



HANDLE AZURE SQL AUDITING WITH EASE

Josephine Bush

She/Hers

DBA, MBA, Author



ABOUT ME

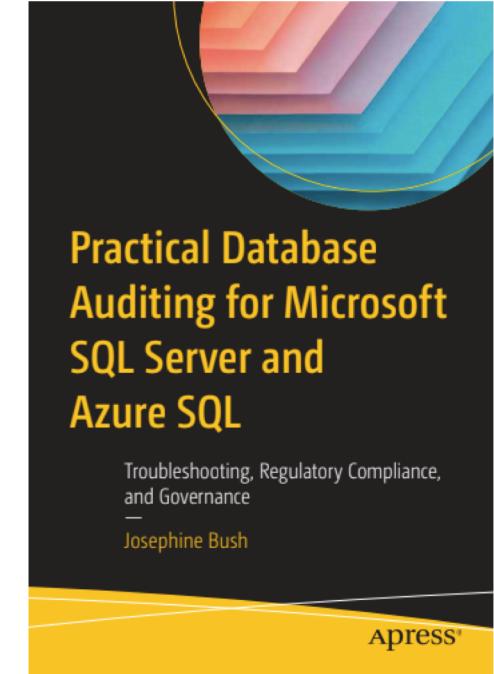


Josephine Bush

10+ years DBA
experience

MBA IT Management

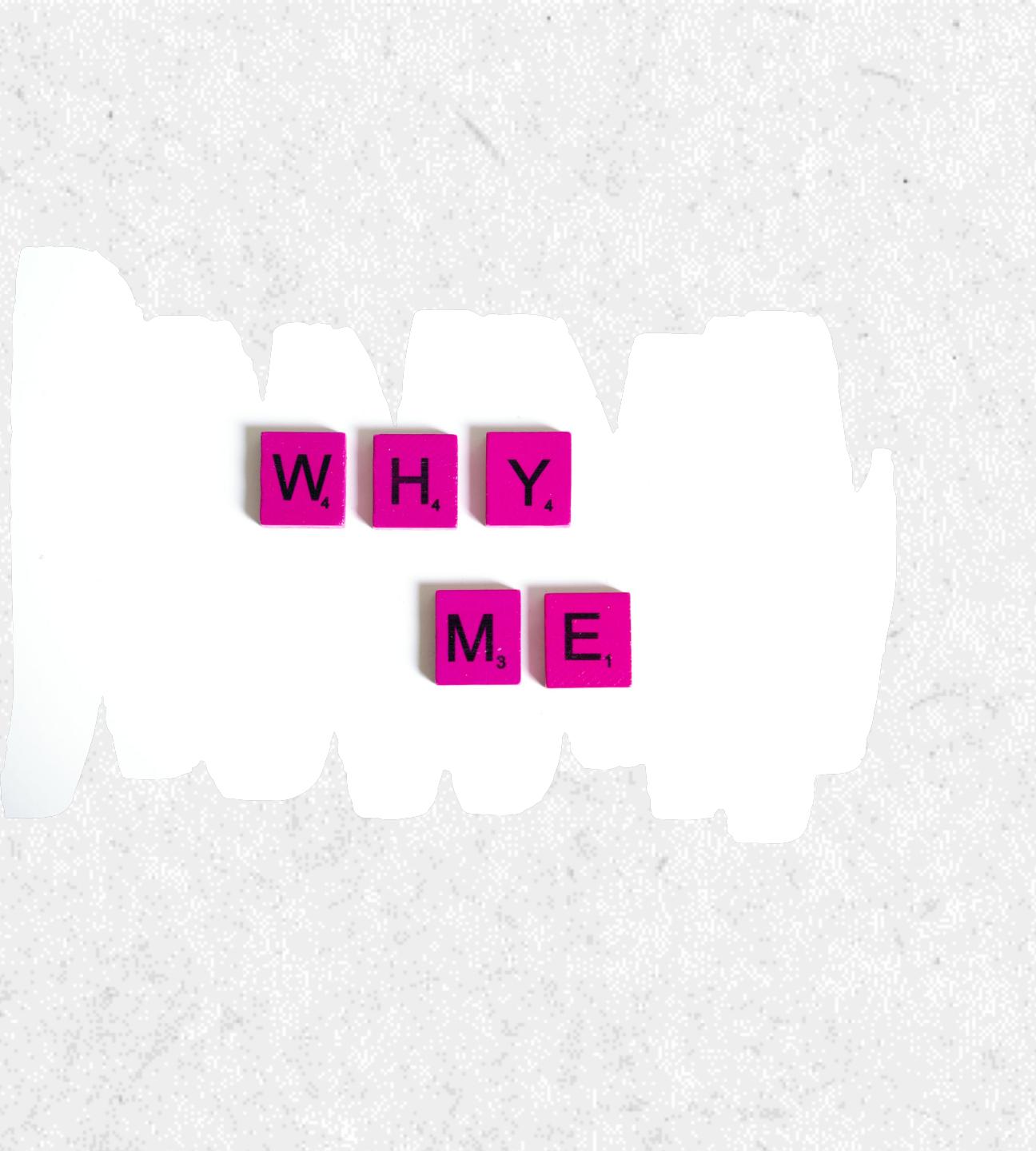
MS Data Analytics



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:	<p>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</p>

