



# HANDLE AZURE SQL AUDITING WITH EASE

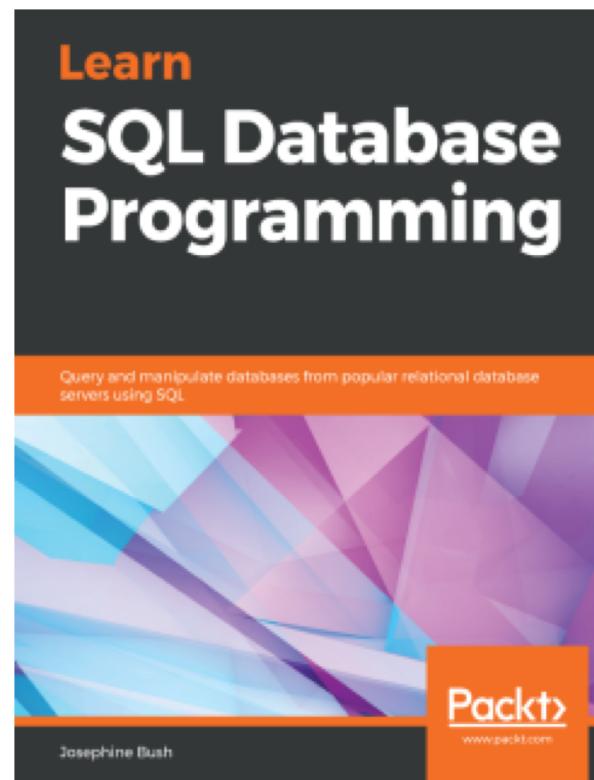
# ABOUT ME

**Josephine Bush**

10+ years DBA  
experience

MBA IT Management

MS Data Analytics



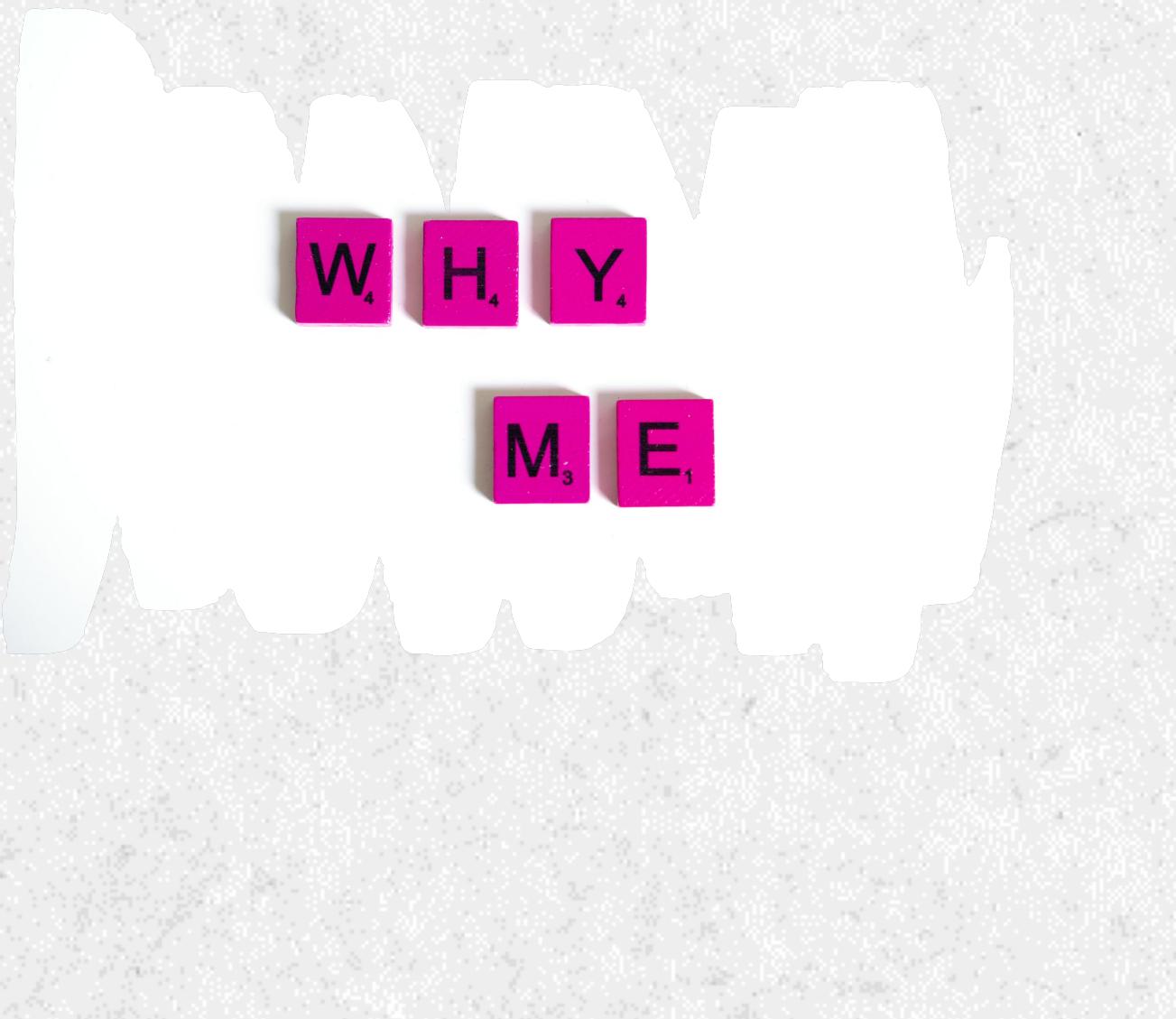
@hellosqlkitty  
[sqlkitty.com](http://sqlkitty.com)



