HANDLE AZURE SQL AUDITING WITH EASE

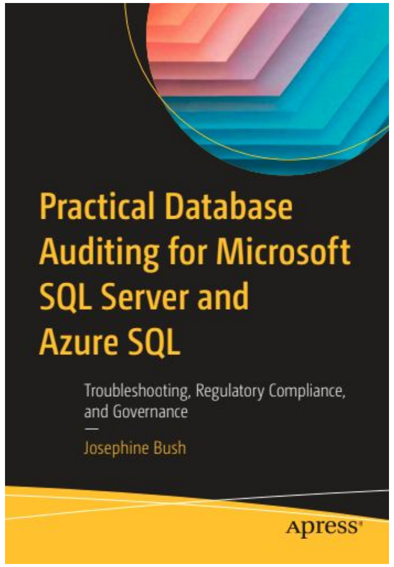
ABOUT ME

Josephine Bush

MVP
Microsoft®
Most Valuable Professional

FEATURED IN THE
redgate
100
MOST INFLUENTIAL IN THE DATABASE COMMUNITY 2022
redgate

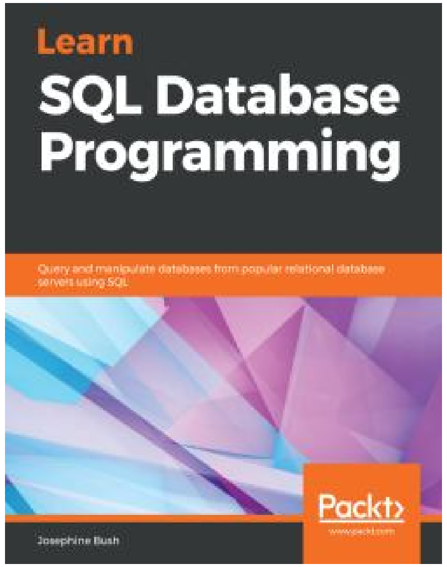
@hellosqlkitty
sqlkitty.com


Practical Database Auditing for Microsoft SQL Server and Azure SQL

Troubleshooting, Regulatory Compliance, and Governance

Josephine Bush

Apress®


Learn SQL Database Programming

Query and manipulate databases from popular relational database servers using SQL

Josephine Bush

Packt›
www.packt.com

Four-Project Series

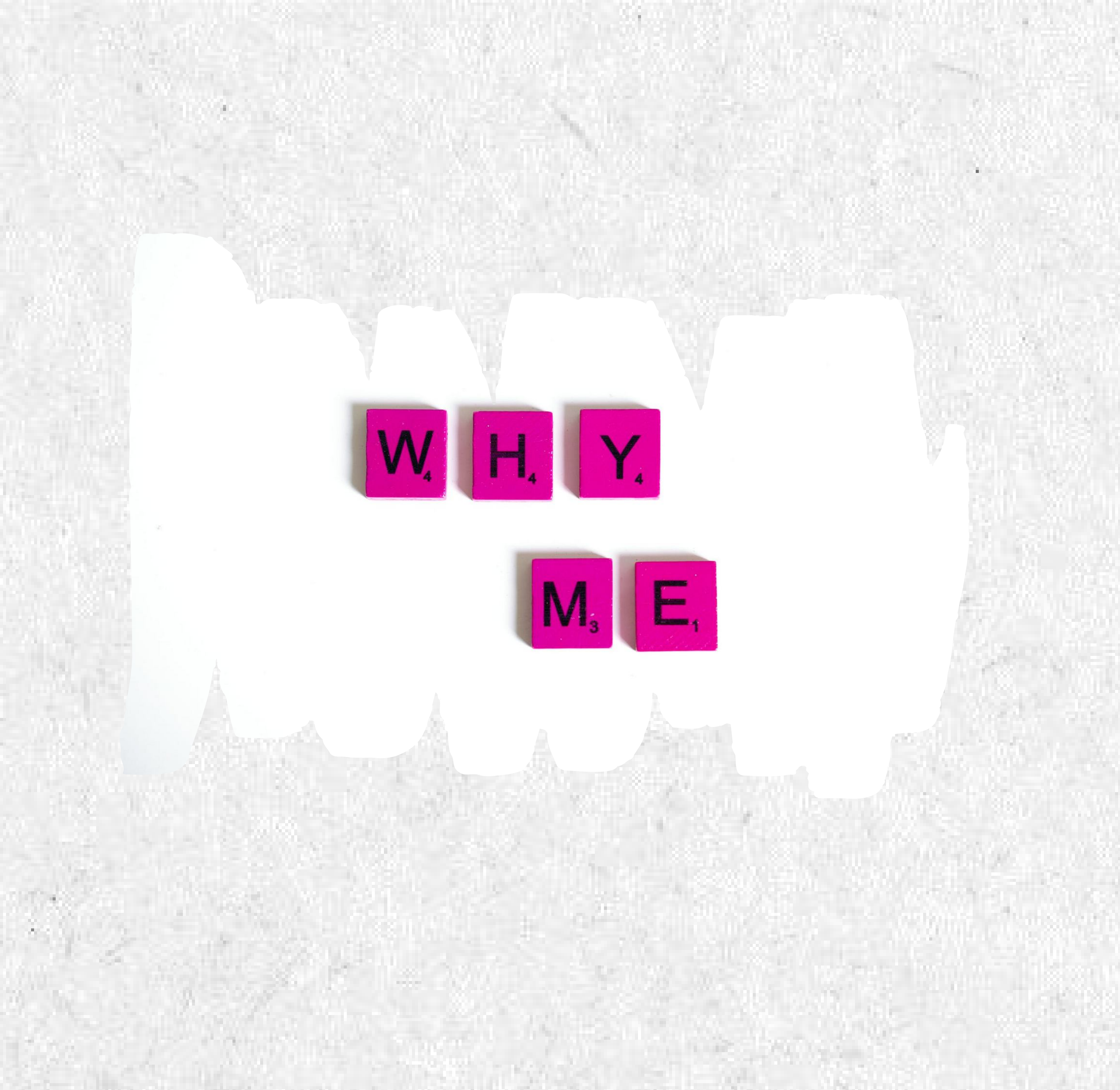
Migrate SQL Server to Azure

MANNING

LIVEPROJECT

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….