SET AZURE SQL AUDITING POLICY

To change your current auditing policy:

```
Set-AzSqlServerAudit -ResourceGroupName 'dbops' -ServerName 'auditingtest' `  
-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](#)

Enable Auditing of Microsoft support operations 

Use different audit log destinations 

- 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](#)



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) i

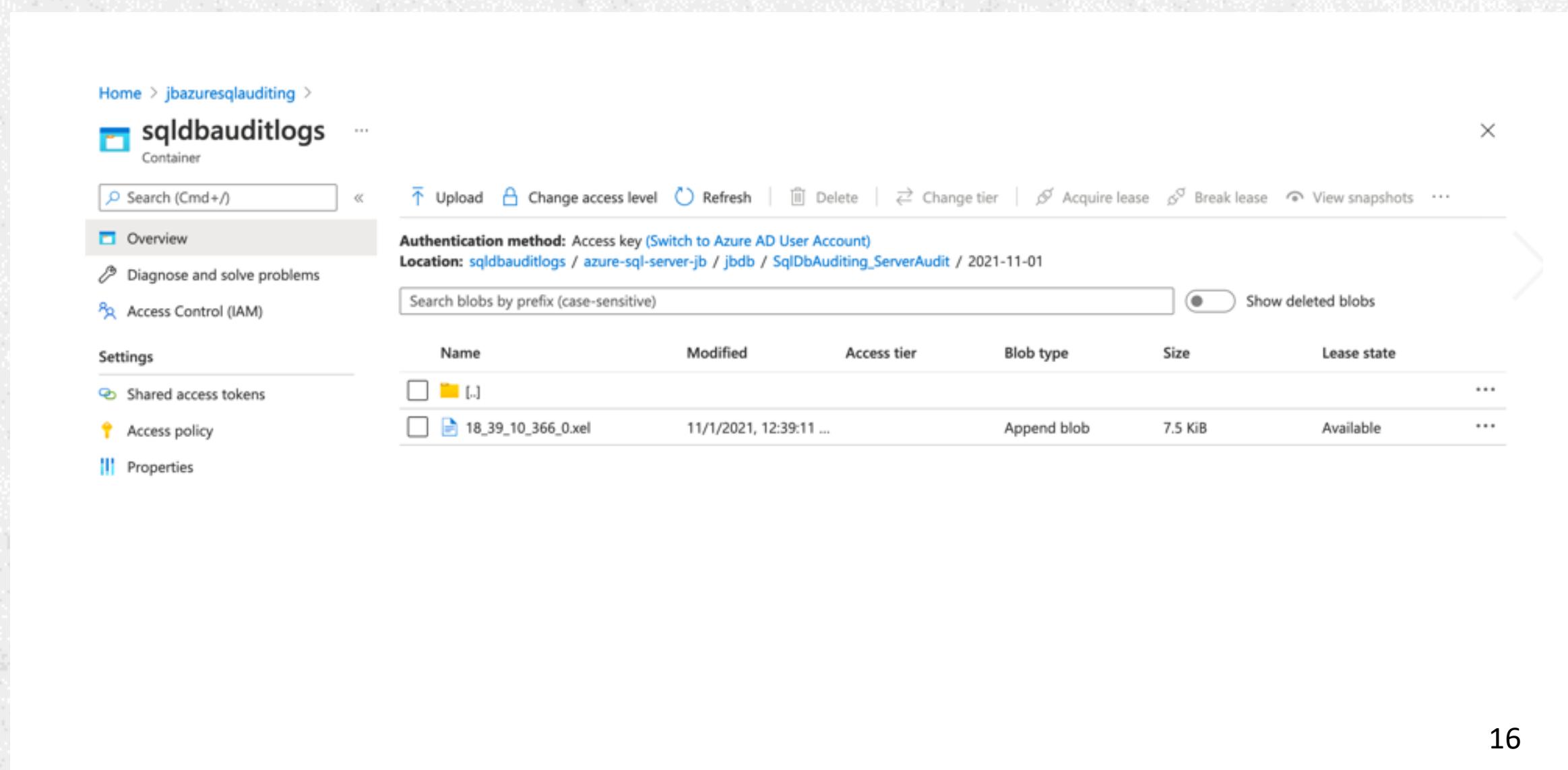
 0

Storage access key i

Primary

Secondary

AZURE SQL AUDITING STORAGE FILES



The screenshot shows the Azure Storage Blob container 'sqldbauditlogs'. The container is a 'Container' type with an 'Access key' authentication method. It is located at 'sqldbauditlogs / azure-sql-server-jb / jbdb / SqIDbAuditing_ServerAudit / 2021-11-01'. The 'Overview' tab is selected. A search bar at the top allows searching by blob prefix. A 'Show deleted blobs' toggle switch is present. The main table lists one blob named '18_39_10_366_0.xls' which is an 'Append blob' of size 7.5 KiB and is 'Available'. The table columns are Name, Modified, Access tier, Blob type, Size, and Lease state.

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 EVENT HUB

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 

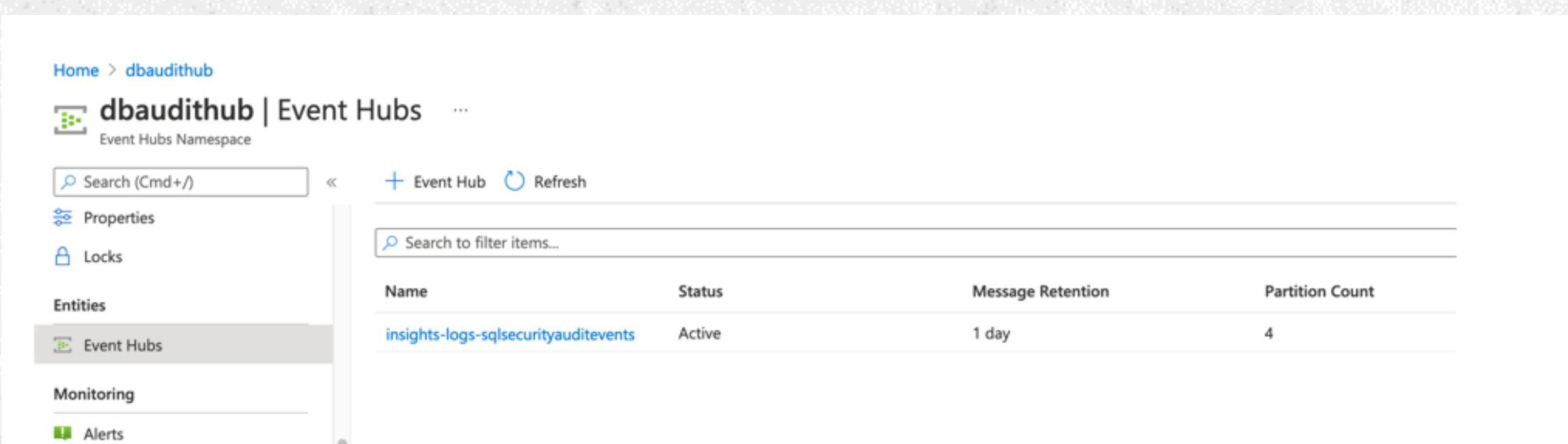
Event hub name (optional)

(Create in selected namespace) 

Event hub policy name *

RootManageSharedAccessKey 

AZURE SQL AUDITING EVENT HUB DATA



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

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) 

AZURE LOG ANALYTICS PRICING

Ingesting data

Region: Currency:

Pricing Tier	Price	Effective Per GB Price ¹	Savings Over Pay-As-You-Go
Pay-As-You-Go	\$2.76 per GB <small>(5 GB per billing account per month included)</small>	\$2.76 per GB	N/A
100 GB per day	\$196 per day	\$1.96 per GB	29%

Retaining data

Region: Currency:

Feature	Days of Included Retention	Price
Data Retention	31 days (or 90 days if Sentinel is enabled), and 90 days for Application Insights data	\$0.12 per GB per month

AZURE LOG ANALYTICS COSTS