# WHAT IS AUDITING?

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

Who broke this?

Who changed this?

Who used this?

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



# CLOUD SQL AUDITING OPTIONS

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

# 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 audit log in your Azure Storage account, Log Analytics workspace or Event Hub. [Learn more about Auditing of Microsoft support operations](#)



## 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

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) ⓘ



Storage access key ⓘ

Primary

Secondary

# AZURE SQL AUDITING STORAGE FILES

The screenshot shows the Azure Storage Blob container interface for 'sqldbauditlogs'. The left sidebar includes navigation links: Home, Overview (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, 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

## 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

database level

The screenshot illustrates the process of viewing audit logs for a database at the database level.

- 1** In the Azure portal, under the "Auditing" blade for the "auditingtest" database, the "View audit logs" button is highlighted with a red box.
- 2** After clicking "View audit logs", the audit records page is displayed. The "Log Analytics" button in the top right corner is highlighted with a red box.
- 3** Clicking "Log Analytics" opens a Jupyter Notebook interface showing a query for audit logs. The query is as follows:

```
1 AzureDiagnostics  
2 | where Category == 'SQLSecurityAuditEvents'  
3 | where ResourceId == '/SUBSCRIPTIONS/[REDACTED]/RESOURCEGROUPS/SQLAUDITING/PROVIDERS/MICROSOFT.SQL/SERVERS/JOSEPHINEBTTEST/DATABASES/MASTER' and database_name_s == 'auditingtest'  
4 | 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  
5 | order by event_time_t desc
```

The results table shows audit records for the last 24 hours. One record is visible:

event_time_t [UTC]	statement_s	succeeded_s	affected_rows_d	server_principal_name_s	client_ip_s	application_name_s	additional_information_s	data_sensitivity_information_s
2/22/2021, 11:21:36.019 PM	ALTER TABLE dbo.testing SET (LOCK_ESCALATION = TABLE)	true	0	josephine				6

