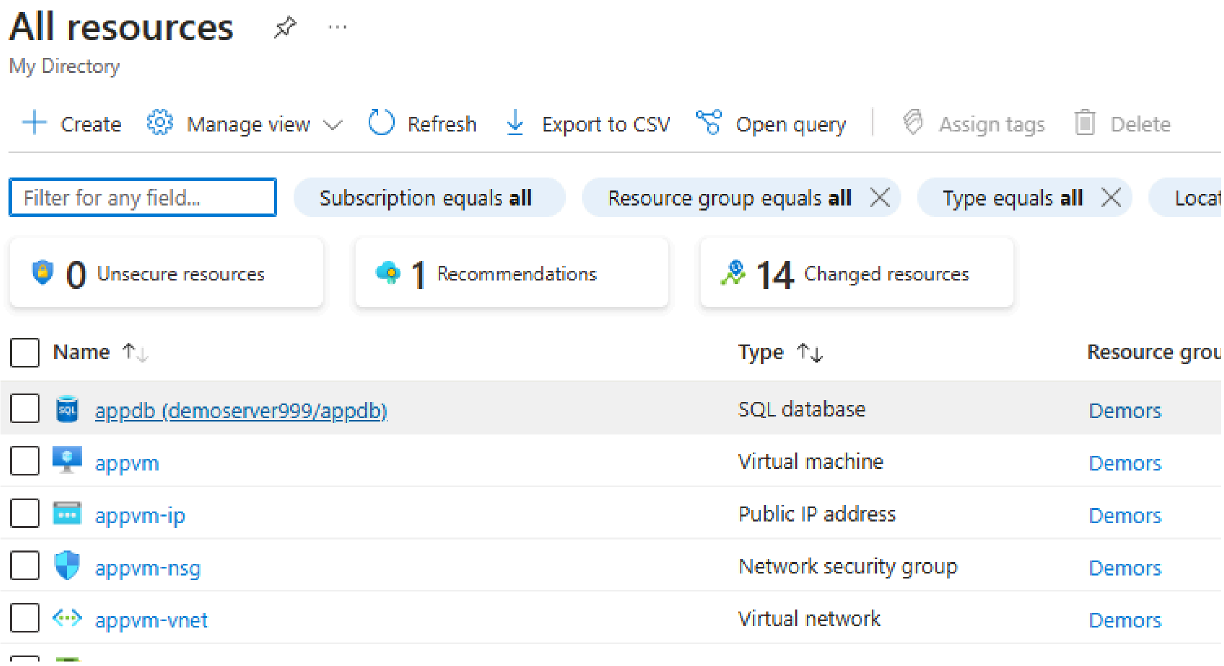
Security Insights: Detects unusual or unauthorized activity.

Integration: Works seamlessly with Azure Monitor, Security Center, and other Azure services. Auditing ensures accountability and supports proactive management of database security.

The end goal of this lab is to enable auditing for an Azure SQL Database to monitor and track database activities for compliance and security purposes. By enabling auditing through the Azure portal and configuring it to send logs to a Log Analytics workspace, all database activity is captured. This includes creating diagnostic settings, performing operations on the database through SQL Server Management Studio (SSMS), and observing the audit logs in the Log Analytics workspace after a short interval. This process ensures enhanced visibility into database operations and provides valuable insights for maintaining security and compliance standards.