Home > Log Analytics workspaces > dbaudit

dbaudit | Usage and estimated costs S Log Analytics workspace

Search (Cmd+/) Usage details Insights Daily cap Data Retention Help

General

- Tables (preview)
- Workspace summary
- Workbooks
- Logs
- Solutions
- Usage and estimated costs**
- Properties
- Service Map

Workspace Data Sources

- Virtual machines
- Storage accounts logs
- System Center
- Azure Activity log
- Scope Configurations (Preview)

Related Resources

- Automation Account

Your Log Analytics cost depends on your choice of pricing tier, data retention and which solutions are used. Here you can see the estimated monthly cost for each of the available pricing tiers, based on your last 31-days of Log Analytics data ingested. These cost estimates can be used to help you select the best pricing tier based on your data ingestion patterns. These estimates include the 500MB/VM/day data allowances if you are using Microsoft Defender. This page does not reflect your actual billed usage. To view that, use Cost Management ([learn more](#)). If you have questions about using this page, [contact us](#). Learn more about [Log Analytics pricing](#).

Pricing Tiers

Pay-as-you-go Recommended Tier Per GB

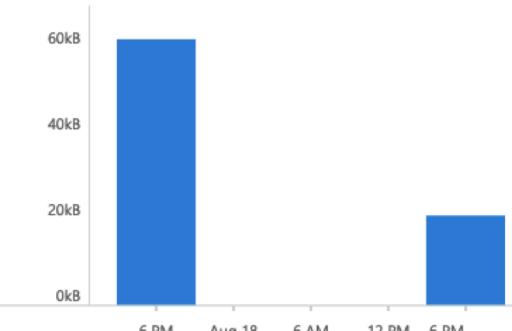
The Pay-as-you-go pricing tier offers flexible consumption pricing in which you are charged per GB of data ingested. There are additional charges if you increase the data retention above the 31 day included retention (or 90 day included retention if using Sentinel on this workspace). Learn more about [Log Analytics pricing](#).

Estimated costs

Item type	Price	Monthly usage (last 31 days)	Estimated monthly cost
Log data ingestion	\$2.76	0.00 GB	\$0.00
Microsoft Defender allowance	\$0.00	0.00 GB	\$0.00
Log data retention (beyond 31 days)	\$0.12	0.00 GB	\$0.00
Total			\$0.00

Usage Charts

Billable data ingestion per solution (last 31 days)

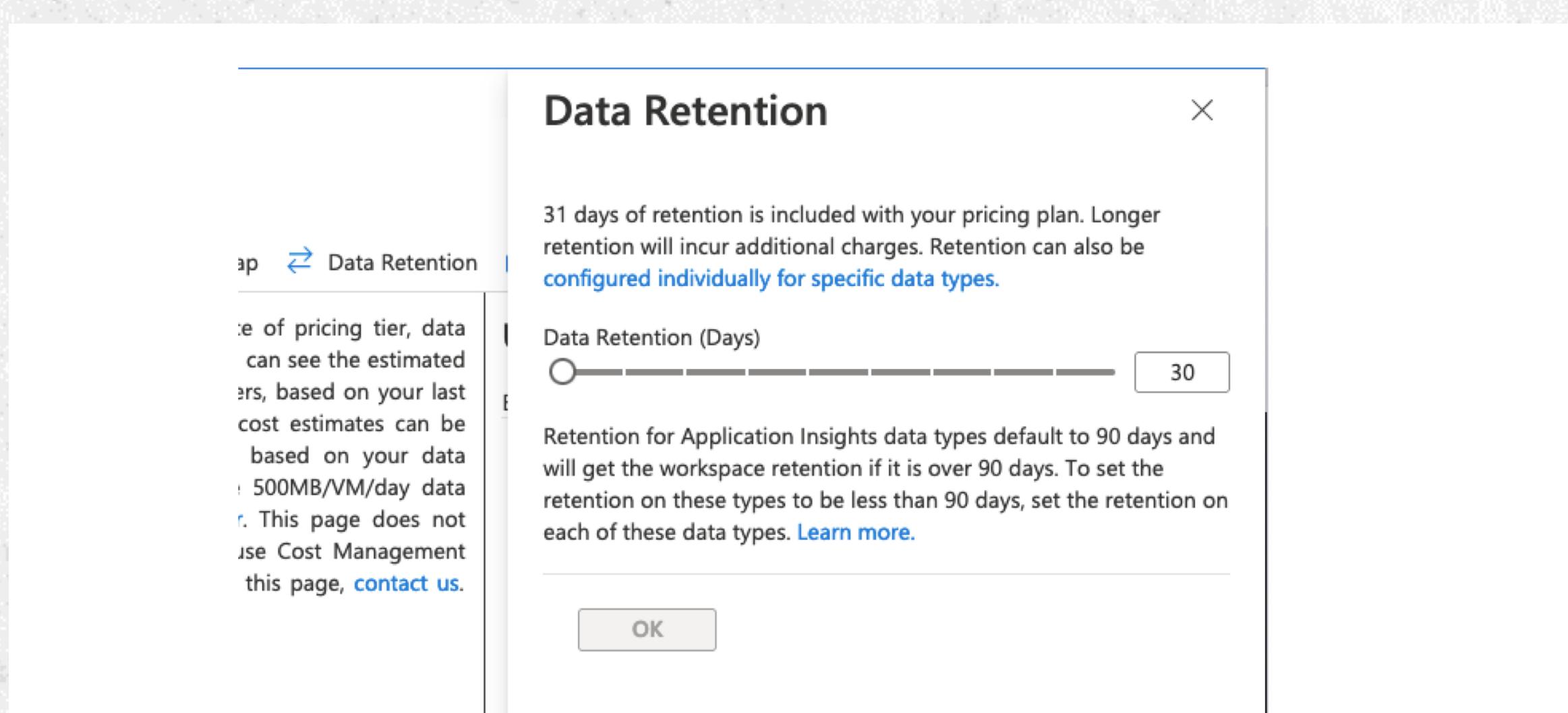


Date	Usage (kB)
Aug 18 6 PM	~60kB
Aug 19 6 PM	~20kB

Data ingested per solution (last 90 days)

Category	Usage
No data	

AZURE LOG ANALYTICS RETENTION