# AZURE SQL AUDITING EVENT HUB

Enable Azure SQL Auditing ⓘ

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

Home > dbaudithub

dbaudithub | Event Hubs

Event Hubs Namespace

Search (Cmd+ /) Event Hub Refresh

Properties

Locks

Entities

Event Hubs

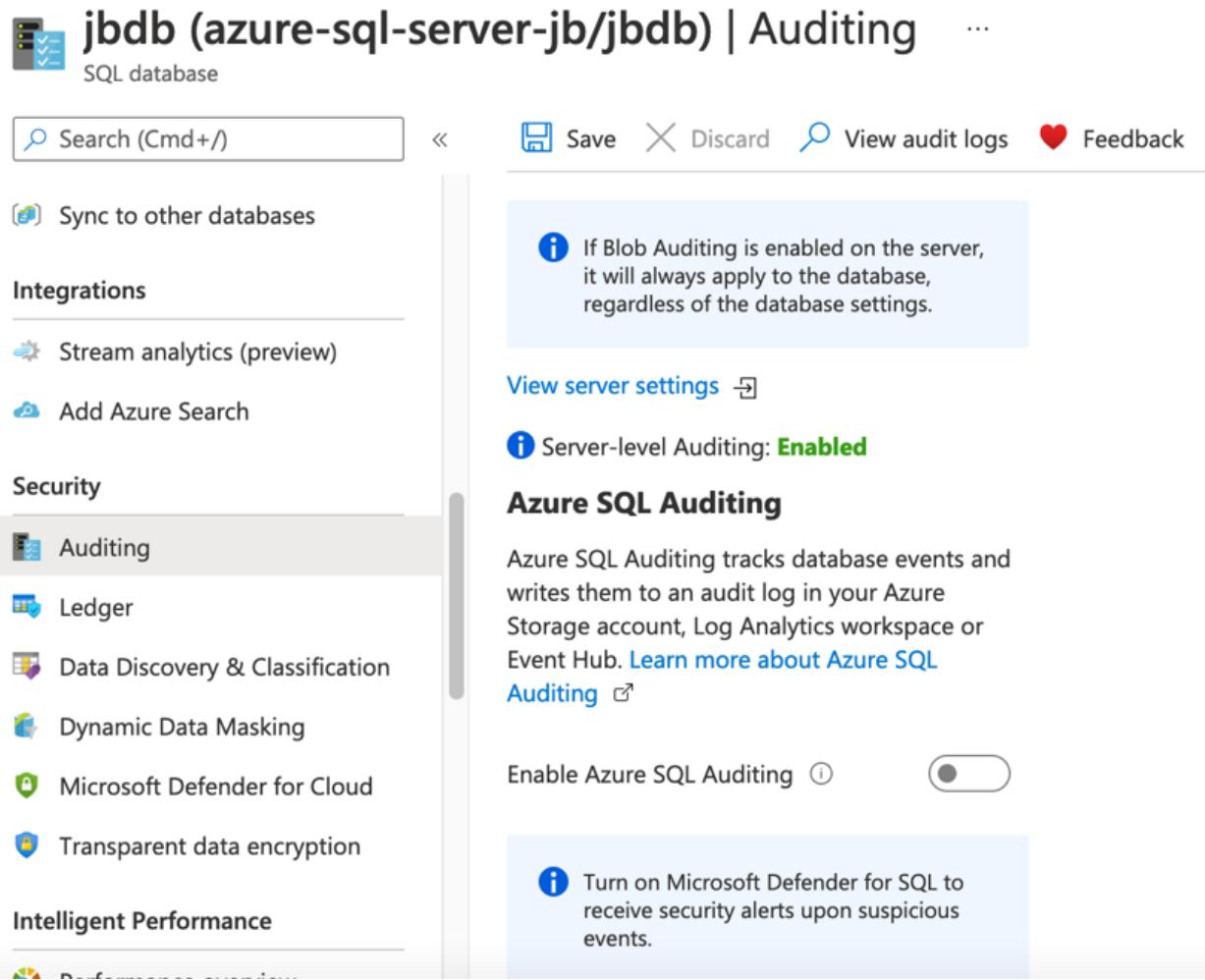
Monitoring

Alerts

Search to filter items...

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

# ENABLING AZURE SQL AUDITING



The screenshot shows the Azure portal interface for managing the 'jbdb' database. The left sidebar has a 'Security' section with 'Auditing' selected. The main content area is titled 'Auditing' and shows the following details:

- A note: "If Blob Auditing is enabled on the server, it will always apply to the database, regardless of the database settings."
- A link: "View server settings"
- A status: "Server-level Auditing: Enabled" (green)
- A section: "Azure SQL Auditing" with a description: "Azure SQL Auditing tracks database events and writes them to an audit log in your Azure Storage account, Log Analytics workspace or Event Hub." It includes a link: "Learn more about Azure SQL Auditing".
- An toggle switch: "Enable Azure SQL Auditing" which is turned off.
- A note: "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