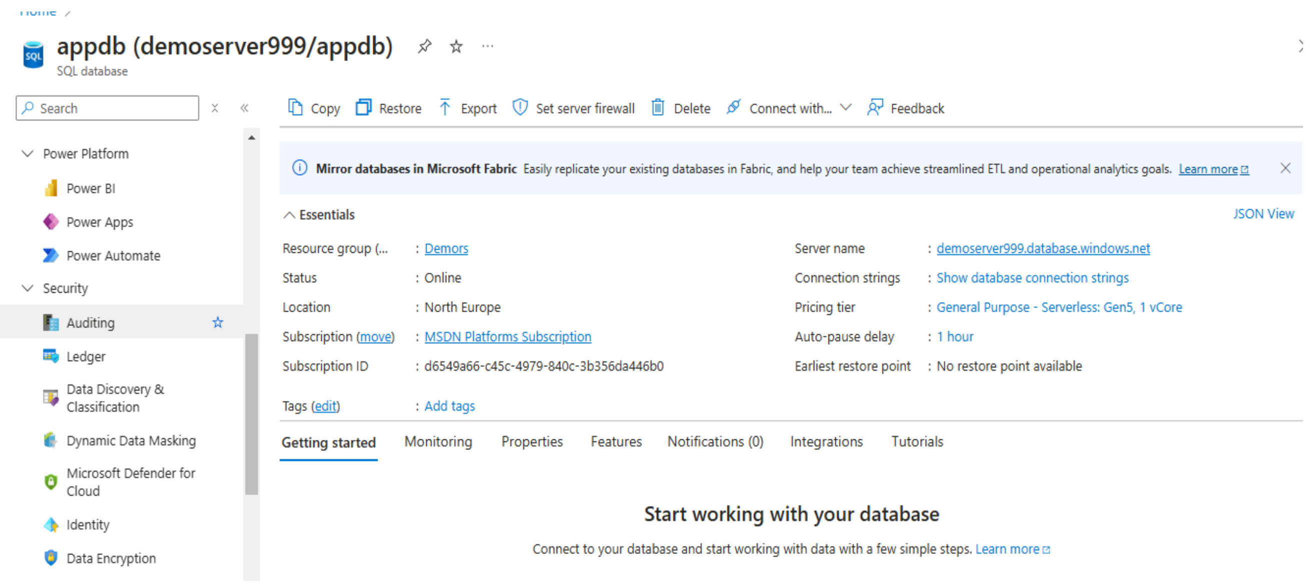
To begin with the lab

1. In this lab we will enable Auditing for our SQL Database, for that access SQL Database in Azure Portal. Log in to the Azure portal and Navigate to your SQL database instance.



Name	Type	Resource grou
appdb (demoserver999/appdb)	SQL database	Demors
appvm	Virtual machine	Demors
appvm-ip	Public IP address	Demors
appvm-nsg	Network security group	Demors
appvm-vnet	Virtual network	Demors

2. Now go to the **Security** tab, select **Auditing**, enable auditing at the database level.



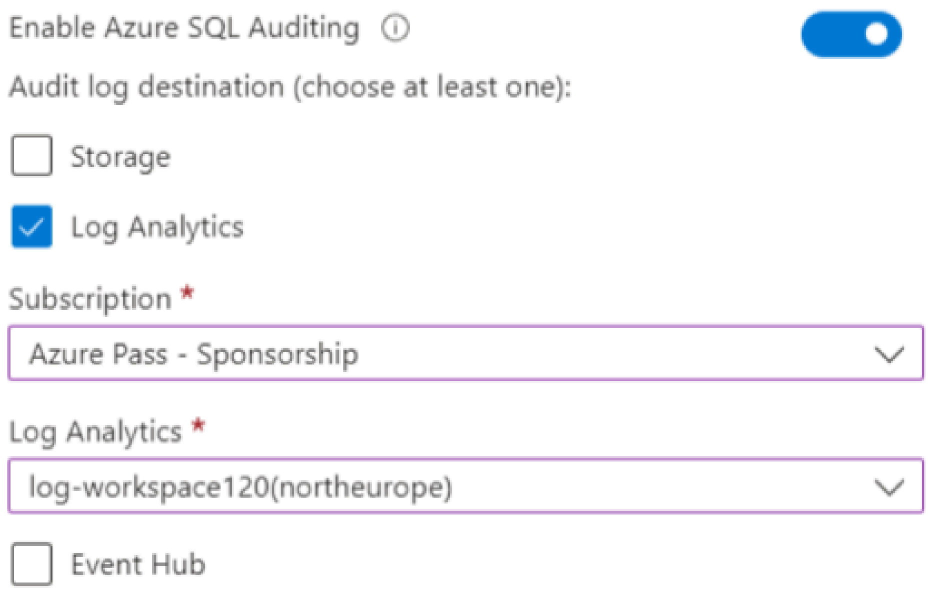
Mirror databases in Microsoft Fabric Easily replicate your existing databases in Fabric, and help your team achieve streamlined ETL and operational analytics goals. Learn more

Resource group (... : Demors
Status : Online
Location : North Europe
Subscription (move) : MSDN Platforms Subscription
Subscription ID : d6549a66-c45c-4979-840c-3b356da446b0
Tags (edit) : Add tags

Server name : demoserver999.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

