



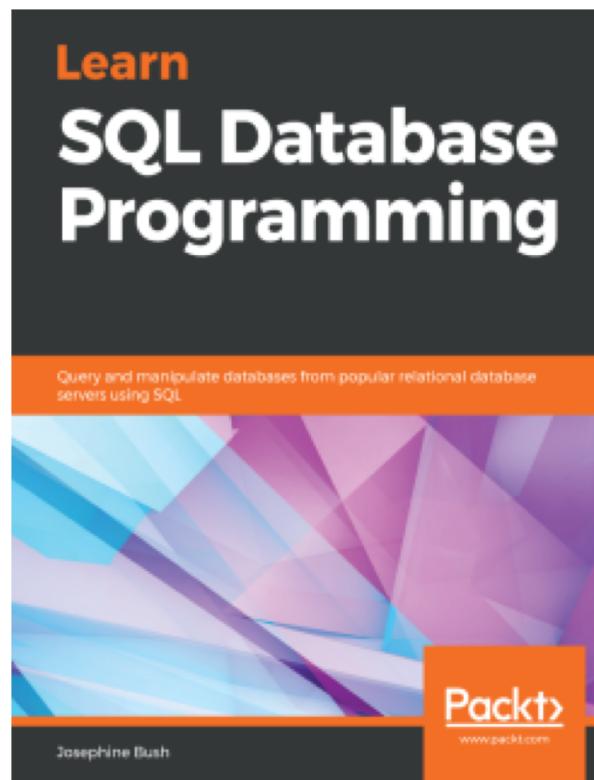
HANDLE AZURE SQL
AUDITING WITH EASE

ABOUT ME

Josephine Bush

10+ years DBA
experience

MBA IT Management
MS Data Analytics



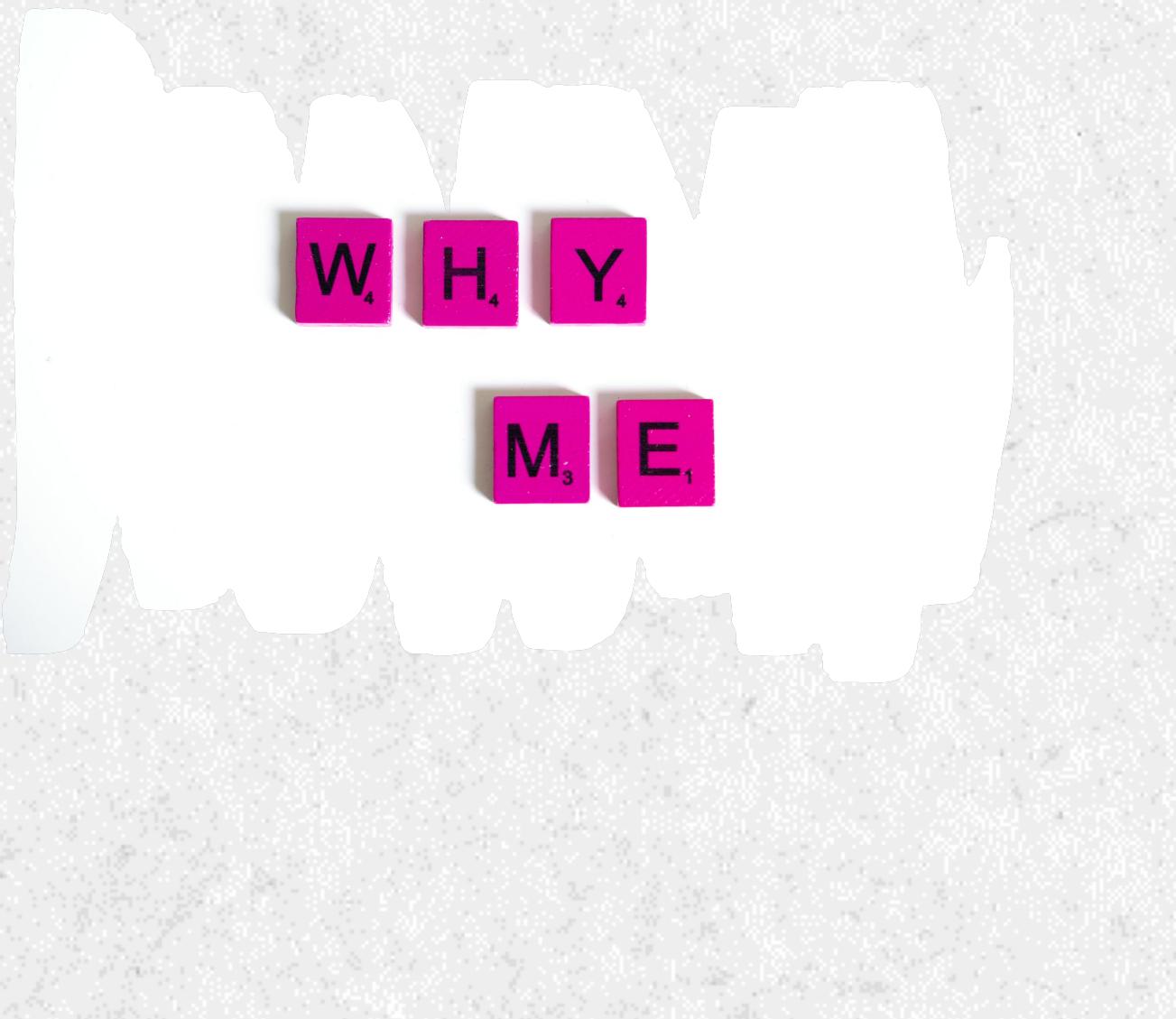
@hellosqlkitty
sqlkitty.com



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

AZURE SQL AUDITING POLICY

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

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

GET AZURE SQL AUDITING POLICY

To get your current auditing policy:

Get-AzSqlServerAudit -ResourceGroupName
'dbops' -Servername 'jbauditing'

```
No results found.  
PS /home/josephine> Get-AzSqlServerAudit -ResourceGroupName 'dbops' -Servername 'jbauditing'  
  
PropertyName : jbauditing  
AuditActionGroup : {SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP, FAILED_DATABASE_AUTHENTICATION_GROUP,  
                      BATCH_COMPLETED_GROUP}  
  
PredicateExpression :  
StorageKeyType : None  
RetentionInDays :  
ResourceGroupName : dbops  
BlobStorageTargetState : Disabled  
StorageAccountResourceId :  
EventHubTargetState : Disabled  
EventHubName :  
EventHubAuthorizationRuleResourceId :  
LogAnalyticsTargetState : Enabled  
WorkspaceResourceId : /subscriptions/bdb84ae3-c42a-4250-9373-07525796c375/resourcegroups/dbops/providers/microsoft.operationalinsights/workspaces/dbauditdata
```

AZURE SQL AUDIT ACTION GROUPS

If you are used to SQL Server Audit, some of these audit action groups are the same and some are not

| | |
|------------------|---|
| Type: | AuditActionGroups[] |
| 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, LEDGER_OPERATION_GROUP, DBCC_GROUP, DATABASE_OWNERSHIP_CHANGE_GROUP, DATABASE_CHANGE_GROUP |

SET AZURE SQL AUDITING POLICY

To change your current auditing policy:

```
Set-AzSqlServerAudit -ResourceGroupName 'dbops' -ServerName 'jbauditing' `  
-AuditActionGroup APPLICATION_ROLE_CHANGE_PASSWORD_GROUP,  
DATABASE_CHANGE_GROUP, `  
DATABASE_OBJECT_CHANGE_GROUP, DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP, `  
DATABASE_OBJECT_PERMISSION_CHANGE_GROUP, DATABASE_OWNERSHIP_CHANGE_GROUP, `  
DATABASE_PERMISSION_CHANGE_GROUP, DATABASE_PRINCIPAL_CHANGE_GROUP, `  
DATABASE_PRINCIPAL_IMPERSONATION_GROUP, DATABASE_ROLE_MEMBER_CHANGE_GROUP, `  
SCHEMA_OBJECT_CHANGE_GROUP, SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP, `  
SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP, USER_CHANGE_PASSWORD_GROUP
```

```
PS /home/josephine> Get-AzSqlServerAudit -ResourceGroupName 'dbops' -Servername 'jbauditing'  
  