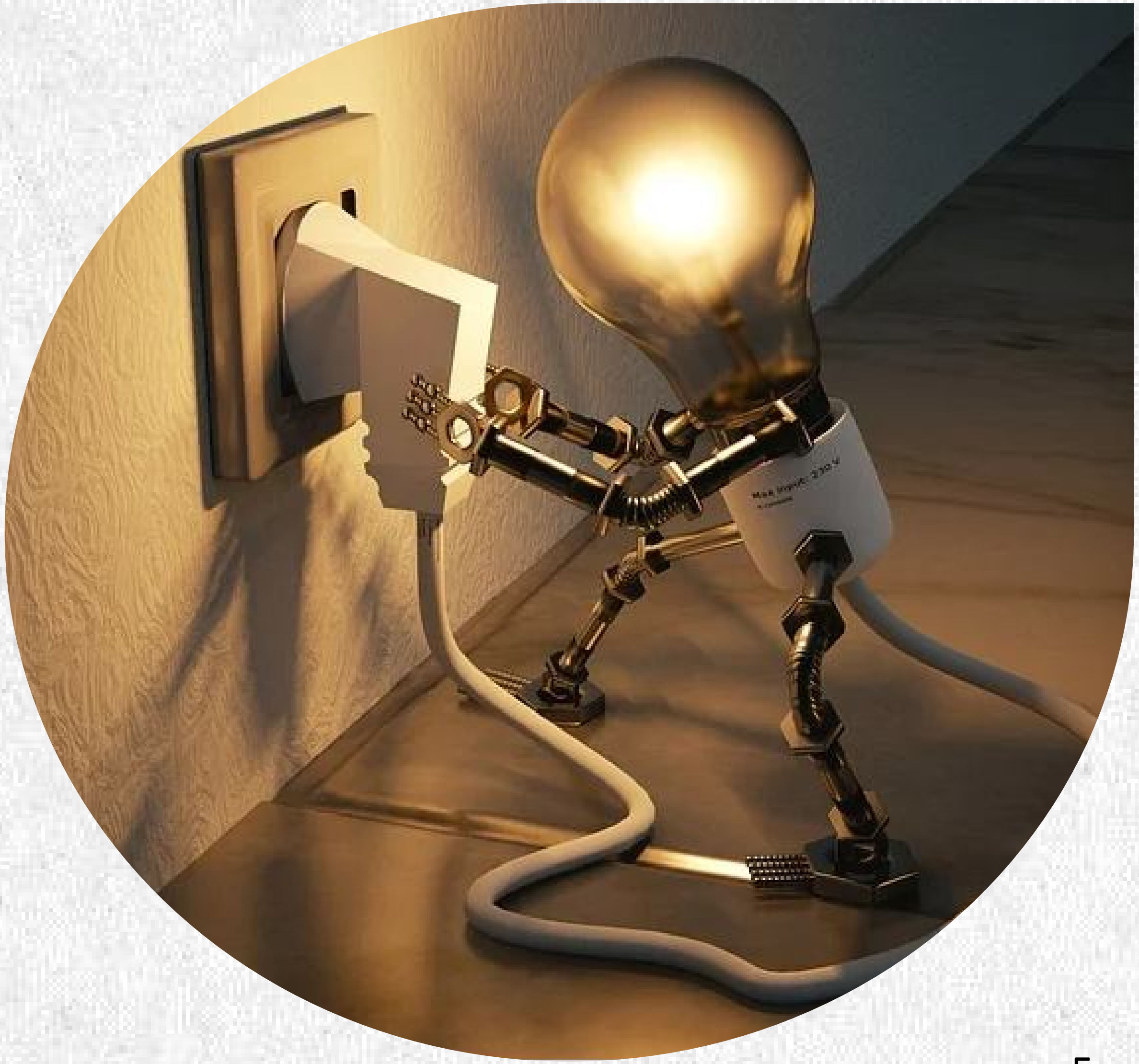
PROBLEMS AUDITING CAN SOLVE

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

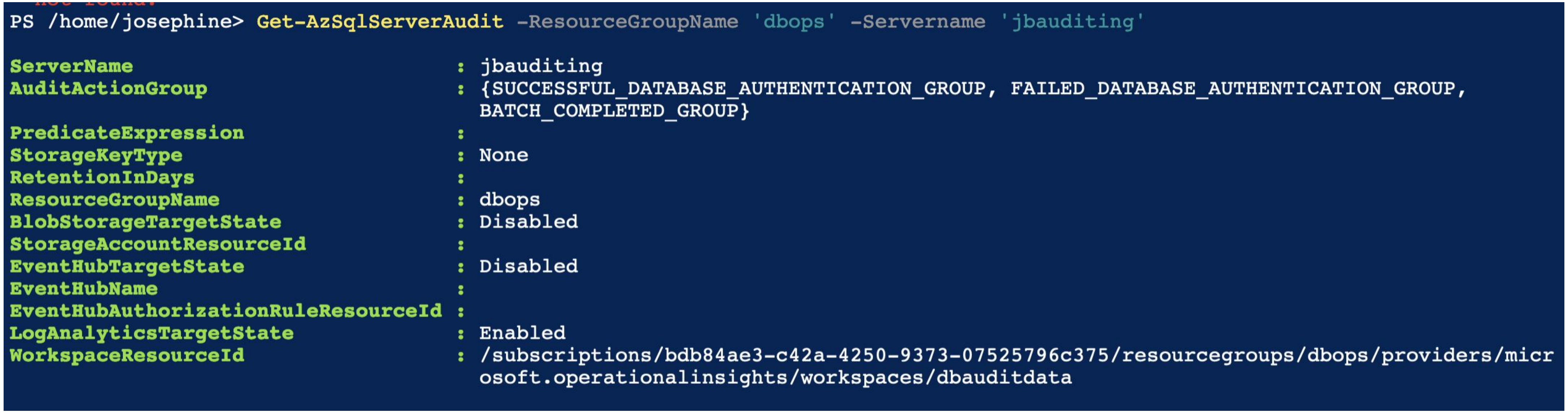
MODIFY AZURE SQL AUDITING POLICY

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'