Start working with your database

Connect to your database and start working with data with a few simple steps. Learn more



Enable Azure SQL Auditing ⓘ ●

Audit log destination (choose at least one):

□ Storage

☑ Log Analytics

Subscription *

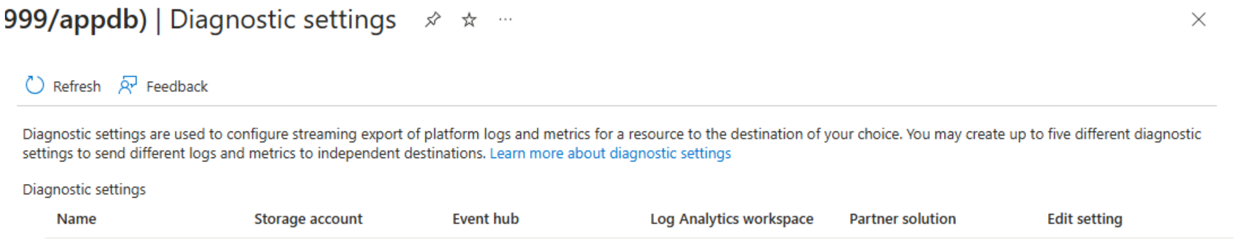
Azure Pass - Sponsorship

Log Analytics *

log-workspace120(northeurope)

□ Event Hub

3. In the Azure Portal, scroll down the left pane of your SQL Database page.
4. Select **Diagnostic settings**. You will see that a diagnostic rule has been automatically created when auditing was enabled. Click **Edit settings** to view or modify the details of the diagnostic rule, including what log categories are being sent to the selected destination



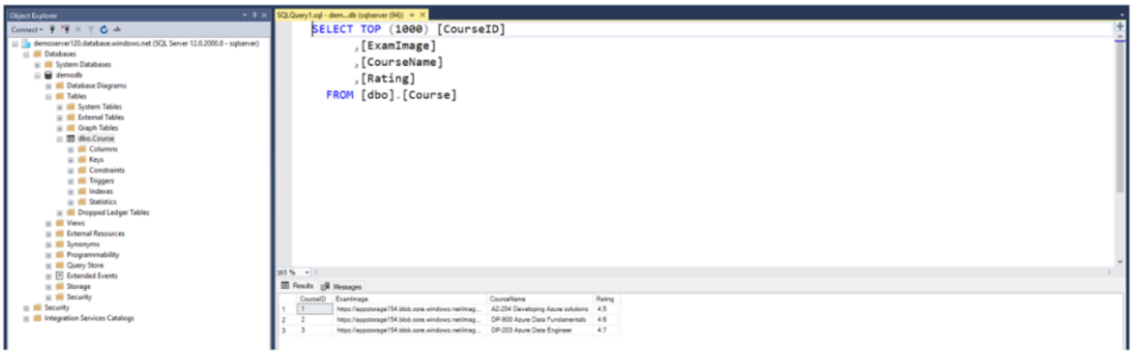
999/appdb) | Diagnostic settings

Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostic settings

Diagnostic settings

Name	Storage account	Event hub	Log Analytics workspace	Partner solution	Edit setting

5. Open **SQL Server Management Studio (SSMS)** on your local machine. If SSMS is not installed, download and install it from the Microsoft website. Copy the **server name** from the database overview in the Azure portal. Use your **SQL username and password** to authenticate.
6. Expand the database in the Object Explorer to locate the **Course** table.



```
SELECT TOP (1000) [CourseID]
      ,[ExamImage]
      ,[CourseName]
      ,[Rating]
  FROM [dbo].[Course]
```

	CourseID	ExamImage	CourseName	Rating
1	1	https://appstorage154.blob.core.windows.net/imag...	AZ-204 Developing Azure solutions	4.5
2	2	https://appstorage154.blob.core.windows.net/imag...	DP-900 Azure Data Fundamentals	4.6
3	3	https://appstorage154.blob.core.windows.net/imag...	DP-203 Azure Data Engineer	4.7

7. Wait for 10–15 minutes to allow logs to stream to the Log Analytics workspace. Navigate to the **Log Analytics Workspace** in the Azure portal. Go to the **Logs** section.Under **Log Management**, find the **Azure Diagnostics** table.
8. Run a query to check for security events or other audit logs.