  PropertyName : jbauditing  
  AuditActionGroup : {APPLICATION_ROLE_CHANGE_PASSWORD_GROUP, DATABASE_CHANGE_GROUP,  
                      DATABASE_OBJECT_CHANGE_GROUP, DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP...}  
  PredicateExpression :  
  StorageKeyType : None
```

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 18_39_10_366_0.xls, 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 |
|--------------------|-------------------------|-------------|-------------|---------|-------------|
| 18_39_10_366_0.xls | 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

View audit data at the database level

auditingtest (josephinebtest/auditingtest) | Auditing
SQL database

1

Search (Ctrl+ /)

Save Discard View audit logs Feedback

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

Logs JBSQLAuditing

New Query 1*

Run Time range : Last 24 hours Save Copy link New alert rule Export Pin to dashboard Format query

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

Feedback Queries Query explorer

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 | c |
|----------------------------|--|-------------|-----------------|-------------------------|---|
| 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

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

Feedback Queries Query explorer

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 | c |
|----------------------------|--|-------------|-----------------|-------------------------|---|
| 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 |

VIEW LOG ANALYTICS WORKSPACE

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 |
| Internal | 54 |

DISTRIBUTION BY IP

IP Address

2

| IP Address | Count |
|------------|-------|
| 67.: | 174 |
| Internal | 6 |

QUERY LOG ANALYTICS AUDITING DATA

Go to your log analytics workspace
Click Logs and run a Kusto query

You may need to filter on this if
you are seeing a lot of entries for
this user:

and server_principal_name_s !=
'NT AUTHORITY\\SYSTEM'

```
AzureDiagnostics
| where Category == 'SQLSecurityAuditEvents'
and TimeGenerated > ago(1d)
| project
event_time_t,
database_name_s,
statement_s,
server_principal_name_s,
succeeded_s,
client_ip_s,
application_name_s,
additional_information_s,
data_sensitivity_information_s
| order by event_time_t desc
```

VIEW LOG ANALYTICS AUDITING DATA

Home > Log Analytics workspaces > dbauditdata

dbauditdata | Logs Log Analytics workspace

Search (Cmd+/) <> New Query 1* + Feedback Queries ...

