

HANDLE AZURE SQL AUDITING WITH EASE

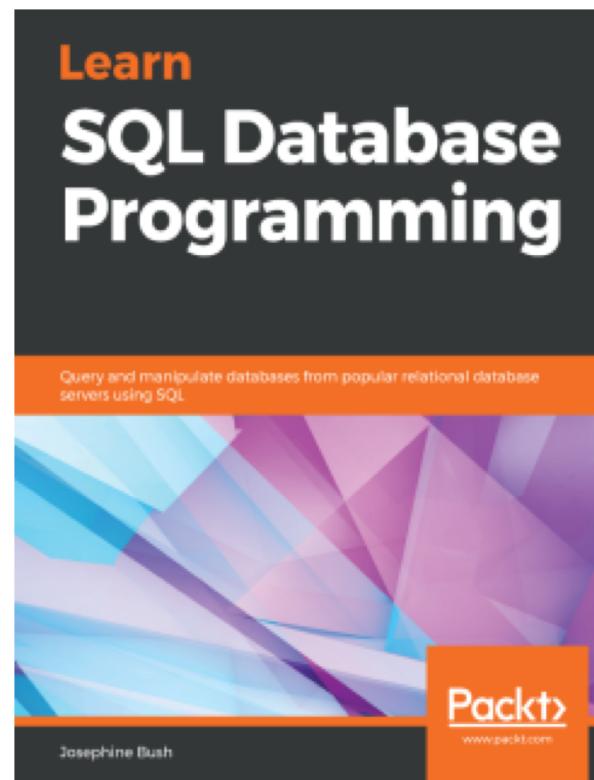
ABOUT ME

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

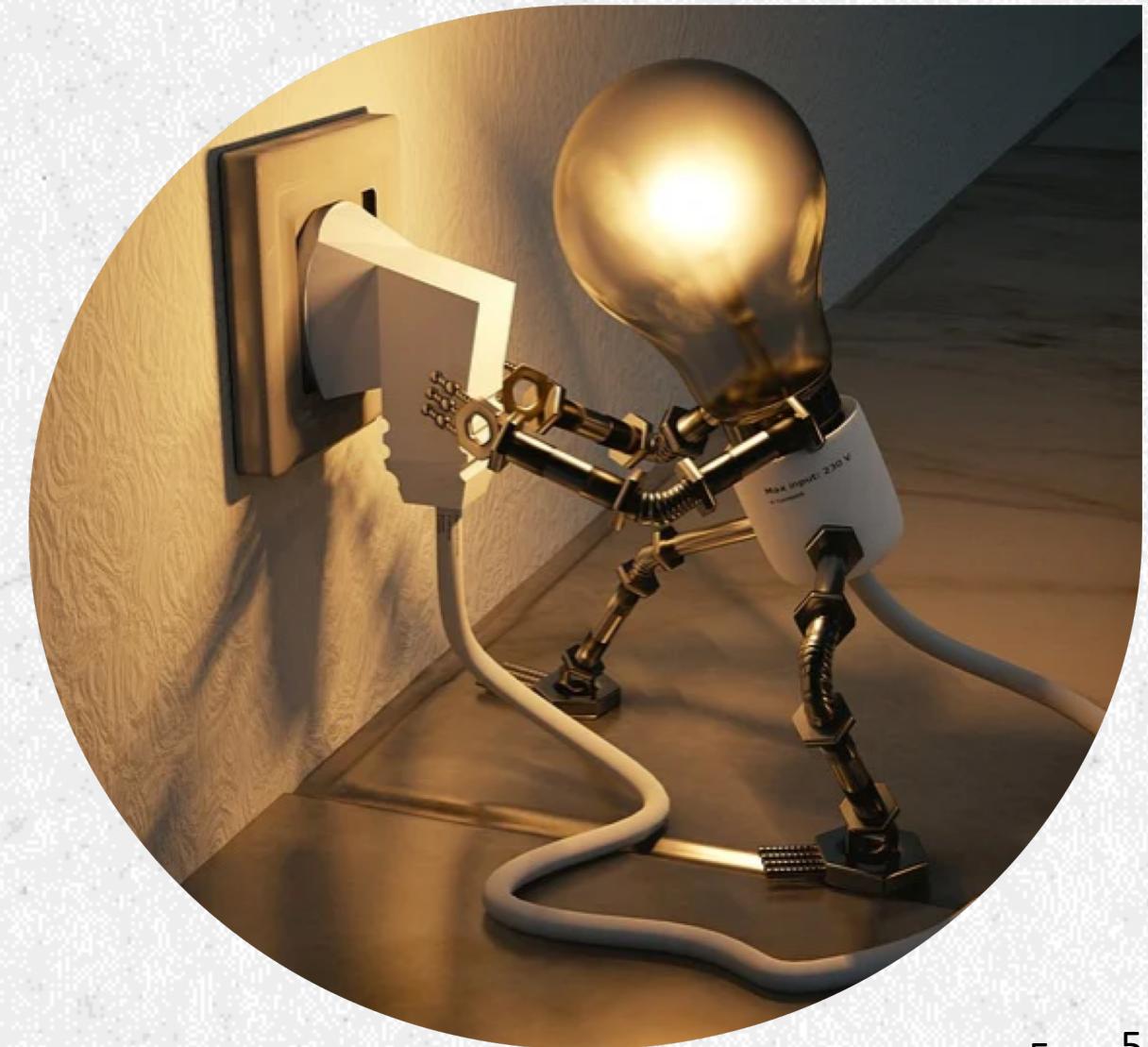
sqlbits

Who broke this?

Who changed this?

Who used this?

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



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

sqlbits



Audit at server and database level
via the portal

Use these to see queries run by
users on Azure SQL

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

sqlbits

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



Audit log destination (choose at least one):

- Storage
- Log Analytics
- Event Hub

AZURE SQL AUDITING STORAGE

sqlbits

Audit log destination (choose at least one):

Storage

Subscription *

Azure for Students



Storage account *

jbazuresqlauditing



[Create new](#)

^ Advanced properties

Retention (Days) ⓘ



Storage access key ⓘ

Primary

Secondary

AZURE SQL AUDITING STORAGE FILES

sqlbits

The screenshot shows the Azure Storage Blob Container interface for the container 'sqldbauditlogs'. The left sidebar includes navigation links: Home, Overview (which is selected), Diagnose and solve problems, Access Control (IAM), Settings, Shared access tokens, Access policy, and Properties. The main area displays the container's properties: Authentication method (Access key) and Location (sqldbauditlogs / azure-sql-server-jb / jbdb / SqIDbAuditing_ServerAudit / 2021-11-01). It features a search bar for blobs by prefix, a 'Show deleted blobs' toggle, and a table listing blobs. The table columns are Name, Modified, Access tier, Blob type, Size, and Lease state. One blob is listed: Name [..], Modified 11/1/2021, 12:39:11 ..., Blob type Append blob, Size 7.5 KiB, Lease state Available.

Name	Modified	Access tier	Blob type	Size	Lease state
[..]	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