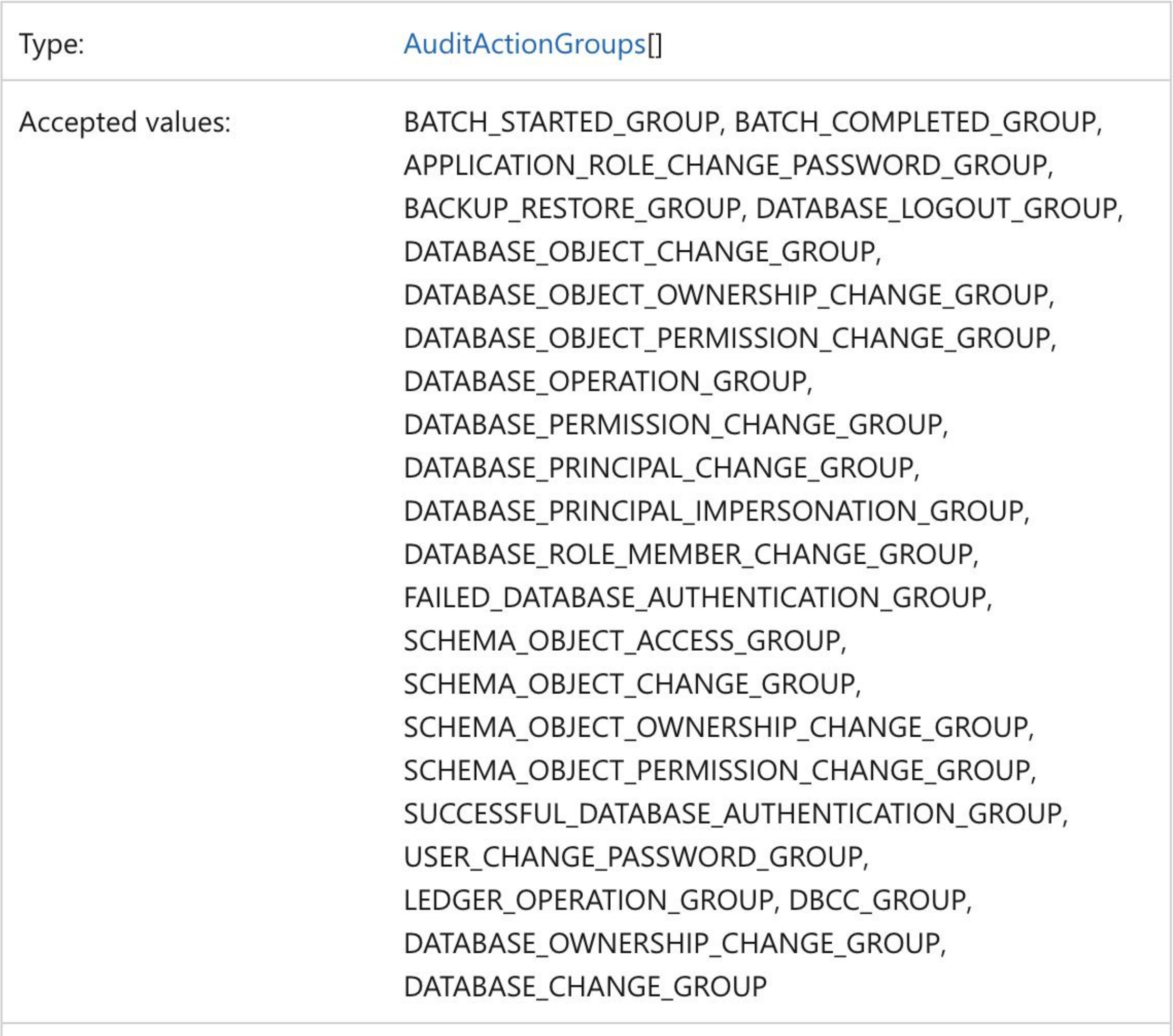


```
PS /home/josephine> Get-AzSqlServerAudit -ResourceGroupName 'dbops' -Servername 'jbauditing'

ServerName                             : 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/micr
                                         osoft.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

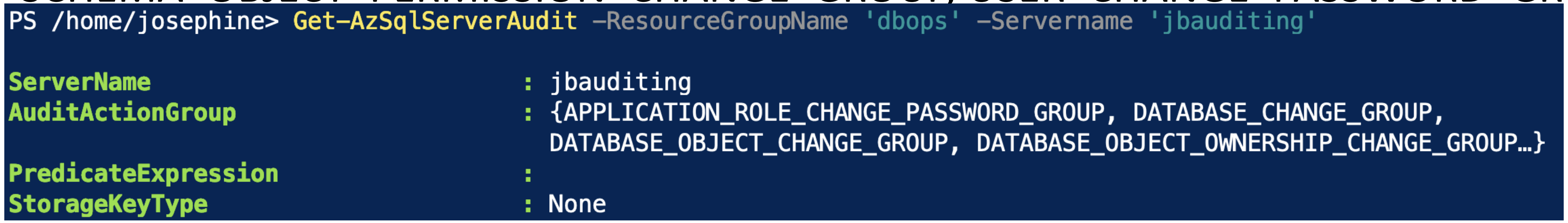


Type:	AuditActionGroups[]
Accepted values:	BATCH_STARTED_GROUP, BATCH_COMPLETED_GROUP, APPLICATION_ROLE_CHANGE_PASSWORD_GROUP, BACKUP_RESTORE_GROUP, DATABASE_LOGOUT_GROUP, DATABASE_OBJECT_CHANGE_GROUP, DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP, DATABASE_OBJECT_PERMISSION_CHANGE_GROUP, DATABASE_OPERATION_GROUP, 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:

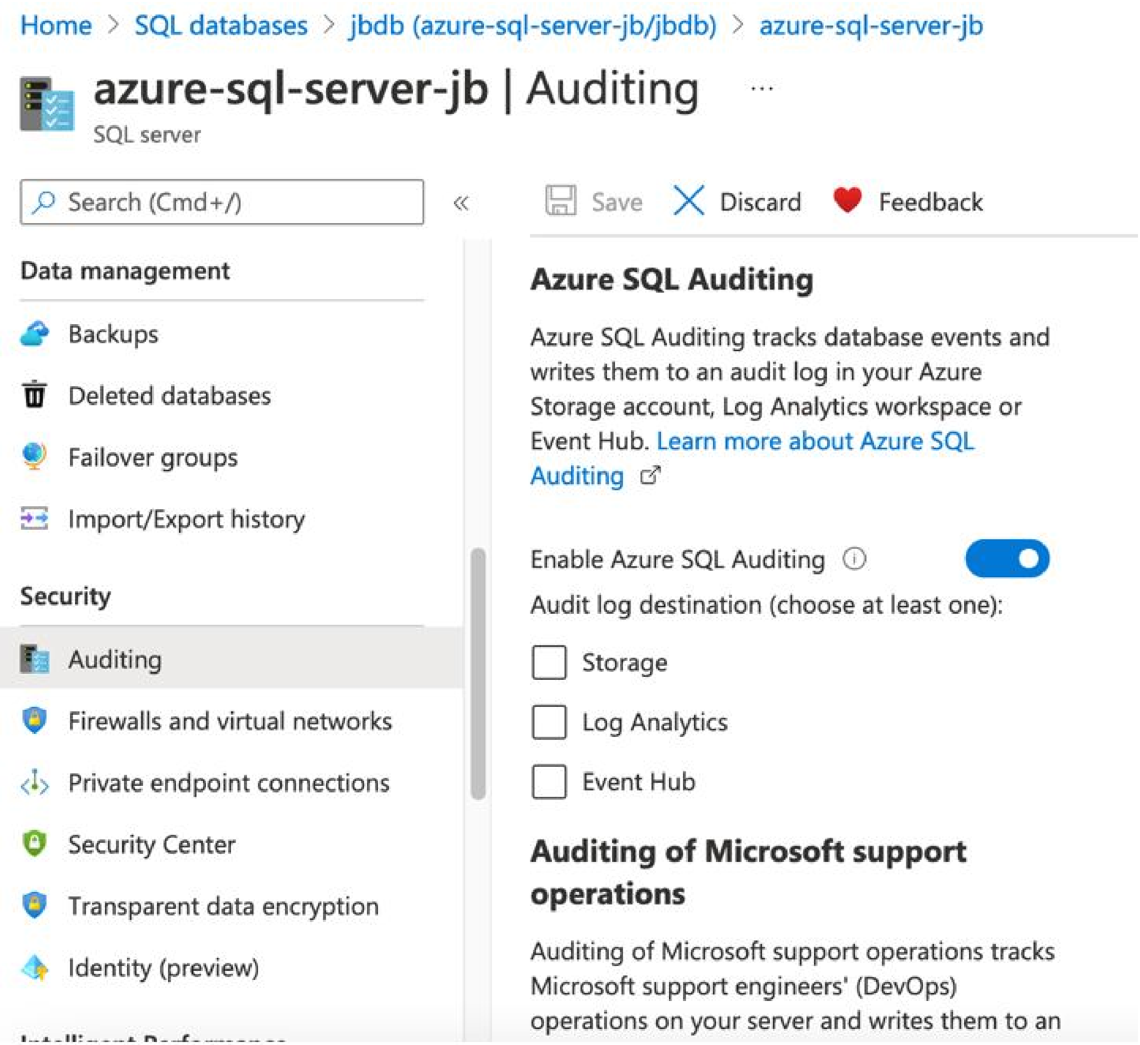
```
Set-AzSqlServerAudit -ResourceGroupName 'rg-sterling-rabbit' -ServerName 'sql2-rg-sterling-rabbit'`
-AuditActionGroup APPLICATION_ROLE_CHANGE_PASSWORD_GROUP,
DATABASE_CHANGE_GROUP, `
DATABASE_OBJECT_CHANGE_GROUP, DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP, `
DATABASE_OBJECT_PERMISSION_CHANGE_GROUP, DATABASE_OWNERSHIP_CHANGE_GROUP, `
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'