Computer Groups Data Export Linked storage accounts Network Isolation

General Workspace summary Workbooks Logs Solutions Usage and estimated costs Properties Service Map

Workspace Data Sources Virtual machines

New Query 1* Select scope Run Time range : Set in query Save Share New alert rule Export

```
1 AzureDiagnostics
2 | where Category == 'SQLSecurityAuditEvents'
3 | where TimeGenerated > ago(1d)
4 | project
5     event_time_t,
6     database_name_s,
7     statement_s,
8     server_principal_name_s,
9     succeeded_s,
10    client_ip_s,
11    application_name_s,
12    additional_information_s,
13    data_sensitivity_information_s
14 | order by event_time_t desc
15
```

Results Chart

| event_time_t [UTC] | database_name_s | statement_s | server_principal_name_s | succeeded_s |
|-----------------------------|-----------------|---|-------------------------|-------------|
| > 4/20/2022, 8:26:07.287 PM | jbdb | exec sp_executesql N'SELECT clmns.column_id AS [ID],... | azureadmin | true |
| > 4/20/2022, 8:26:06.146 PM | jbdb | SELECT satypes.name AS [Schema], atypes.name AS [...] | azureadmin | true |
| > 4/20/2022, 8:26:06.068 PM | jbdb | SELECT SCHEMA_NAME(tt.schema_id) AS [Schema], tt... | azureadmin | true |
| > 4/20/2022, 8:26:05.990 PM | jbdb | SELECT sst.name AS [Schema], st.name AS [Name] FR... | azureadmin | true |

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

The screenshot shows the Azure portal interface for managing Event Hubs. The top navigation bar includes 'Home > dbaudithub'. The main title is 'dbaudithub | Event Hubs' with a subtitle 'Event Hubs Namespace'. On the left, a sidebar lists 'Properties', 'Locks', 'Entities' (selected), 'Event Hubs' (selected), and 'Monitoring' (with 'Alerts'). The main content area has a search bar 'Search (Cmd+)/' and a 'Refresh' button. A table displays the following data:

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

ENABLING AZURE SQL AUDITING

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

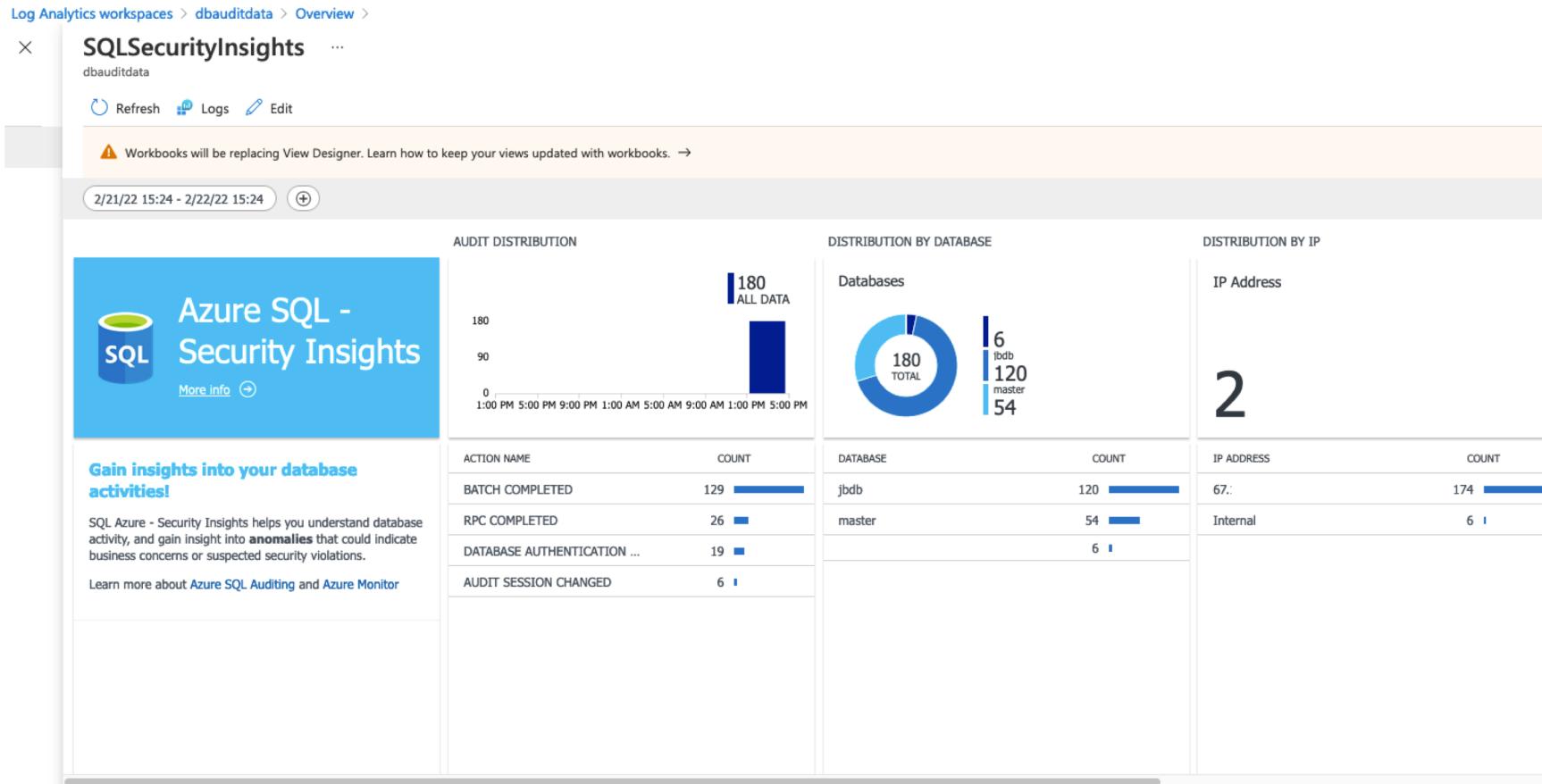
Don't do this if you already enabled at server level