The screenshot shows a modal dialog box titled "Data Retention". The dialog contains the following text: "31 days of retention is included with your pricing plan. Longer retention will incur additional charges. Retention can also be [configured individually for specific data types](#).

Data Retention (Days) 30

Retention for Application Insights data types default to 90 days and will get the workspace retention if it is over 90 days. To set the retention on these types to be less than 90 days, set the retention on each of these data types. [Learn more](#).

OK

VIEW LOG ANALYTICS AUDIT DATA

View audit data at the database level

auditingtest (josephinebtest/auditingtest) | Auditing

SQL database

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.

1

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

Audit Logs JBSQLAuditing New Query 1* Select scope Run Time range: Last 24 hours Save Copy link New alert rule Export Pin to dashboard Format query

2

Azure JBSQLAuditing Tables Queries Filter Search Filter Group by: Solution

Enable Audit logs Favorites You can add favorites by clicking on the star icon

LogManagement AzureDiagnostics Functions

3

Stream analytics (preview)

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.

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

3

Feedback Queries Query explorer Format query

AzureDiagnostics where Category == 'SQLSecurityAuditEvents' where ResourceId == '/SUBSCRIPTIONS/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

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 + (1)

AUDIT DISTRIBUTION



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

DISTRIBUTION BY DATABASE



Database	Count
jbdb	6
master	120
Others	54

DISTRIBUTION BY IP

IP Address

IP Address	Count
67.174.120.120	174
Internal	6



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](#)

24

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 Gear

Custom logs 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

dbauditdata Select scope Run Time range : Set in query Save Share New alert rule Export

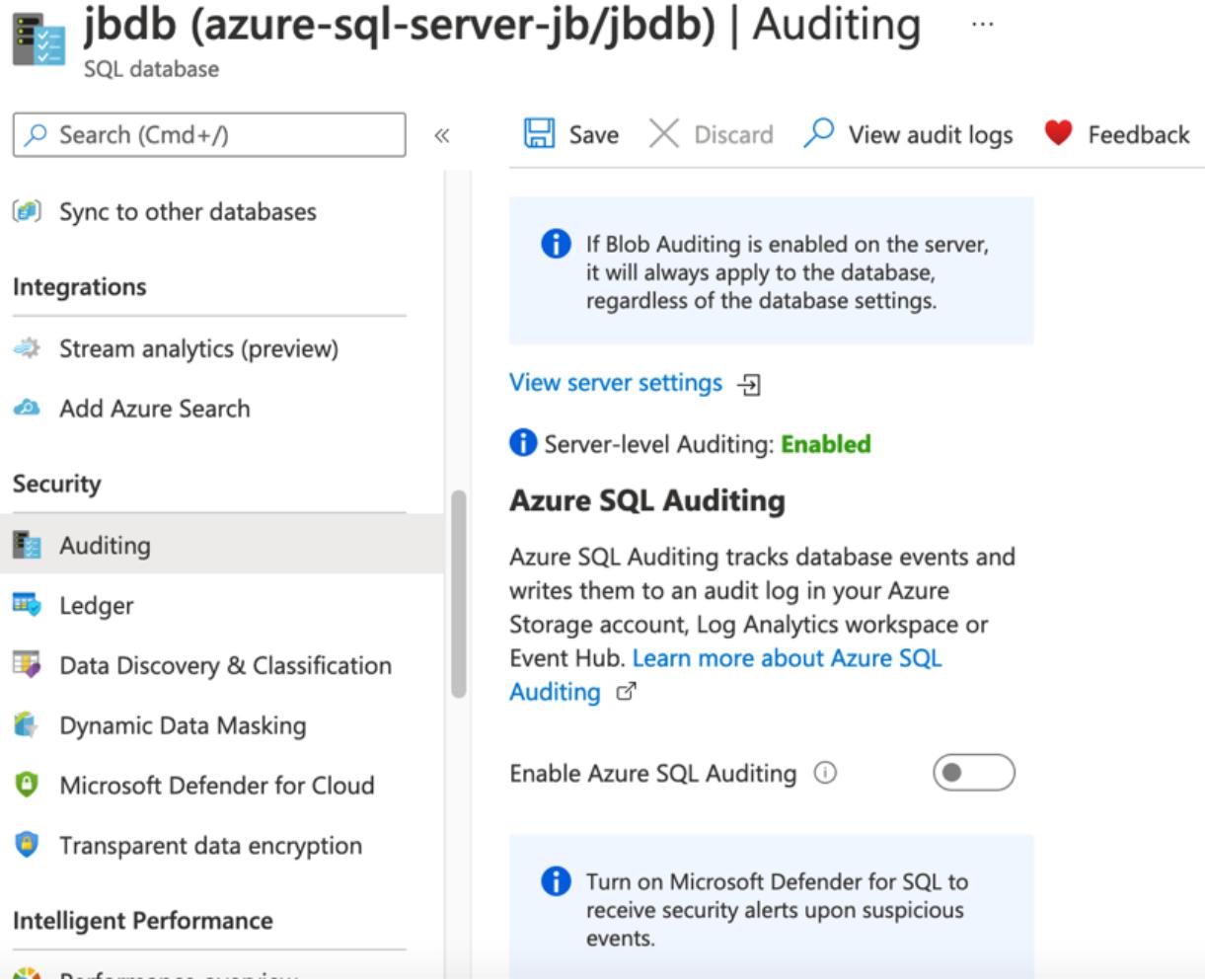
```