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+ /)

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.

Settings

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

Integrations

- Stream analytics (preview)

Security

- Auditing
- Data Discovery & Classification

2

Audit records

Refresh Filter Log Analytics View dashboard

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	Action status
No audit records found.		

3

New Query 1*

Logs JBSQLAuditing

Run Time range : Last 24 hours

Save Copy link New alert rule Export Pin to dashboard Format query

Azure JBSQLAuditing Select scope

Tables Queries Filter

Search

Filter Group by: Solution

Enable

Collapse all

Favorites

You can add favorites by clicking on the star icon

LogManagement

- AzureDiagnostics
- Functions

Completed. Showing results from the last 24 hours.

event_time_t [UTC]	statement_s	succeeded_s	affected_rows_d	server_principal_name_s	client_ip_s	application_name_s
2/22/2021, 11:21:36.019 PM	ALTER TABLE dbo.testing SET (LOCK_ESCALATION = TABLE)	true	0	josephine	6	
2/22/2021, 11:21:35.972 PM	CREATE TABLE dbo.testing (testing nchar(10) NULL) ON [PRIMARY]	true	0	josephine	6	
2/22/2021, 11:21:35.941 PM		true	0	josephine	6	
2/22/2021, 11:21:35.894 PM	DECLARE @edition sysname; SET @edition = cast(SERVERPROPERTY...	true	4	josephine	6	
2/22/2021, 11:21:35.894 PM	GO	true	0	josephine	6	

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

VIEW LOG ANALYTICS WORKSPACE

sqlbits

View audit data in workspace summary

Log Analytics workspaces > dbauditdata > Overview >

SQLSecurityInsights

dbauditdata

Refresh Logs Edit

⚠️ Workbooks will be replacing View Designer. Learn how to keep your views updated with workbooks. →

2/21/22 15:24 - 2/22/22 15:24 +

Azure SQL - Security Insights

More info ↗

Gain insights into your database activities!