ServerName                         : 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

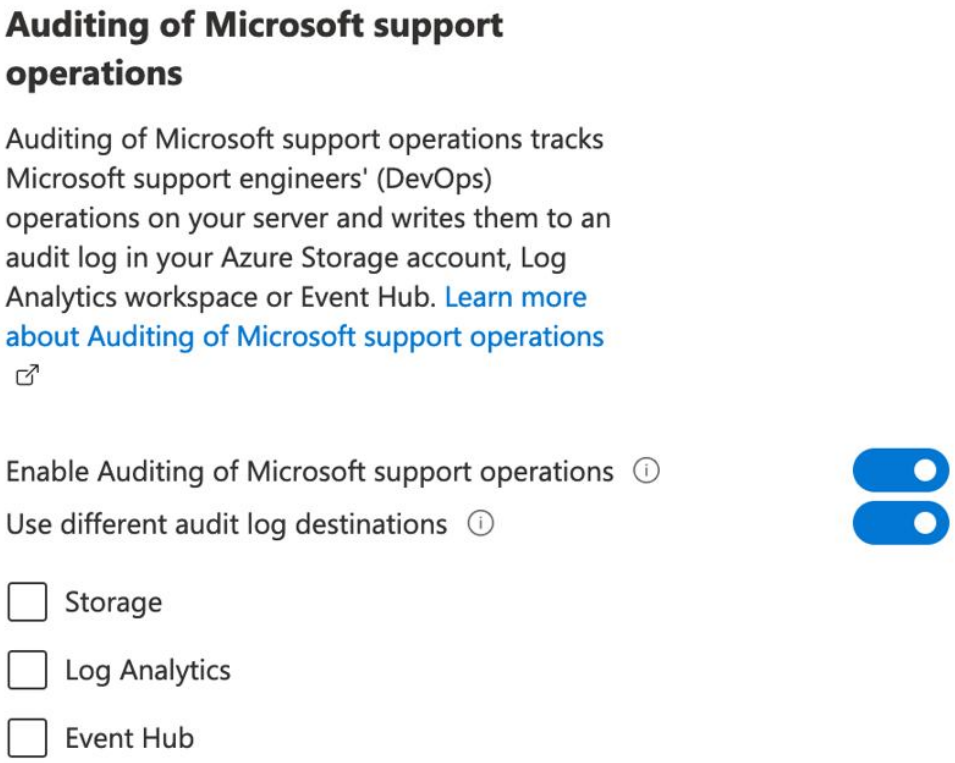
Enable Azure SQL Auditing ⓘ ●

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



Auditing of Microsoft support operations

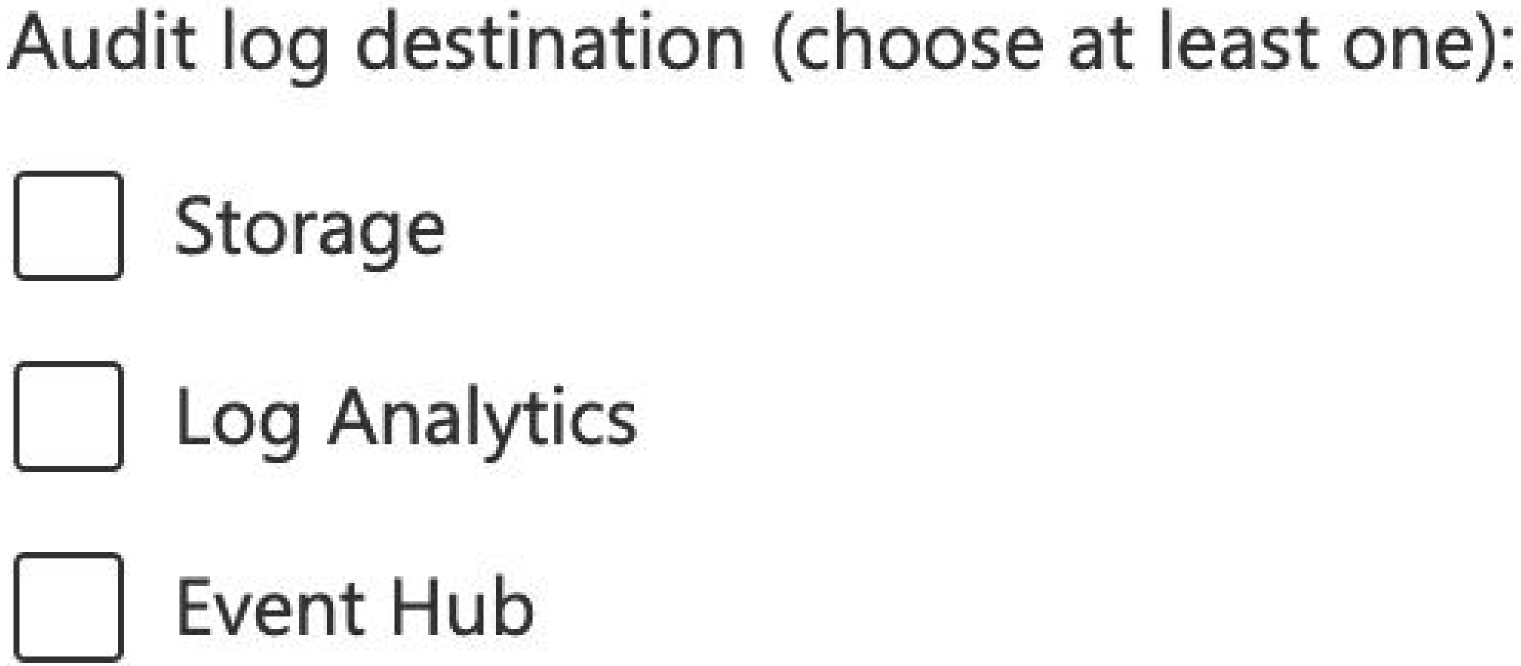
Auditing of Microsoft support operations tracks Microsoft support engineers' (DevOps) operations on your server and writes them to an audit log in your Azure Storage account, Log Analytics workspace or Event Hub. Learn more about Auditing of Microsoft support operations

