sqlbits
HANDLE AZURE SQL
AUDITING WITH EASE

ABOUT ME

sqlbits

Josephine Bush

10+ years DBA experience

MBA IT Management

MS Data Analytics

@hellosqlkitty

sqlkitty.com

WHAT IS AUDITING?

sqlbits

Collecting and examining information to determine proper use or misuse

WHY AUDIT?

Maybe your company says they don’t value knowing what’s going on in your databases, but….

PROBLEMS AUDITING CAN SOLVE

sqlbits

Who broke this?

Who changed this?

Who used this?

You can audit pretty much everything anyone does in SQL Server!

5

CLOUD SQL AUDITING OPTIONS

sqlbits

Cloud solution	SQL Server Audit Available	Extended Events Available	Auditing differences
Azure SQL	No	Yes	SQL Server audit quasi equivalent via Azure portal
Azure SQL Managed Instance	Yes	Yes	Need to use cloud storage
SQL Server VM	Yes	Yes	Uses disk storage
Amazon Web Services RDS	Yes	Yes	Need to use cloud storage

AZURE SQL AUDITING

Audit at server and database level via the portal

Use these to see queries run by users on Azure SQL

AZURE SQL AUDITING POLICY

sqlbits

Audits all queries and stored procedures executed against the database, and all successful and failed logins

Using these audit actions:
BATCH_COMPLETED_GROUP
SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP
FAILED_DATABASE_AUTHENTICATION_GROUP

MODIFY AZURE SQL AUDITING POLICY

sqlbits

Allows you to audit fewer actions and filter those actions using Azure PowerShell

Set-AZSqlServerAudit to modify server auditing policy
Get-AZSqlServerAudit to see current server auditing policy

ENABLING AZURE SQL AUDITING

Home > SQL databases > jbdb (azure-sql-server-jb/jbdb) > azure-sql-server-jb

azure-sql-server-jb | Auditing ...

SQL server

Search (Cmd+/)

Save Discard Feedback

Data management

- Backups
- Deleted databases
- Failover groups
- Import/Export history

Security

- Auditing
- Firewalls and virtual networks
- Private endpoint connections
- Security Center
- Transparent data encryption
- Identity (preview)

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
- [ ] 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

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

- [ ] Storage
- [ ] Log Analytics
- [ ] Event Hub

AZURE SQL AUDITING OPTIONS

sqlbits

Audit log destination (choose at least one):

- [ ] Storage
- [ ] Log Analytics
- [ ] Event Hub

AZURE SQL AUDITING STORAGE

Audit log destination (choose at least one):

☑ Storage

Subscription *

Azure for Students

Storage account *

jbazuresqlauditing

Create new

Advanced properties

Retention (Days) ⓘ

0

Storage access key ⓘ

Primary Secondary

AZURE SQL AUDITING STORAGE FILES

Home > jbazuresqlauditing >

sqldbauditlogs
Container

Search (Cmd+/)

- Overview
- Diagnose and solve problems
- Access Control (IAM)

Settings

- Shared access tokens
- Access policy
- Properties

Upload | Change access level | Refresh | Delete | Change tier | Acquire lease | Break lease | View snapshots

Authentication method: Access key (Switch to Azure AD User Account)
Location: sqldbauditlogs / azure-sql-server-jb / jbdb / SqlDbAuditing_ServerAudit / 2021-11-01

Search blobs by prefix (case-sensitive)

Show deleted blobs

Name	Modified	Access tier	Blob type	Size	Lease state
[..]					
18_39_10_366_0.xel	11/1/2021, 12:39:11 ...		Append blob	7.5 KiB	Available

AZURE SQL AUDITING LOG ANALYTICS

sqlbits

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
- [x] Log Analytics

Subscription *

Azure for Students

Log Analytics *

dbaudit(eastus2)

VIEW LOG ANALYTICS AUDIT DATA

sqlbits

View audit data at the database level

auditingtest (josephinebtest/auditingtest) | Auditing
SQL database

Search (Ctrl+/)

Settings
- Configure
- Geo-Replication
- Connection strings
- Sync to other databases
- Add Azure Search
- Properties
- Locks

Integrations
- Stream analytics (preview)

Security
- Auditing
- Data Discovery & Classification

Save | Discard | View audit logs | Feedback

1

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

Audit records

Refresh | Filter | Log Analytics | View dashboard

2

Click here to learn more about methods for viewing & analyzing audit records.