AZURE SQL AUDITING DEMO



CENTRALIZING AUDITING DATA

Store Azure SQL audit data in the same log analytics workspace



REPORTING ON AUDITING DATA

Home > auditreport

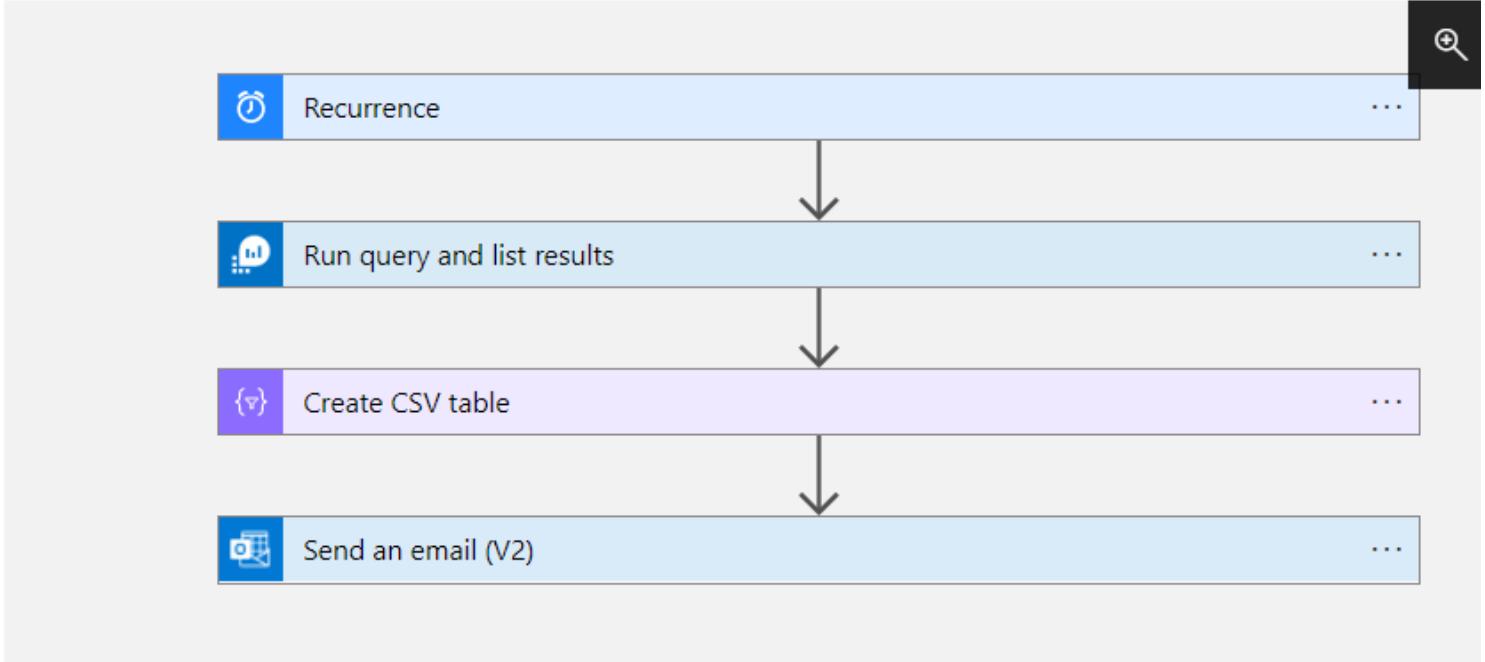
 auditreport | Logic app designer ...