Enable Auditing of Microsoft support operations ⓘ ●

Use different audit log destinations ⓘ ●

- □ Storage
- □ Log Analytics
- □ Event Hub

AZURE SQL AUDITING OPTIONS



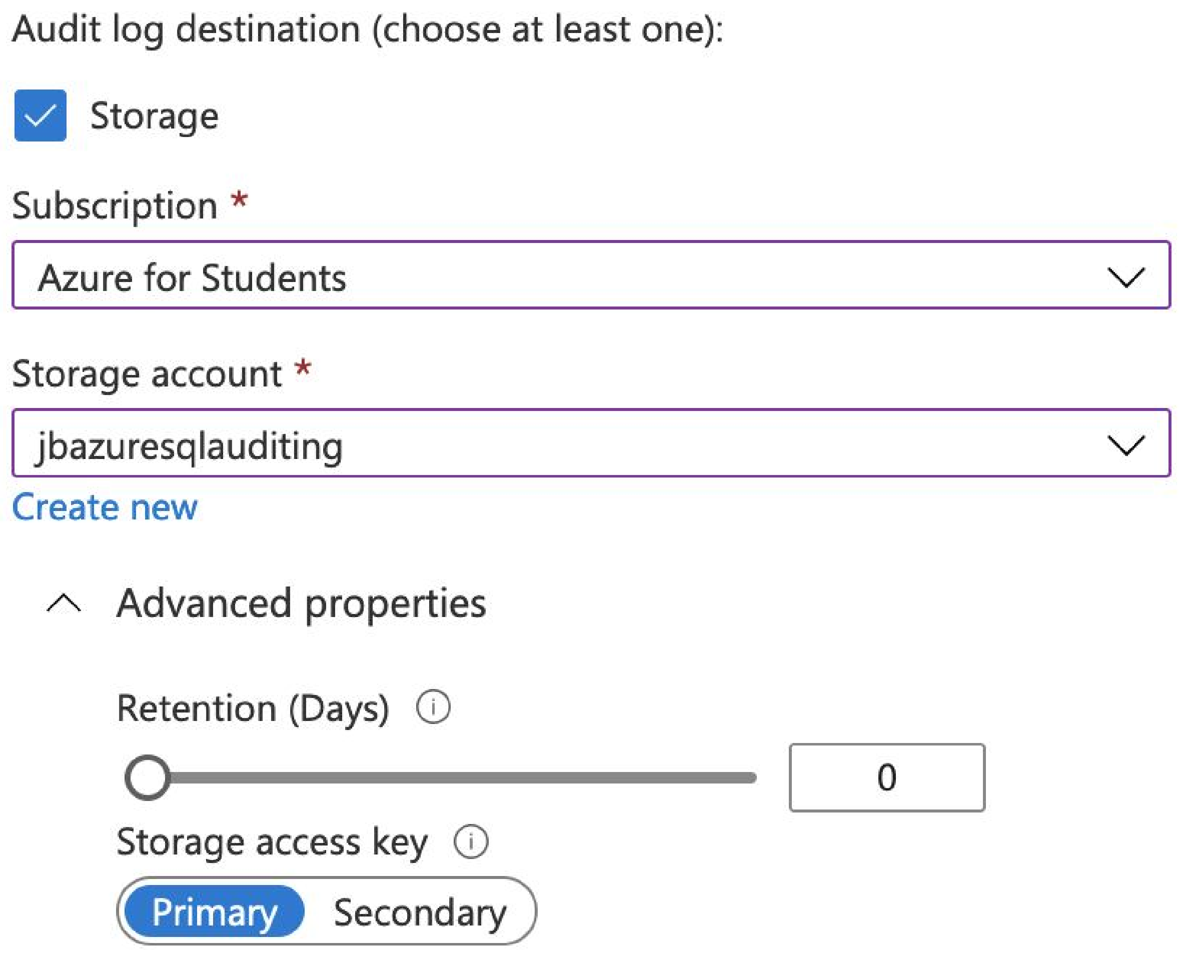
Audit log destination (choose at least one):