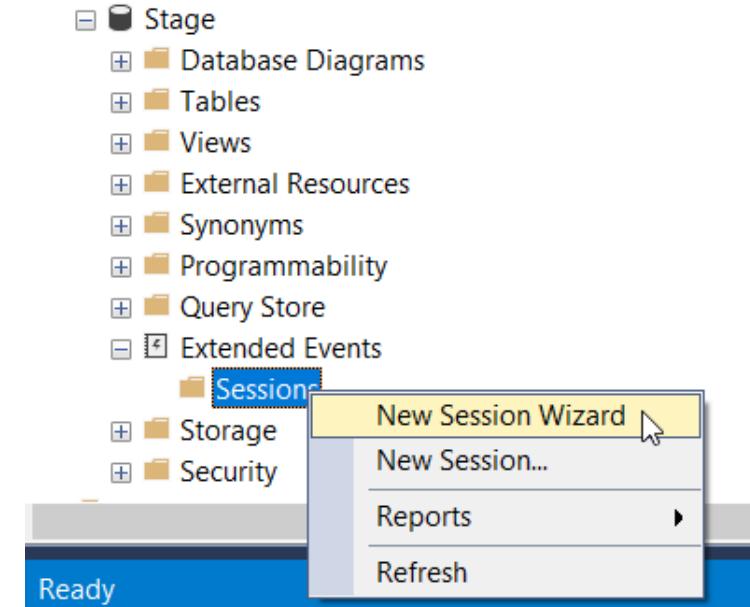
Don't do this if you already enabled at server level