Logic app

Search (Ctrl+ /) Save Discard Run Trigger Designer Code view Parameters Templates Connect

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

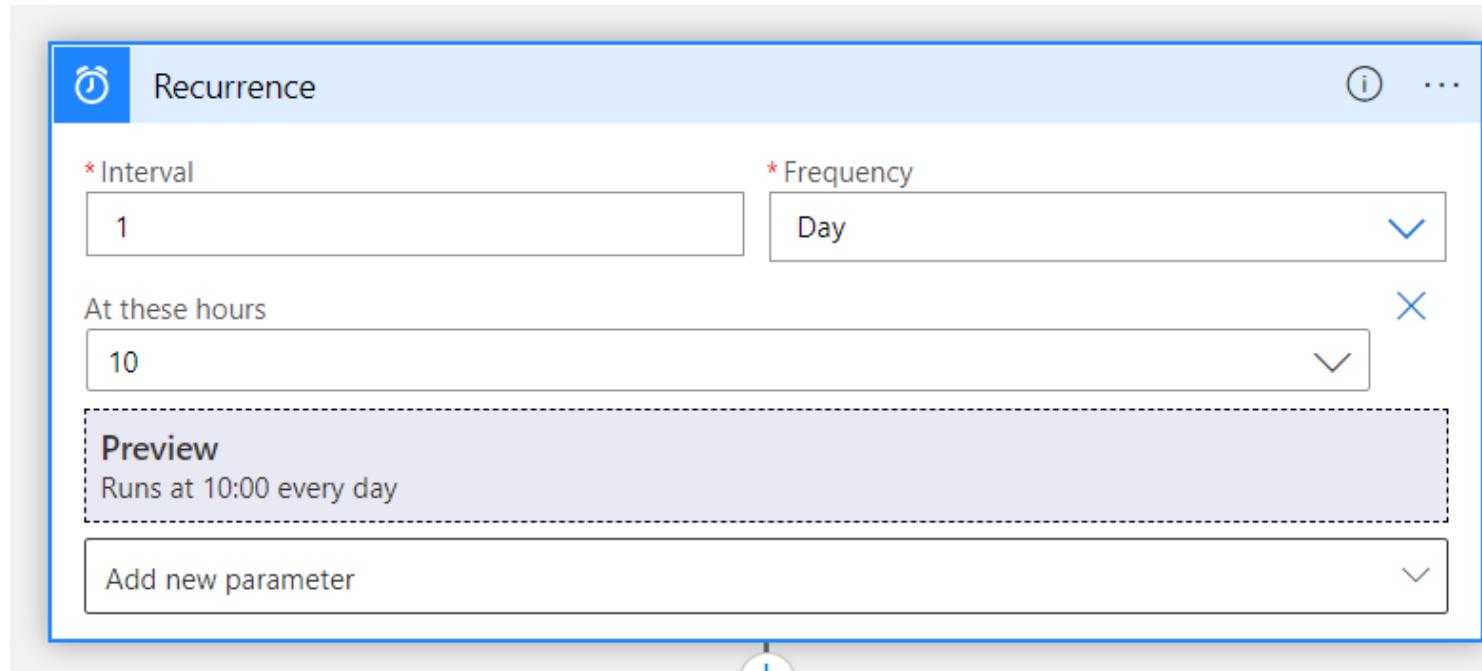
Development Tools Logic app designer Logic app code view Versions API connections



```
graph TD; Recurrence[Recurrence] --> RunQuery[Run query and list results]; RunQuery --> CreateTable[Create CSV table]; CreateTable --> SendEmail[Send an email (V2)]
```

SETUP LOGIC APP - RECURRENCE

Setup a schedule with Recurrence step



SETUP LOGIC APP –KUSTO QUERY

Setup a Run query and list results step with your kusto query

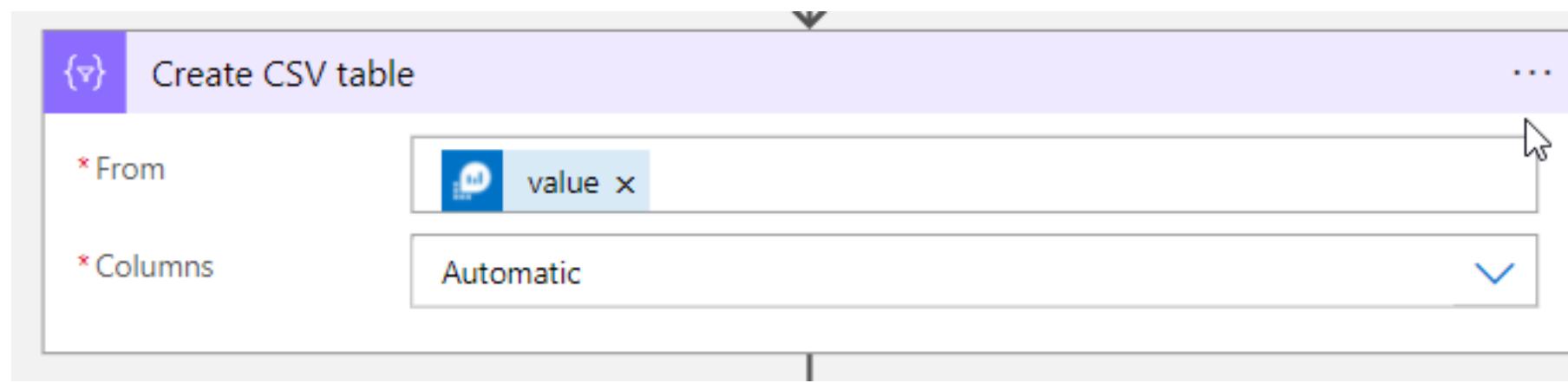
The screenshot shows the configuration for a 'Run query and list results' step in a Logic App. The step has the following settings:

- Subscription:** tenant
- Resource Group:** dbops
- Resource Type:** Log Analytics Workspace
- Resource Name:** dbauditdata
- Query:**

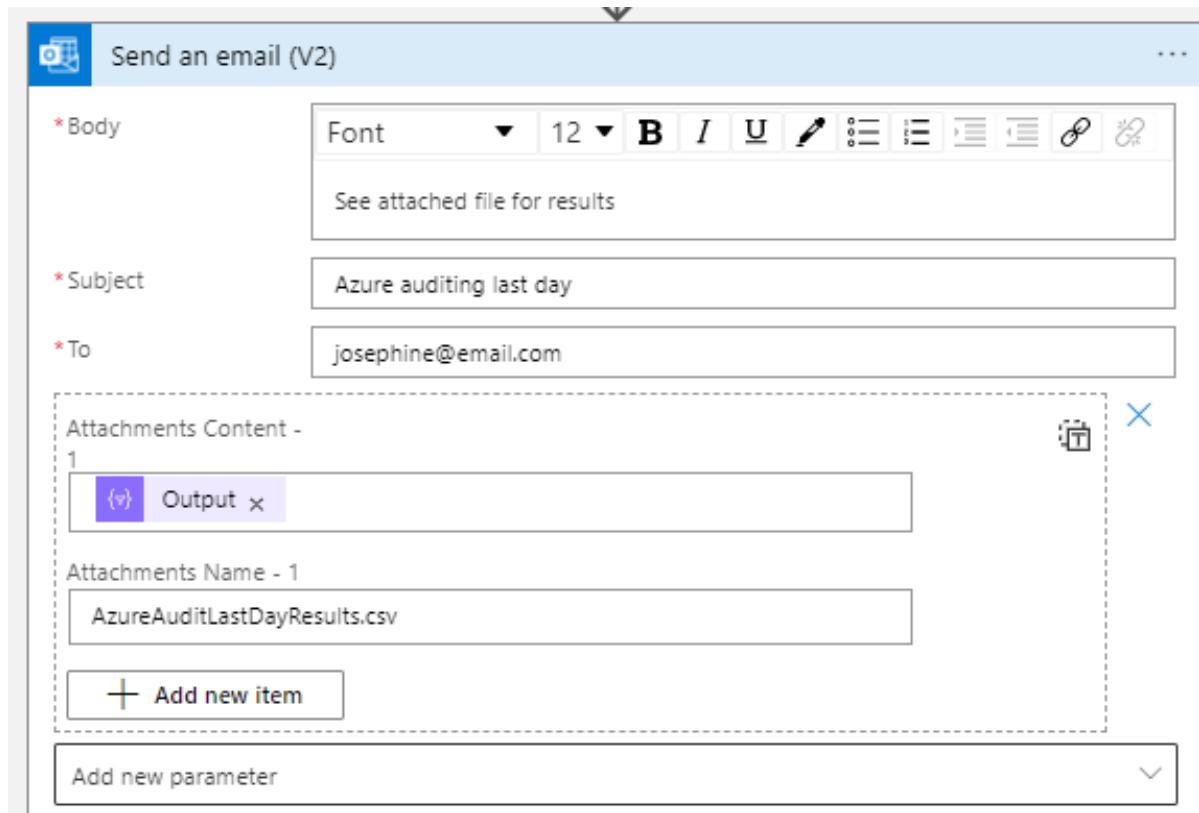
```
AzureDiagnostics  
| where Category == 'SQLSecurityAuditEvents'  
| where TimeGenerated > ago(1d)  
| project  
    event_time_t,  
    database_name_s,  
    statement_s,  
    server_principal_name_s,  
    succeeded_s,  
    client_ip_s,  
    application_name_s,  
    additional_information_s,  
    data_sensitivity_information_s  
| order by event_time_t desc
```
- Time Range:** Last 24 hours