□ 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

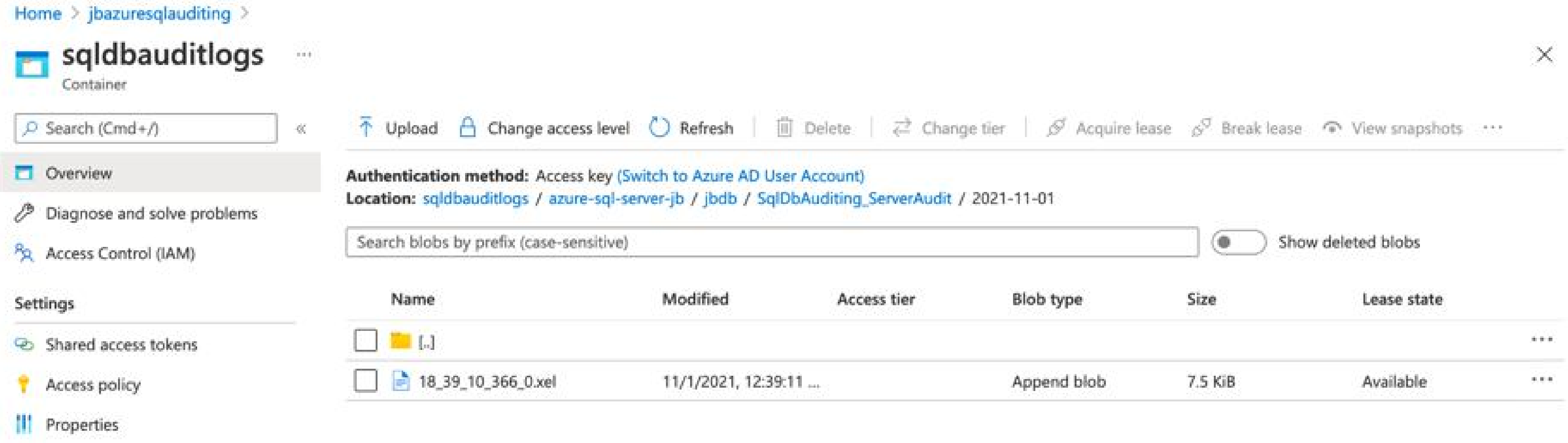
Retention (Days) ⓘ

0

Storage access key ⓘ

[✓ Primary] Secondary

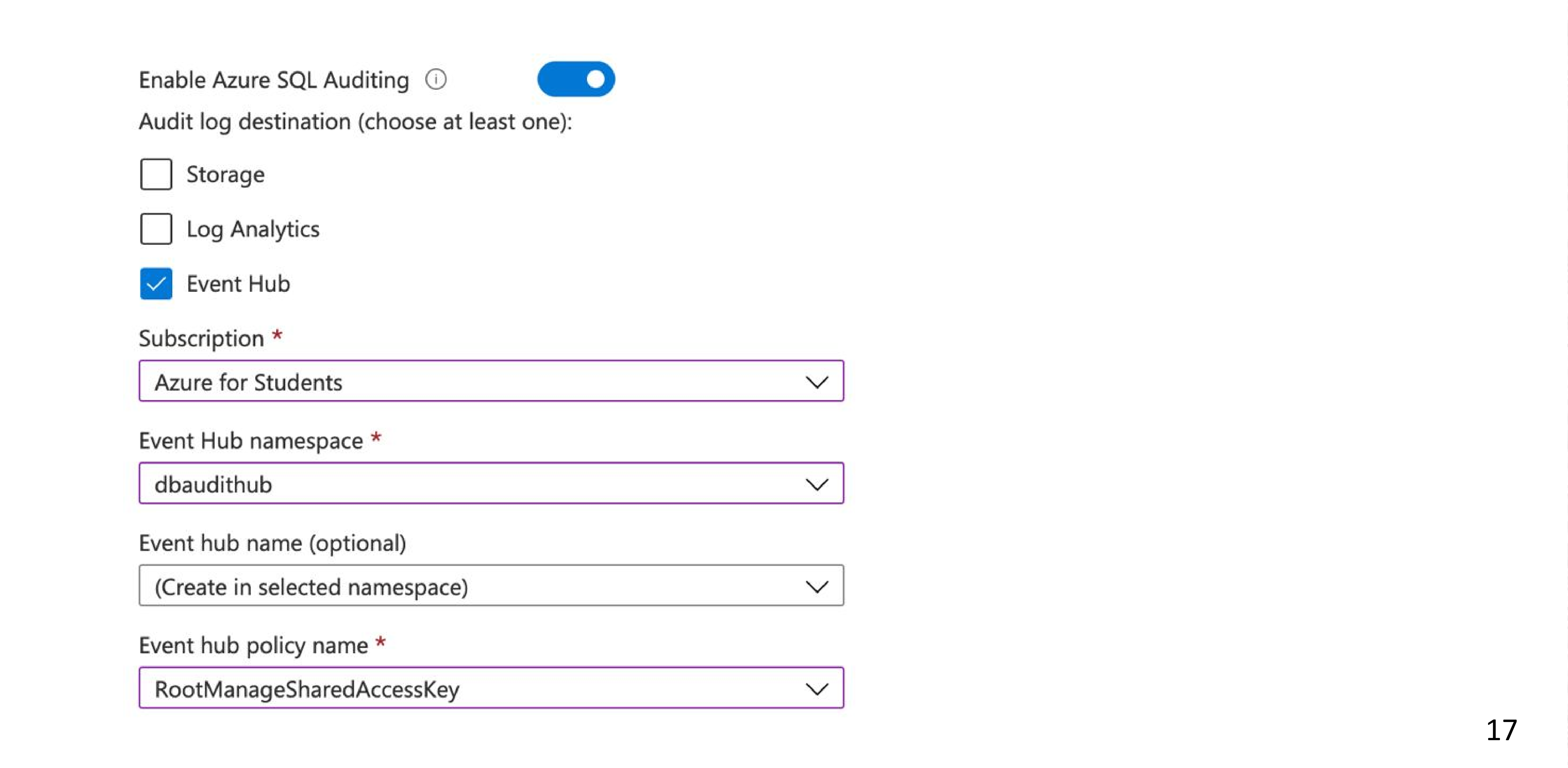
AZURE SQL AUDITING STORAGE FILES



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

	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 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

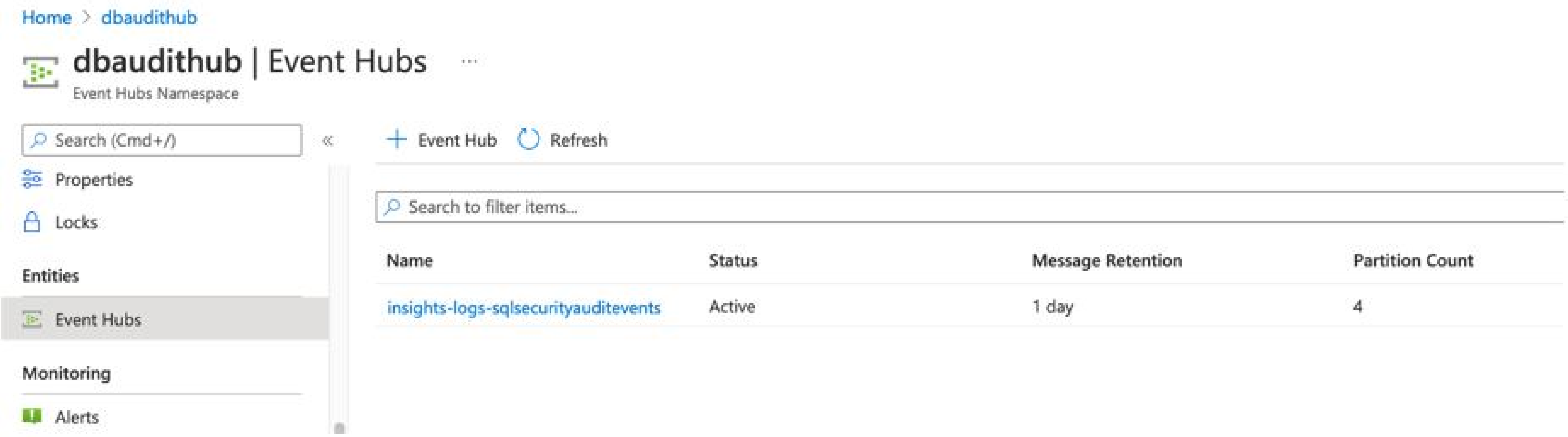
Event hub name (optional)

(Create in selected namespace)