SQL Azure - Security Insights helps you understand database activity, and gain insight into **anomalies** that could indicate business concerns or suspected security violations.

Learn more about [Azure SQL Auditing](#) and [Azure Monitor](#)

AUDIT DISTRIBUTION

180 ALL DATA

Time	Count
1:00 PM	180
5:00 PM	0

ACTION NAME COUNT

Action Name	Count
BATCH COMPLETED	129
RPC COMPLETED	26
DATABASE AUTHENTICATION ...	19
AUDIT SESSION CHANGED	6

DISTRIBUTION BY DATABASE

Databases

180 TOTAL

Database	Count
jbdb	6
master	120
Others	54

DISTRIBUTION BY IP

IP Address

2

IP Address	Count
67.:	174
Internal	6

AZURE SQL AUDITING EVENT HUB

sqlbits

Enable Azure SQL Auditing (i) 

Audit log destination (choose at least one):

Storage

Log Analytics

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

sqlbits

Home > dbaudithub

dbaudithub | Event Hubs

Event Hubs Namespace

Search (Cmd+ /) Event Hub Refresh

Properties Locks

Entities

Event Hubs

Monitoring

Alerts

Name	Status	Message Retention	Partition Count
insights-logs-sqlsecurityauditevents	Active	1 day	4

ENABLING AZURE SQL AUDITING

sqlbits

jbdb (azure-sql-server-jb/jbdb) | Auditing

SQL database

Search (Cmd+/)

Save Discard View audit logs Feedback

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

View server settings

Server-level Auditing: Enabled

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

Turn on Microsoft Defender for SQL to receive security alerts upon suspicious events.

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



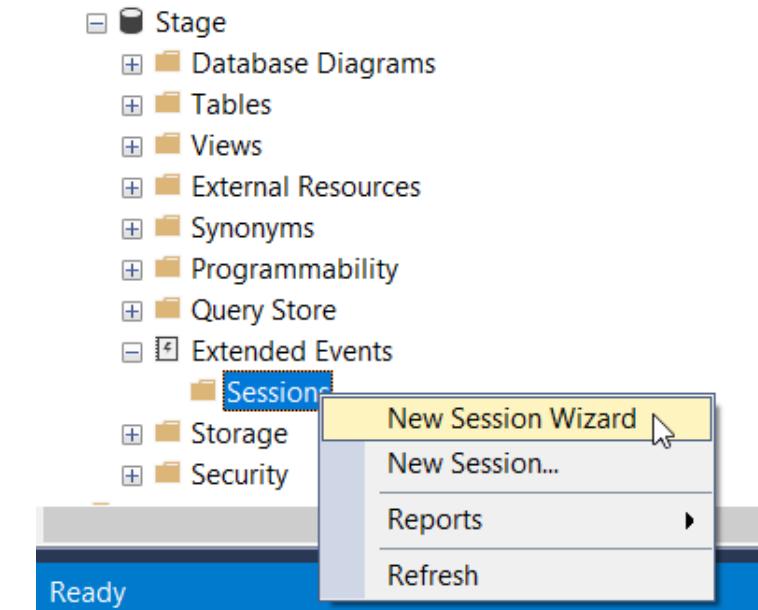
AZURE SQL AUDITING EXTENDED EVENTS

sqlbits

Script

```
CREATE EVENT SESSION [audit] ON DATABASE
ADD EVENT sqlserver.rpc_completed(
ACTION(sqlserver.client_app_name,sqlserver.client_hostname,
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_hostname,
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)
```