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

ENABLING AZURE SQL AUDITING



The screenshot shows the Azure portal interface for managing a database named 'jbdb' on a server 'azure-sql-server-jb/jbdb'. The left sidebar has sections like 'Sync to other databases', 'Integrations', 'Stream analytics (preview)', 'Add Azure Search', 'Security' (with 'Auditing' selected), 'Ledger', 'Data Discovery & Classification', 'Dynamic Data Masking', 'Microsoft Defender for Cloud', and 'Transparent data encryption'. The main content area shows the 'Auditing' tab under 'Azure SQL Auditing'. It displays a note about Blob Auditing, a status message 'Server-level Auditing: Enabled', a detailed description of Azure SQL Auditing, and a toggle switch labeled 'Enable Azure SQL Auditing' which is turned off. A note at the bottom encourages turning on Microsoft Defender for SQL.

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

Log Analytics workspaces > dbauditdata > Overview >

SQLSecurityInsights ...

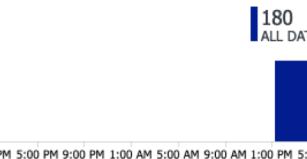
dbauditdata

Refresh Logs Edit

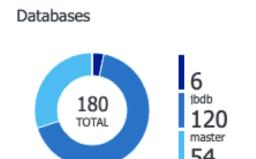
⚠️ Workbooks will be replacing View Designer. Learn how to keep your views updated with workbooks. →

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

AUDIT DISTRIBUTION



DISTRIBUTION BY DATABASE



DATABASE	COUNT
jbdb	6
master	120
Others	54

DISTRIBUTION BY IP

IP Address

IP ADDRESS	COUNT
67.174.125.125	174
Internal	6

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](#)

REPORTING ON AUDITING DATA

Home > auditreport

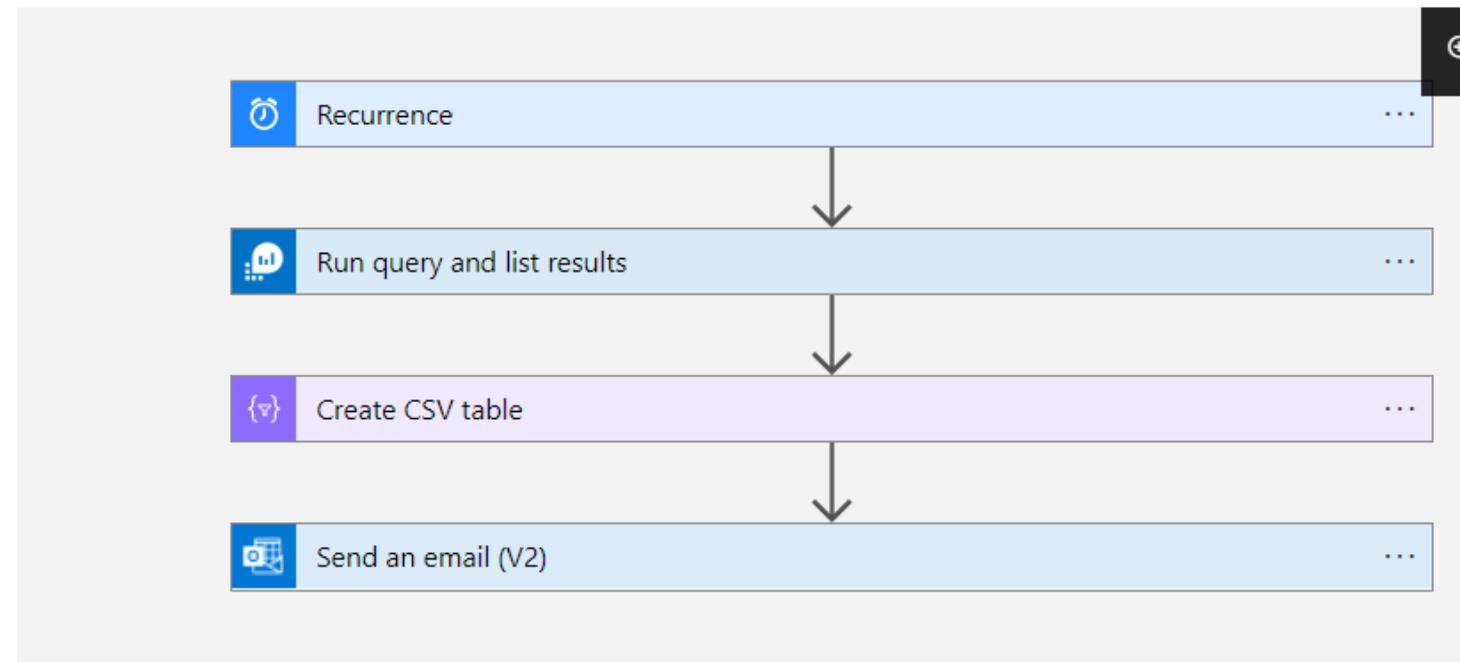
 **auditreport | Logic app designer** ...

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

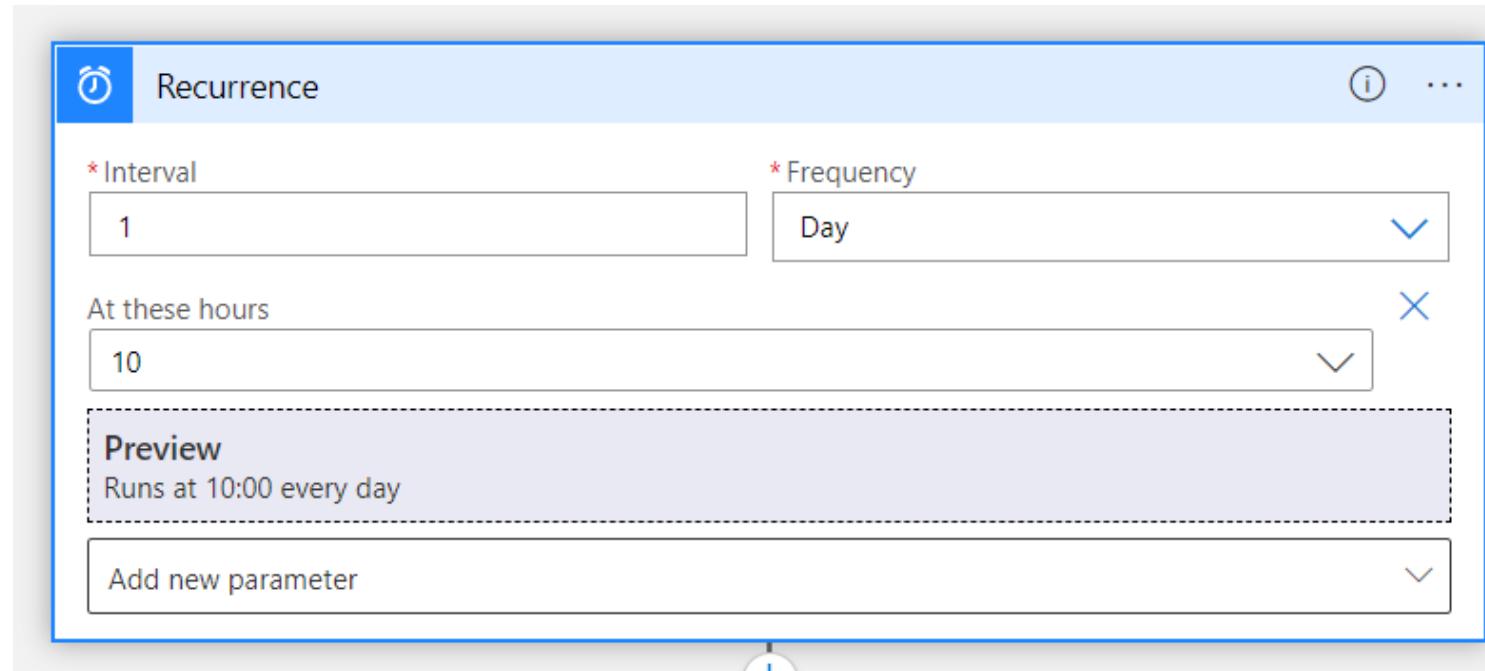
Development Tools Logic app designer Logic app code view Versions API connections