Event hub policy name *

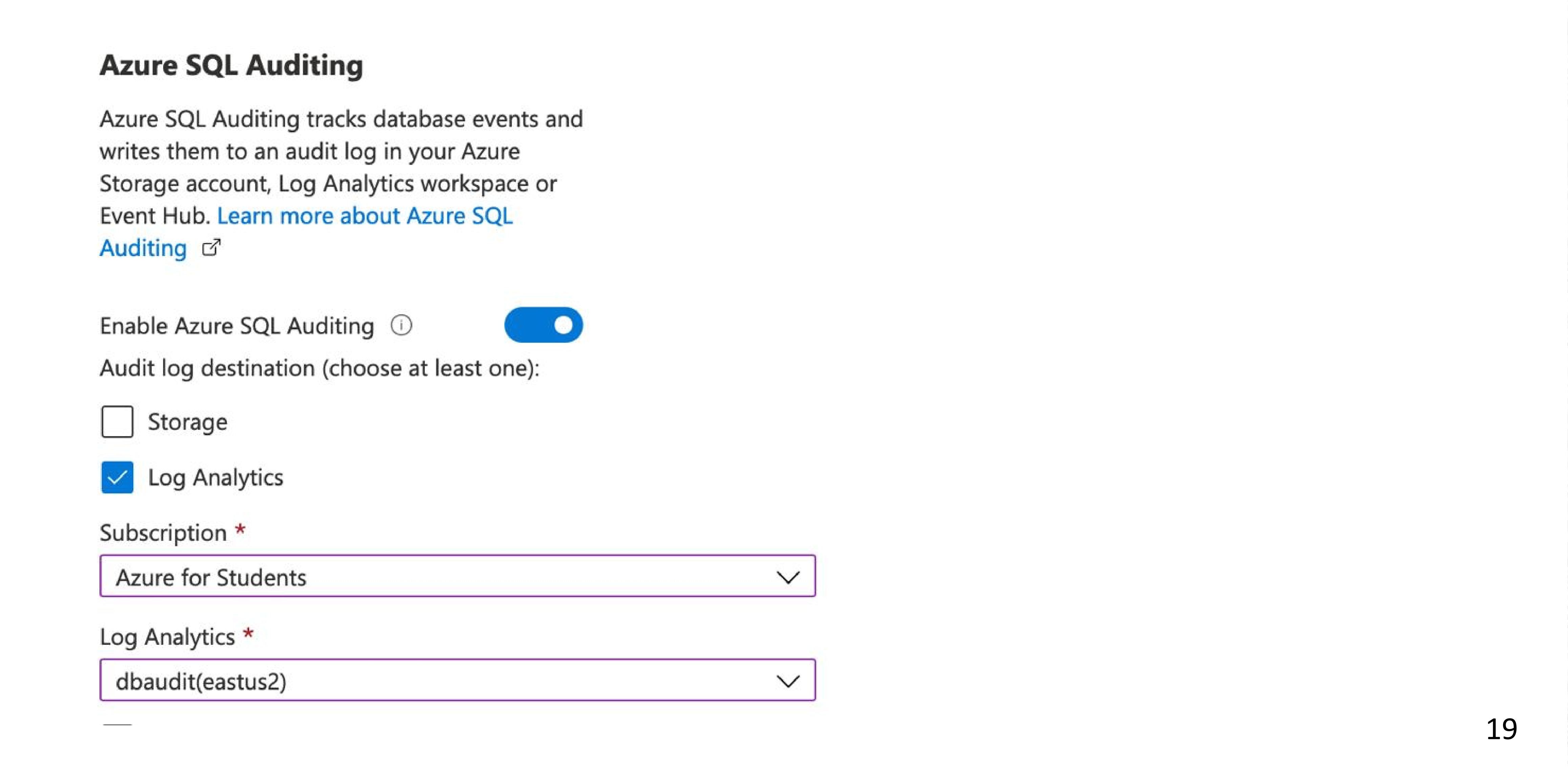
RootManageSharedAccessKey

AZURE SQL AUDITING EVENT HUB DATA



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 *

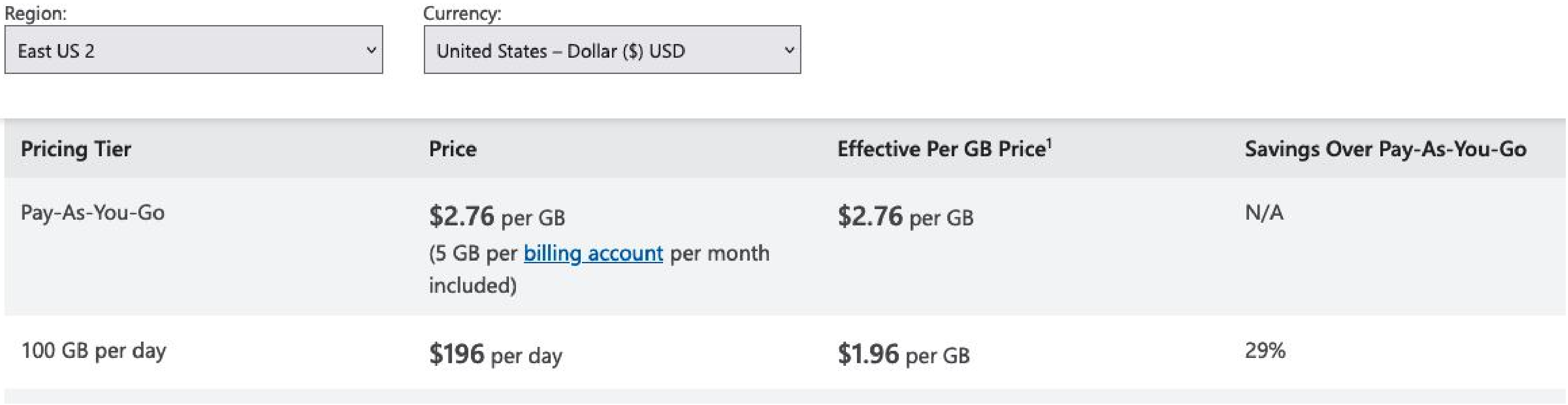
Azure for Students

Log Analytics *

dbaudit(eastus2)