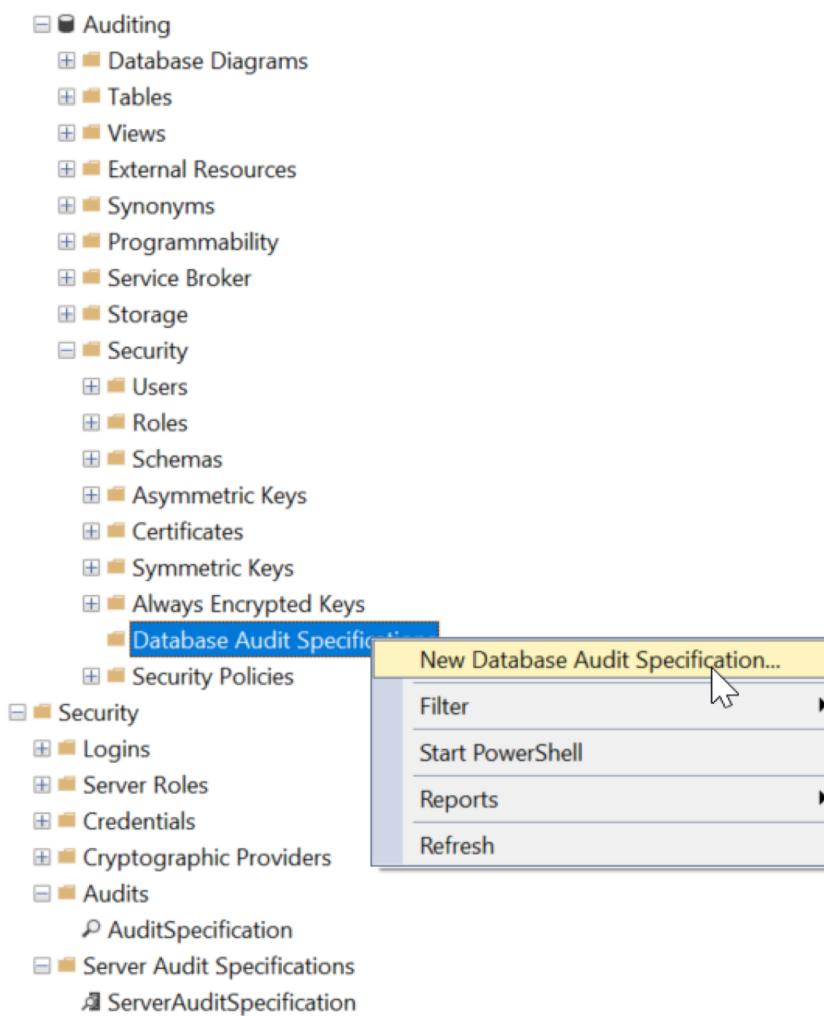
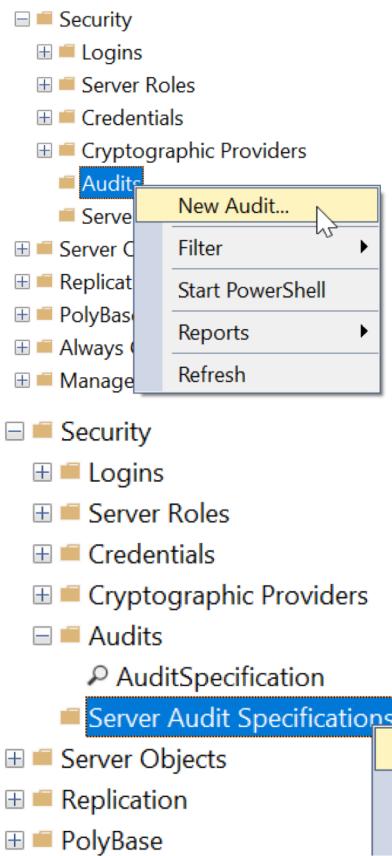
GUI



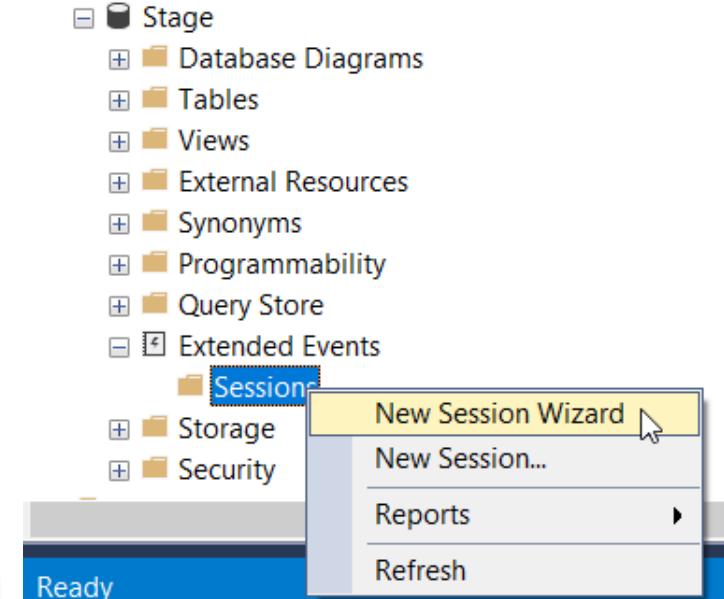
MANAGED INSTANCE AUDITING

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

sqlbits



<https://sqlb.it/?7194>



Thank
you!

THANK YOU FOR ATTENDING

Contact me @hellosqlkitty
or visit me at sqlkitty.com