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

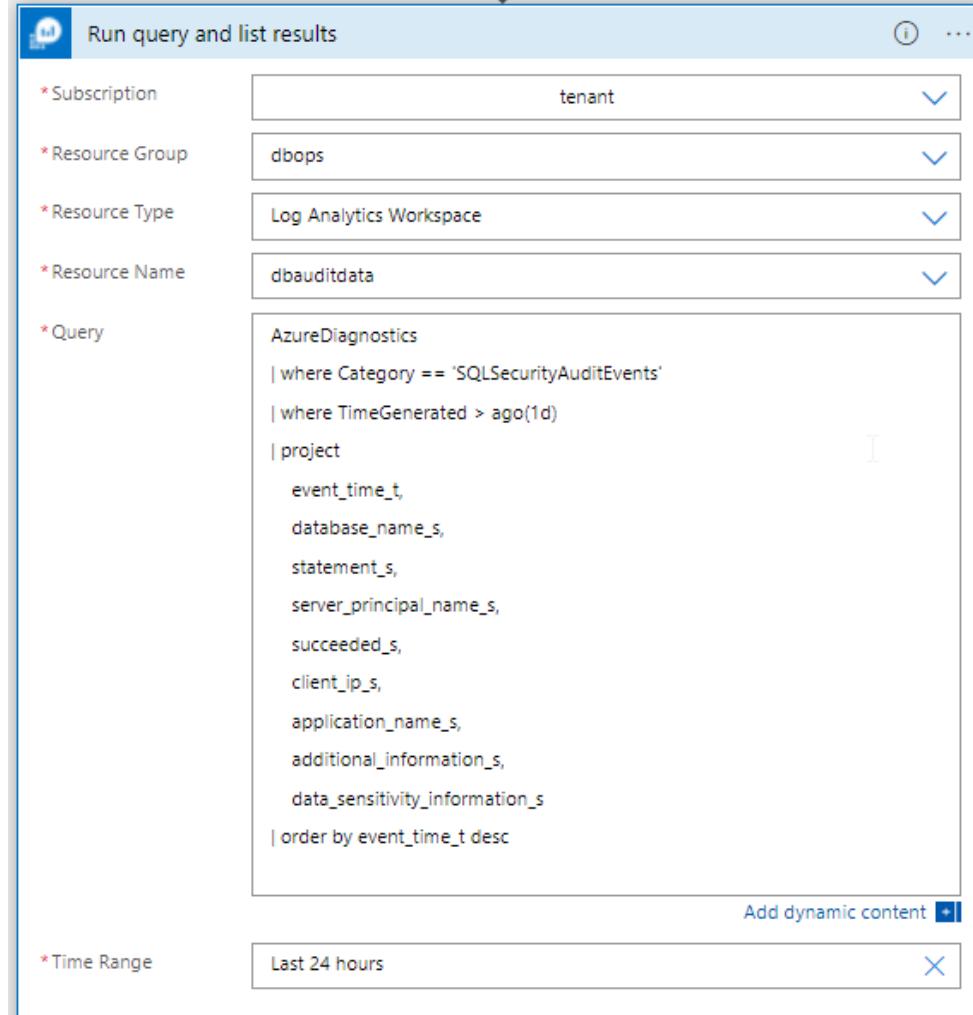
SETUP LOGIC APP - RECURRENCE

Setup a schedule with Recurrence step



SETUP LOGIC APP –KUSTO QUERY

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



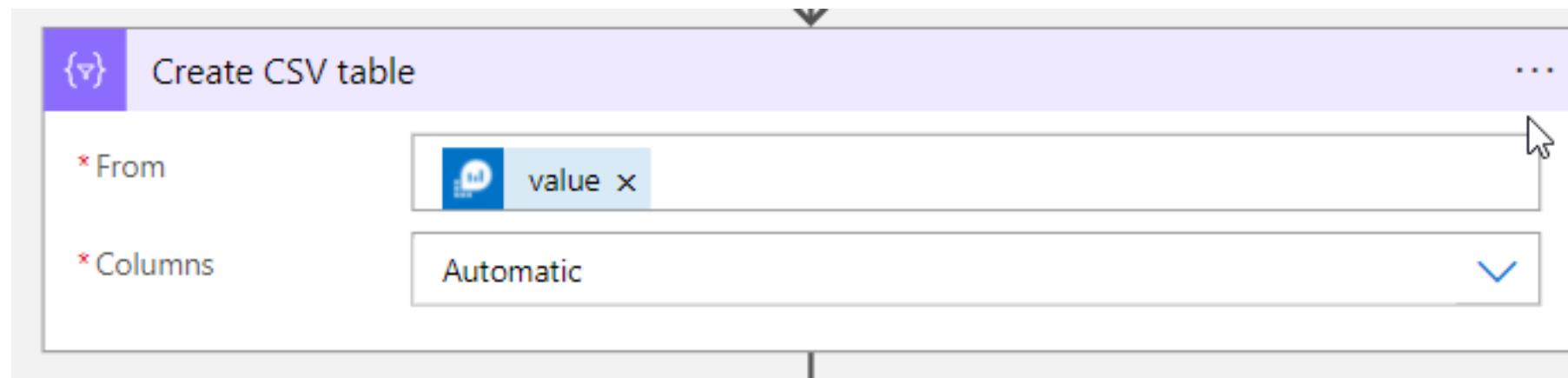
The screenshot shows the configuration of a 'Run query and list results' step in an Azure Logic App. The step has the following settings:

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

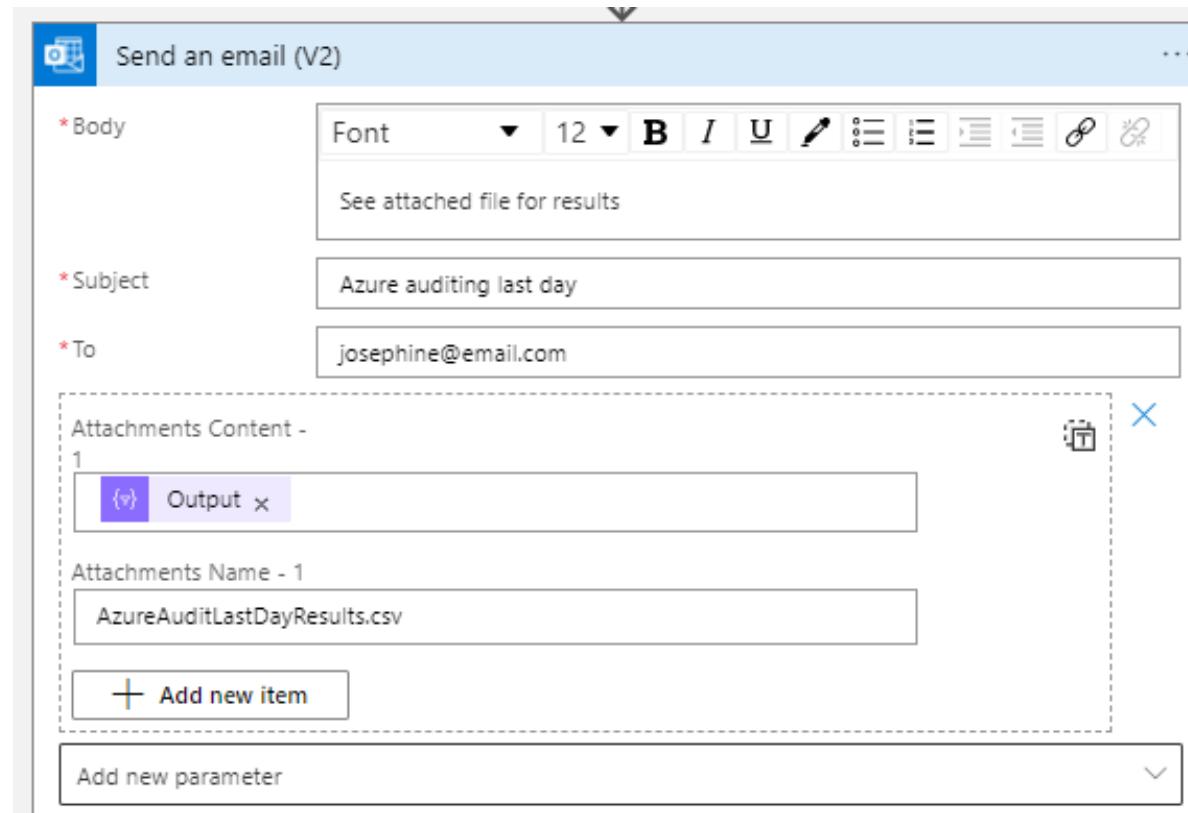
```
AzureDiagnostics  
| where Category == 'SQLSecurityAuditEvents'  
| where TimeGenerated > ago(1d)  
| project  
    event_time_t,  
    database_name_s,  
    statement_s,  
    server_principal_name_s,  
    succeeded_s,  
    client_ip_s,  
    application_name_s,  
    additional_information_s,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

SETUP LOGIC APP – CSV FILE

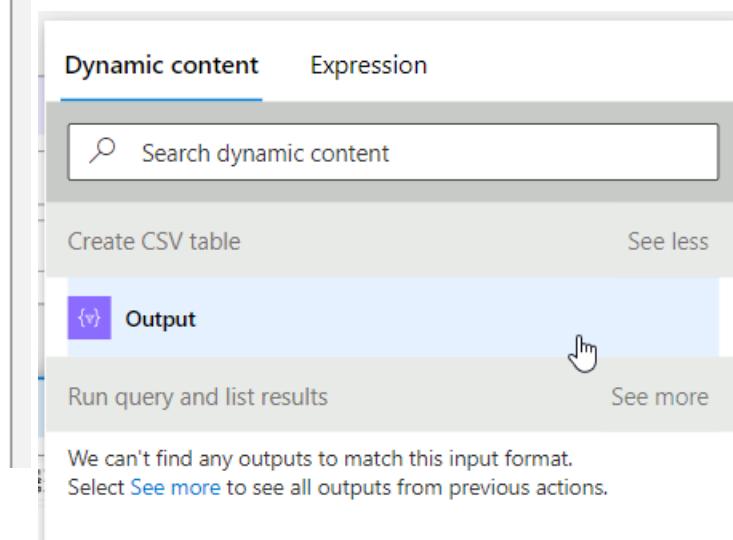
Create CSV table step to create a CSV file attachment



SETUP LOGIC APP – SEND EMAIL



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



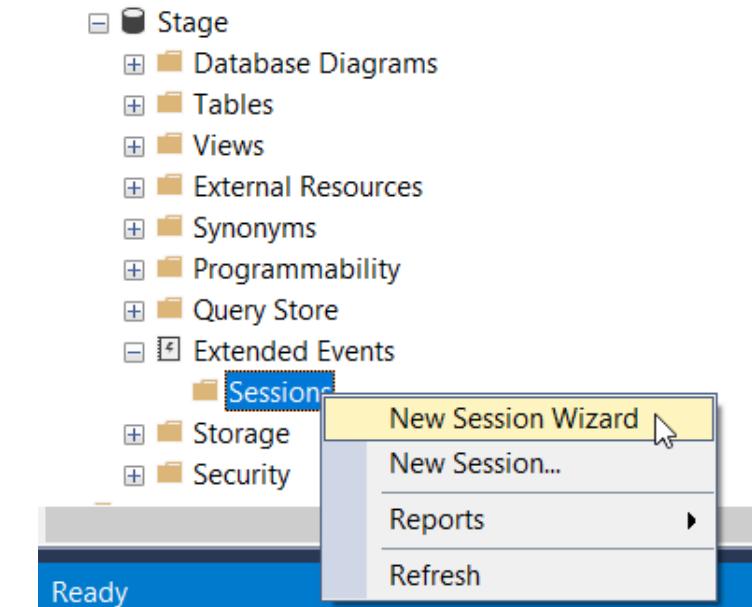
AZURE SQL AUDITING EXTENDED EVENTS

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)
  