Audit source: Server audit | Database audit

Showing audit records up to Mon, 22 Feb 2021 23:26:44 UTC.

Event time (UTC)	Principal name	Event type	Action status
No audit records found.			

Logs
JBSQLAuditing

3

New Query 1*

JBSQLAuditing | Select scope | Run | Time range : Last 24 hours | Save | Copy link | New alert rule | Export | Pin to dashboard | Format query | Feedback | Queries | Query explorer

Tables | Queries | Filter

Search

Filter | Group by: Solution

Collapse all

Favorites

You can add favorites by clicking on the ☆ icon

LogManagement
- AzureDiagnostics

Functions

```
AzureDiagnostics
| where Category == 'SQLSecurityAuditEvents'
| where ResourceId == '/SUBSCRIPTION[redacted]RESOURCEGROUPS/SQLAUDITING/PROVIDERS/MICROSOFT.SQL/SERVERS/JOSEPHINEBTEST/DATABASES/MASTER' and database_name_s == 'auditingtest'
| project event_time_t, statement_s, succeeded_s, affected_rows_d, server_principal_name_s, client_ip_s, application_name_s, additional_information_s, data_sensitivity_information_s
| order by event_time_t desc
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed. Showing results from the last 24 hours. 00:00.5 | 100 records

event_time_t [UTC]	statement_s	succeeded_s	affected_rows_d	server_principal_name_s
2/22/2021, 11:21:36.019 PM	ALTER TABLE dbo.testing SET (LOCK_ESCALATION = TABLE)	true	0	josephine
2/22/2021, 11:21:35.972 PM	CREATE TABLE dbo.testing (testing nchar(10) NULL) ON [PRIMARY]	true	0	josephine
2/22/2021, 11:21:35.941 PM		true	0	josephine
2/22/2021, 11:21:35.894 PM	DECLARE @edition sysname; SET @edition = cast(SERVERPROPERTY...	true	4	josephine

Page 1 of 2 | 50 items per page | 1 - 50 of 100 items

VIEW LOG ANALYTICS WORKSPACE

sqlbits

View audit data in workspace summary

AZURE SQL AUDITING EVENT HUB

Enable Azure SQL Auditing

Audit log destination (choose at least one):

- [ ] Storage
- [ ] Log Analytics
- [x] Event Hub

Subscription *

Azure for Students

Event Hub namespace *

dbaudithub

Event hub name (optional)

(Create in selected namespace)

Event hub policy name *

RootManageSharedAccessKey

AZURE SQL AUDITING EVENT HUB DATA

ENABLING AZURE SQL AUDITING

Enabling at database level instead of server level to audit only one database

Don’t do this if you already enabled at server level

AZURE SQL AUDITING DEMO

sqlbits

AZURE SQL AUDITING EXTENDED EVENTS

Script

```
CREATE EVENT SESSION [audit] ON DATABASE
ADD EVENT sqlserver.rpc_completed(
ACTION(sqlserver.client_app_name,sqlserver.client_hostna
me,sqlserver.database_name,sqlserver.sql_text,sqlserver.
username)
    WHERE ([sqlserver].[username]=N'josephine')),
ADD EVENT sqlserver.sql_batch_completed(
ACTION(sqlserver.client_app_name,sqlserver.client_hostna
me,sqlserver.database_name,sqlserver.sql_text,sqlserver.
username)
    WHERE ([sqlserver].[username]=N'josephine'))
ADD TARGET package0.event_file(SET
filename=N'https://StorageAccount.blob.core.windows.net/
Container/audit.xel')
WITH (STARTUP_STATE=ON)
```

GUI

MANAGED INSTANCE AUDITING

sqlbits

SQL Server Audit

Extended Events

RESOURCES

Azure SQL Audit Overview

https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview

Azure SQL Audit Modify Auditing Policy

https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview#manage-auditing

Kusto Query Language (KQL)

https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/

AWS RDS Auditing

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.SQLServer.Options.Audit.html

https://aws.amazon.com/blogs/database/set-up-extended-events-in-amazon-rds-for-sql-server/

Azure SQL Managed Instance Auditing

https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/auditing-configure

Azure SQL Extended Events

https://docs.microsoft.com/en-us/azure/azure-sql/database/xevent-db-diff-from-svr

FEEDBACK

https://sqlb.it/?7194

THANK YOU FOR ATTENDING

Contact me @hellosqlkitty

or visit me at sqlkitty.com

sqlbits