# AZURE SQL AUDITING EXTENDED EVENTS

## Script

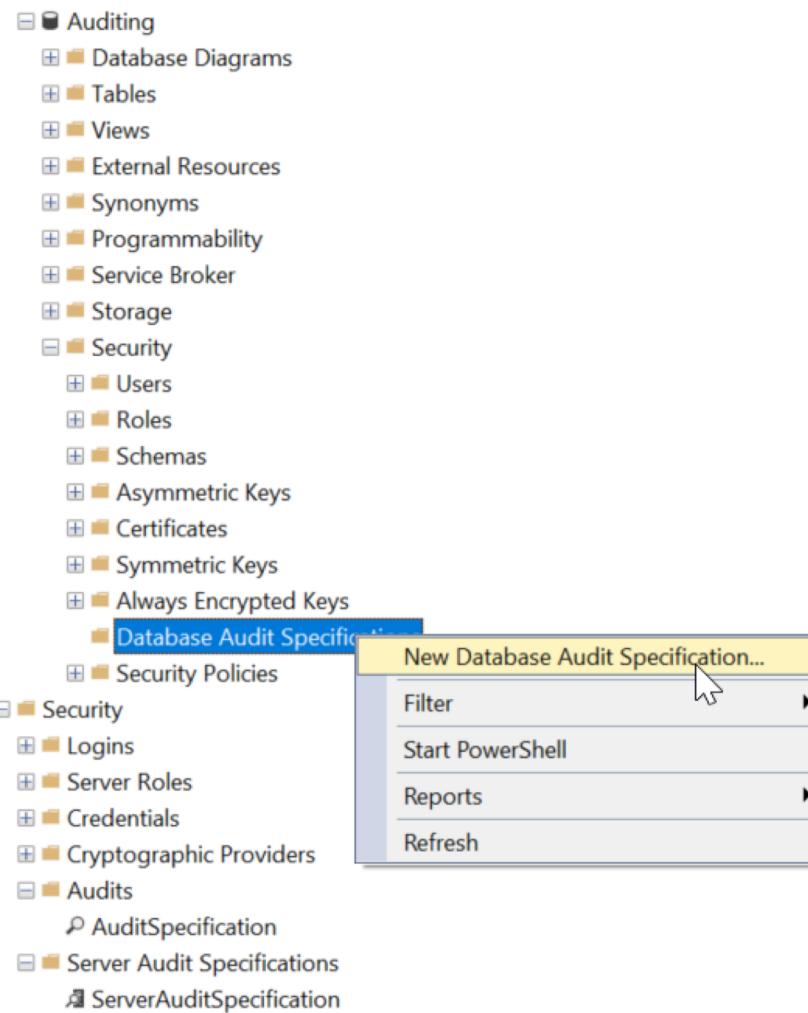
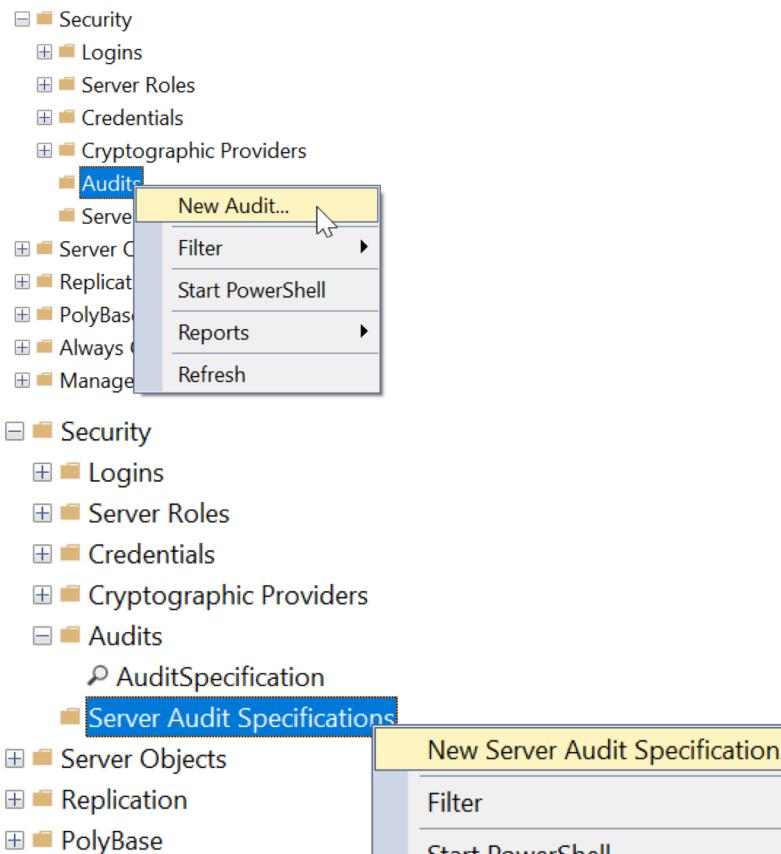
```
CREATE EVENT SESSION [audit] ON DATABASE
ADD EVENT sqlserver.rpc_completed(
ACTION(sqlserver.client_app_name,sqlserver.client_hostname,
sqlserver.database_name,sqlserver.sql_text,sqlserver.username)
      WHERE ([sqlserver].[username]=N'josephine')),
ADD EVENT sqlserver.sql_batch_completed(
ACTION(sqlserver.client_app_name,sqlserver.client_hostname,
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

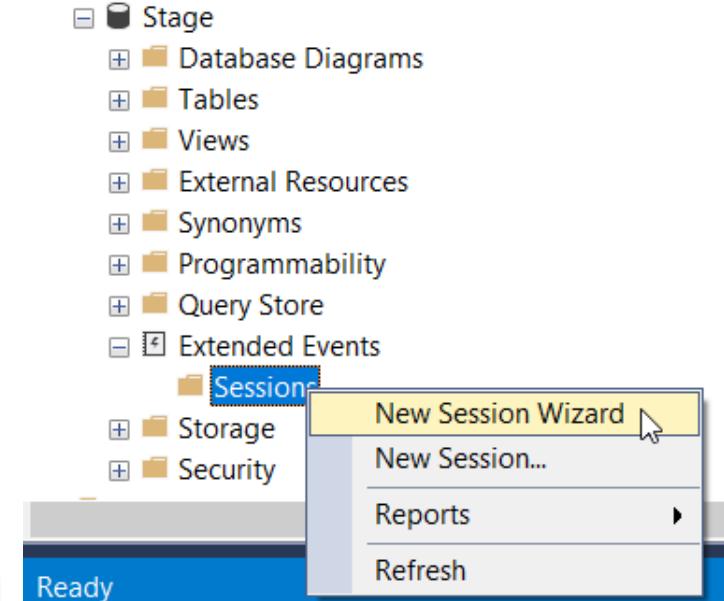


# MANAGED INSTANCE AUDITING

## SQL Server Audit



## Extended Events



# RESOURCES

## Azure SQL Audit Overview

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

## Azure SQL Extended Events

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

## Azure SQL Managed Instance Auditing

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

## 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/>



Thank  
you!

# THANK YOU FOR ATTENDING

---

Contact me @hellosqlkitty  
or visit me at [sqlkitty.com](http://sqlkitty.com)