```

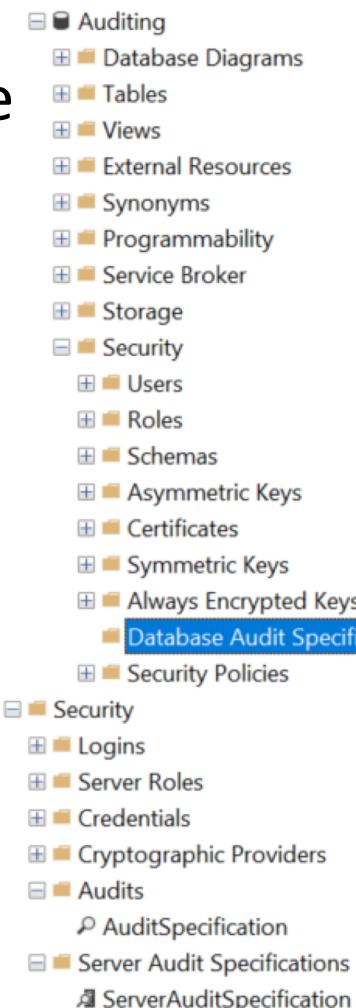
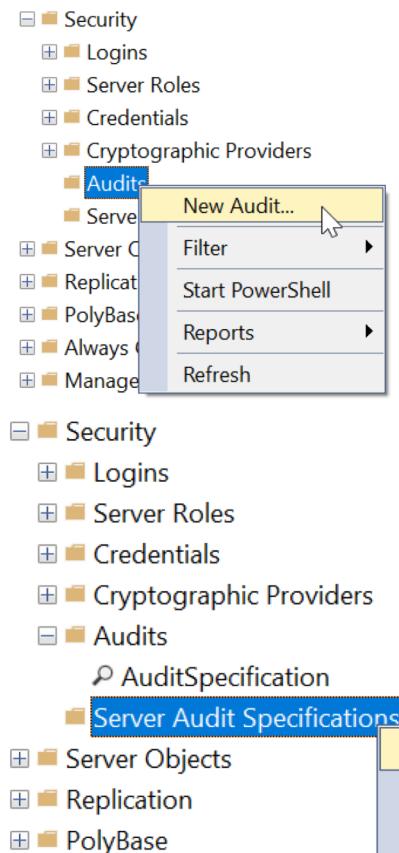
GUI



You need a credential setup to use the URL to the storage account in the filename

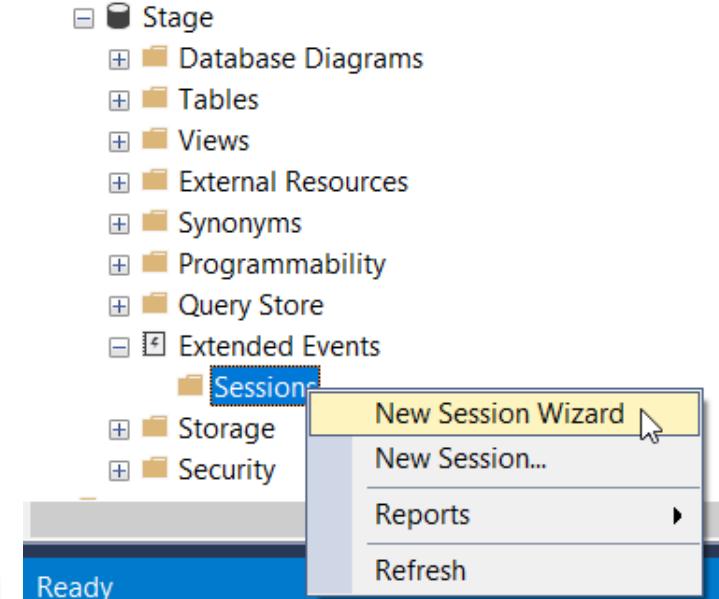
MANAGED INSTANCE AUDITING

SQL Server Audit



Or use diagnostic settings with Log Analytics workspace

Extended Events



DIAGNOSTIC SETTINGS

Diagnostic setting to store audit events in a Log Analytics workspace

Diagnostic setting ...

 Save  Discard  Delete  Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name *

miauditing



Logs

Category groups ⓘ

allLogs

audit

Categories

ResourceUsageStats

DevOpsOperationsAudit

SQLSecurityAuditEvents

Destination details

Send to Log Analytics workspace

Subscription

Dev

Log Analytics workspace

dbopsaudit (eastus2)

Archive to a storage account

USING DIAGNOSTIC SETTING

Create SQL Server Audit with diagnostic setting

```
USE [master];
CREATE SERVER AUDIT [miaudit] TO
EXTERNAL_MONITOR;
ALTER SERVER AUDIT [miaudit] WITH
(STATE = ON);
```

Setup server and/or database audit to use the server audit

Query SQL Server Audit

To access the audit data, you will need to go to the Log Analytics workspace you chose in your diagnostic setting

AWS RDS AUDITING SETUP

Required components

S3 bucket – To store audit files

Option group – To allow RDS SQL Server to use audit functionality.
This also determines which S3 bucket and IAM role to use.

IAM role – This will allow your RDS instance to access your S3 bucket

SQL Server Audit and Server or Database Audit – To audit actions on SQL Server

AWS RDS SQL AUDIT SETUP

The audit has to write to this path: D:\rdsdbdata

Don't use MAX_FILES at all.

```
USE [master];
CREATE SERVER AUDIT [AuditSpecification]
TO FILE (

```

```
    FILEPATH = N'D:\rdsdbdata\SQLAudit\' ,
    MAXSIZE = 10 MB, /* must be between 2 MB and 50 MB */
    MAX_ROLLOVER_FILES = 2147483647, /* don't change this setting */
    RESERVE_DISK_SPACE = OFF )
```

```
WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
```

```
WHERE ([database_name]<>'rdsadmin');
```

Don't configure SQL Server
to shut down the DB
instance if it fails to write
the audit record

AWS RDS QUERY SQL AUDIT

```
SELECT DISTINCT event_time, aa.name as audit_action, statement,
succeeded, database_name, server_instance_name, schema_name,
session_server_principal_name, server_principal_name,
object_Name, file_name, client_ip, application_name, file_name
FROM msdb.dbo.rds_fn_get_audit_file ('D:\rdsdbdata\SQLAudit\*.
sqlaudit',default,default) af
INNER JOIN sys.dm_audit_actions aa ON aa.action_id = af.action_id
WHERE event_time > DATEADD(HOUR, -1, GETDATE())
ORDER BY event_time DESC;
```

AWS RDS XEVENTS

You have to put your extended events in the path
D:\rdsdbdata\Log\

Otherwise, setup and query is like SQL Server on a VM

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>

Log analytics pricing

<https://azure.microsoft.com/en-us/pricing/details/monitor/#pricing>

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 Setup

<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>

Session evaluation

Your feedback is important to us



Evaluate this session at:

www.PASSDataCommunitySummit.com/evaluation



Thank you

Thank you for taking part in the
PASS Data Community Summit 2022.

Any questions?

Please email speakers@passsummit.com

Josephine

@hellosqlkitty / sqlkitty.com

