Audit Setup

Last updated by | Vitor Tomaz | Feb 18, 2021 at 3:29 AM PST

Contents

Auditing for Azure SQL Database tracks database events and writes them to an audit log in your Azure storage account, Log Analytics workspace or Event Hubs.

Auditing also:

- Helps you maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations.
- Enables and facilitates adherence to compliance standards, although it doesn't guarantee compliance. For more information about Azure programs that support standards compliance, see the Azure Trust Center where you can find the most current list of SQL Database compliance certifications.

Setup

Check official documentation Azure SQL Auditing for Azure SQL Database

For **Audit to LOG Analytics** follow up **AZURE SQL DB AND LOG ANALYTICS BETTER TOGETHER - Post Series**

- PART #1 - How to setup and query
- PART #2 – ALERTS
- PART #3 - Query AUDIT data or Who dropped my TABLE?

Setup (NON DEFAUL EVENTS)

The default auditing policy includes all actions and the following set of action groups, which will audit all the queries and stored procedures executed against the database, as well as successful and failed logins:

- BATCH_COMPLETED_GROUP
- SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP
- FAILED_DATABASE_AUTHENTICATION_GROUP

You can configure auditing for different types of actions and action groups using PowerShell, as described in the Manage SQL database auditing using Azure PowerShell.

Accepted values:

- BATCH_STARTED_GROUP
- BATCH_COMPLETED_GROUP
- APPLICATION_ROLE_CHANGE_PASSWORD_GROUP
- BACKUP_RESTORE_GROUP
- DATABASE_LOGOUT_GROUP
- DATABASE_OBJECT_CHANGE_GROUP
- DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP
- DATABASE_OBJECT_PERMISSION_CHANGE_GROUP
- DATABASE_OPERATION_GROUP
- DATABASE_PERMISSION_CHANGE_GROUP
- DATABASE_PRINCIPAL_CHANGE_GROUP
- DATABASE_PRINCIPAL_IMPERSONATION_GROUP
- DATABASE_ROLE_MEMBER_CHANGE_GROUP
- FAILED_DATABASE_AUTHENTICATION_GROUP
- SCHEMA_OBJECT_ACCESS_GROUP
- SCHEMA_OBJECT_CHANGE_GROUP
- SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP
- SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP
- SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP
- USER_CHANGE_PASSWORD_GROUP

Limitations

- Premium storage is currently not supported.
- Hierarchical namespace for Azure Data Lake Storage Gen2 storage account is currently not supported.
- Enabling auditing on a paused Azure SQL Data Warehouse is not supported. To enable auditing, resume the Data Warehouse.

Public Doc Reference

- Azure SQL Auditing for Azure SQL Database
- Write audit to a storage account behind VNet and firewall
- SQL Database Audit Log Format

Internal Reference

- How to check if it is enabled CMS
- Security Vulnerabilities reported in Azure SQL DB
- Known issues
- Audit troubleshooting on Jarvis
- REST API sample
- SQL Managed Instance Auditing
- Audit log Alerts

- Azure SQL Auditing impact

How good have you found this content?

🙂 🙁