SETUP LOGIC APP – CSV FILE

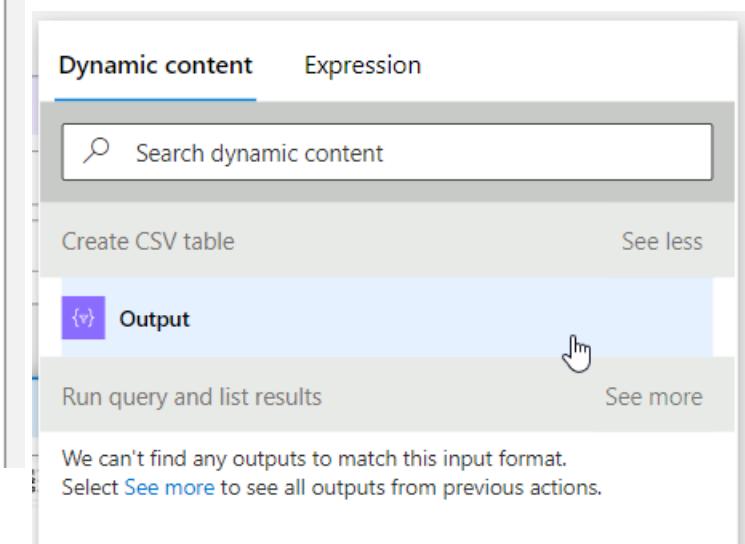
Create CSV table step to create a CSV file attachment



SETUP LOGIC APP – SEND EMAIL



Setup an Outlook Send an Email step to send an email with the CSV attachment

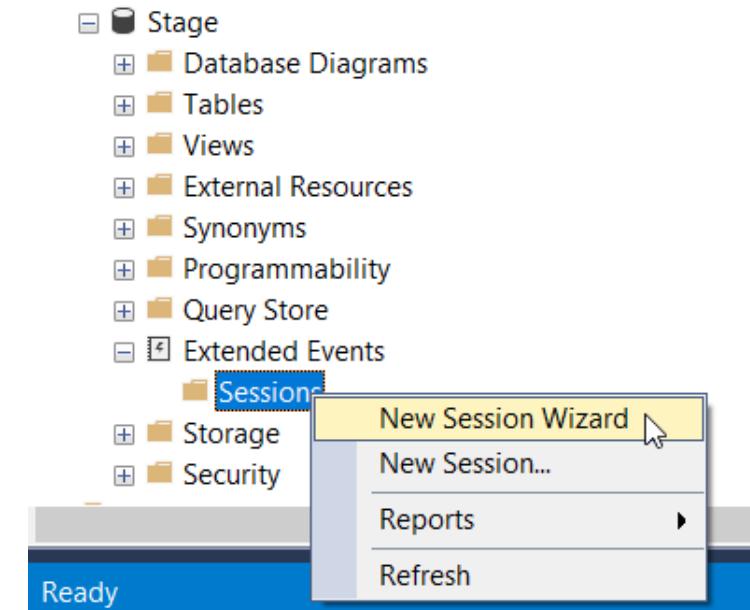


AZURE SQL AUDITING EXTENDED EVENTS

Script

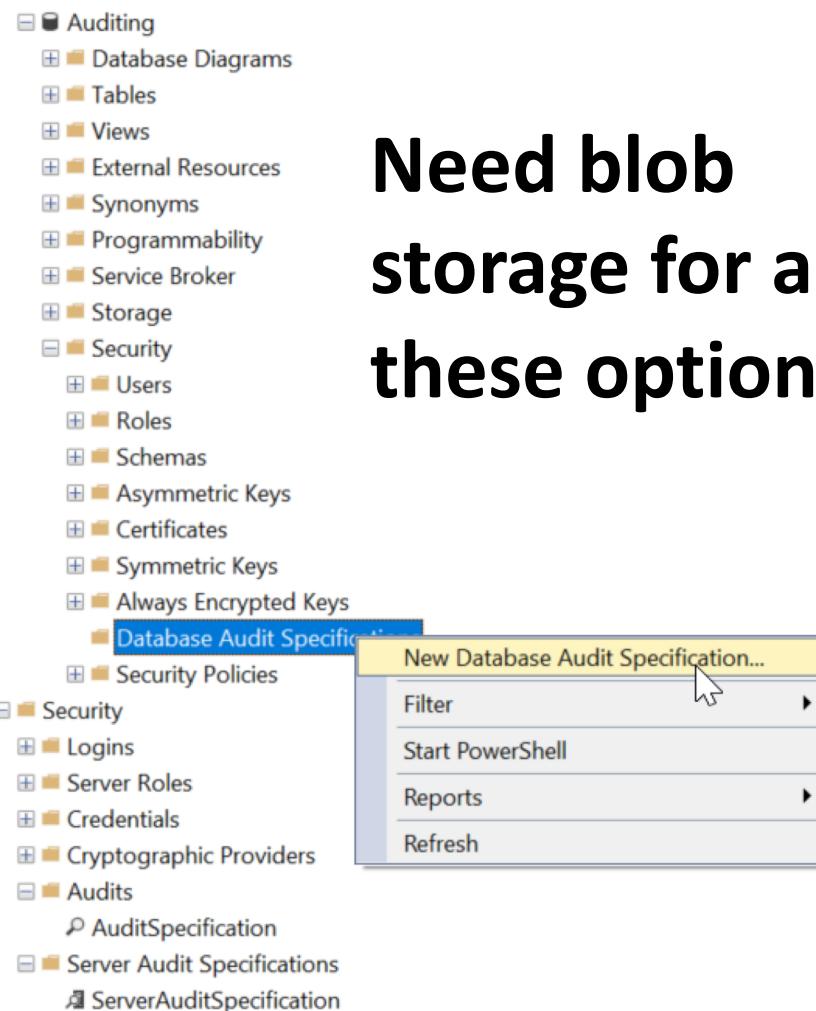
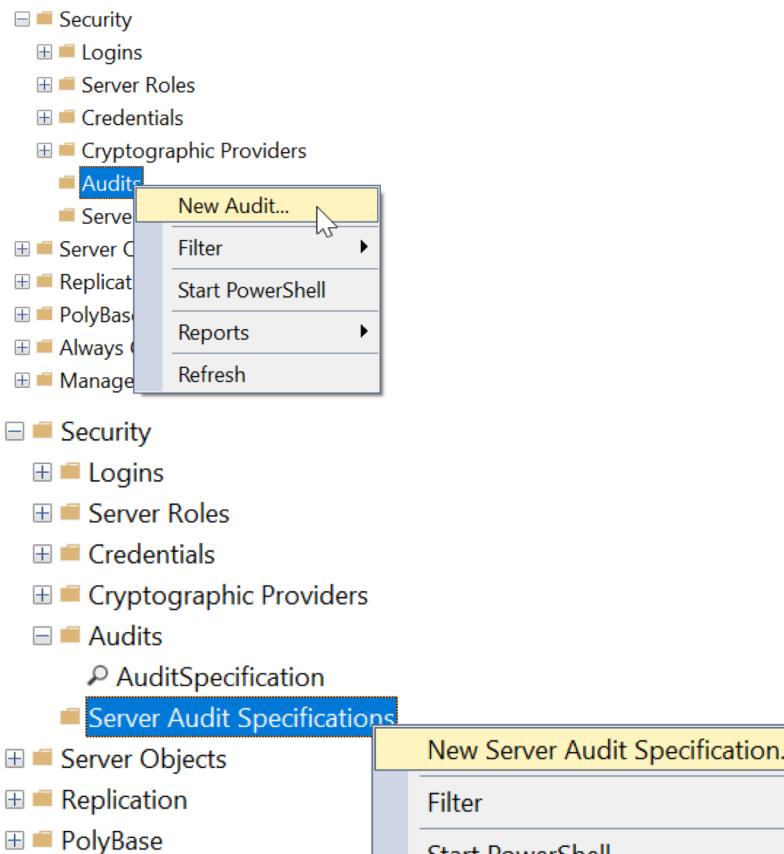
```
CREATE EVENT SESSION [audit] ON DATABASE
ADD EVENT sqlserver.rpc_completed(
ACTION(sqlserver.client_app_name,sqlserver.client_hostname,
sqlserver.database_name,sqlserver.sql_text,sqlserver.username)
      WHERE ([sqlserver].[username]=N'josephine')),
ADD EVENT sqlserver.sql_batch_completed(
ACTION(sqlserver.client_app_name,sqlserver.client_hostname,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



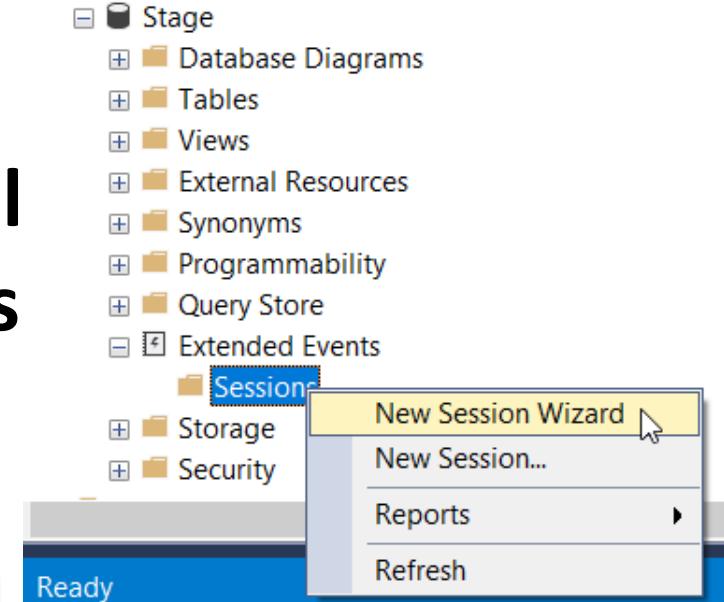
MANAGED INSTANCE AUDITING

SQL Server Audit



Need blob storage for all these options

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/>

Create Azure Logic Apps in the Azure portal

<https://docs.microsoft.com/en-us/azure/logic-apps/quickstart-create-first-logic-app-workflow>

Get started with log queries in Azure Monitor

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries>

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>

Azure SQL Create or Update Database Auditing Policy

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



Thank
you!

THANK YOU FOR ATTENDING

Contact me @hellosqlkitty
or visit me at sqlkitty.com