AZURE LOG ANALYTICS PRICING

Ingesting data

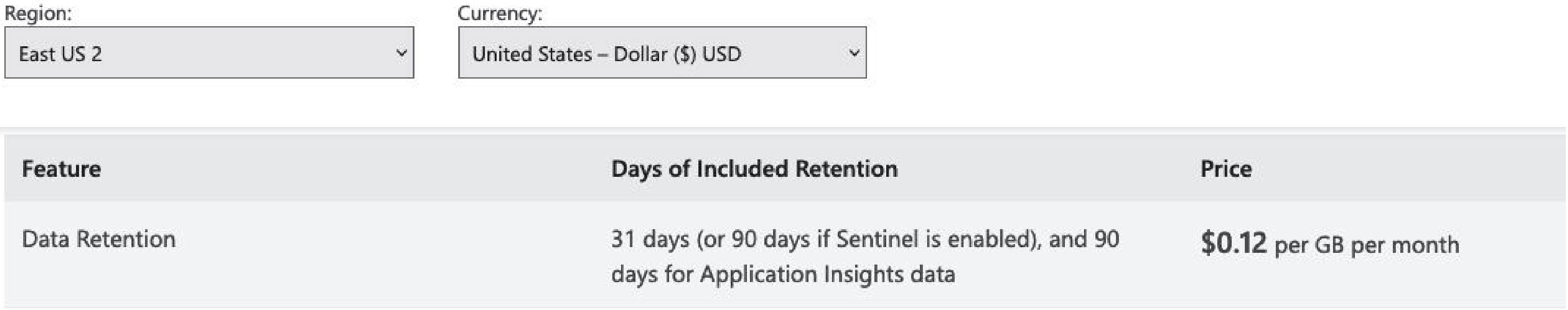


Region: East US 2

Currency: United States – Dollar ($) USD

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

Retaining data

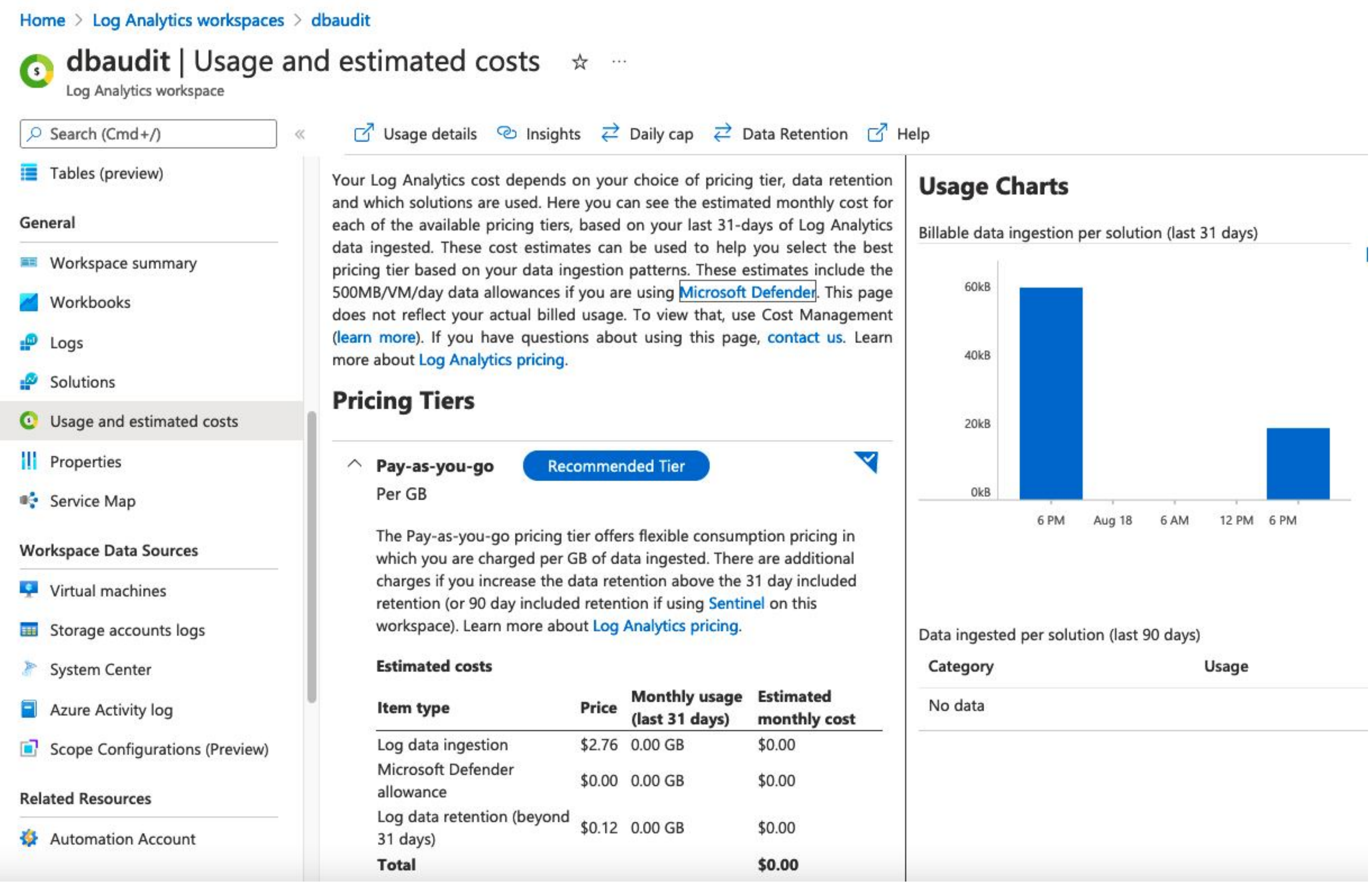


Region: East US 2

Currency: United States – Dollar ($) USD

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



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.

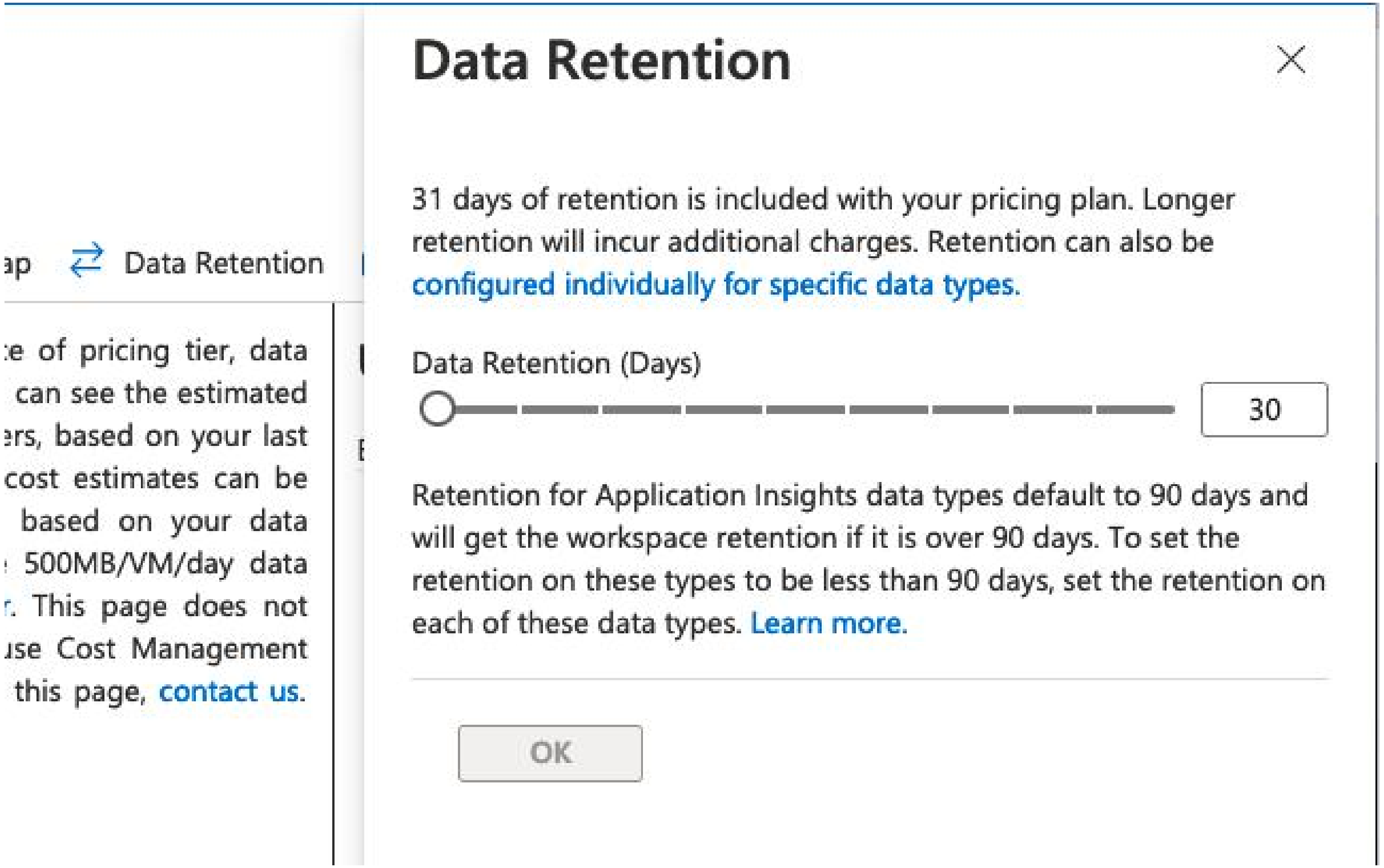
Estimated costs

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**

Data ingested per solution (last 90 days)

Category	Usage
No data	

AZURE LOG ANALYTICS RETENTION



ap ⇄ Data Retention

e of pricing tier, data can see the estimated rs, based on your last cost estimates can be based on your data 500MB/VM/day data . This page does not use Cost Management this page, contact us.

Data Retention

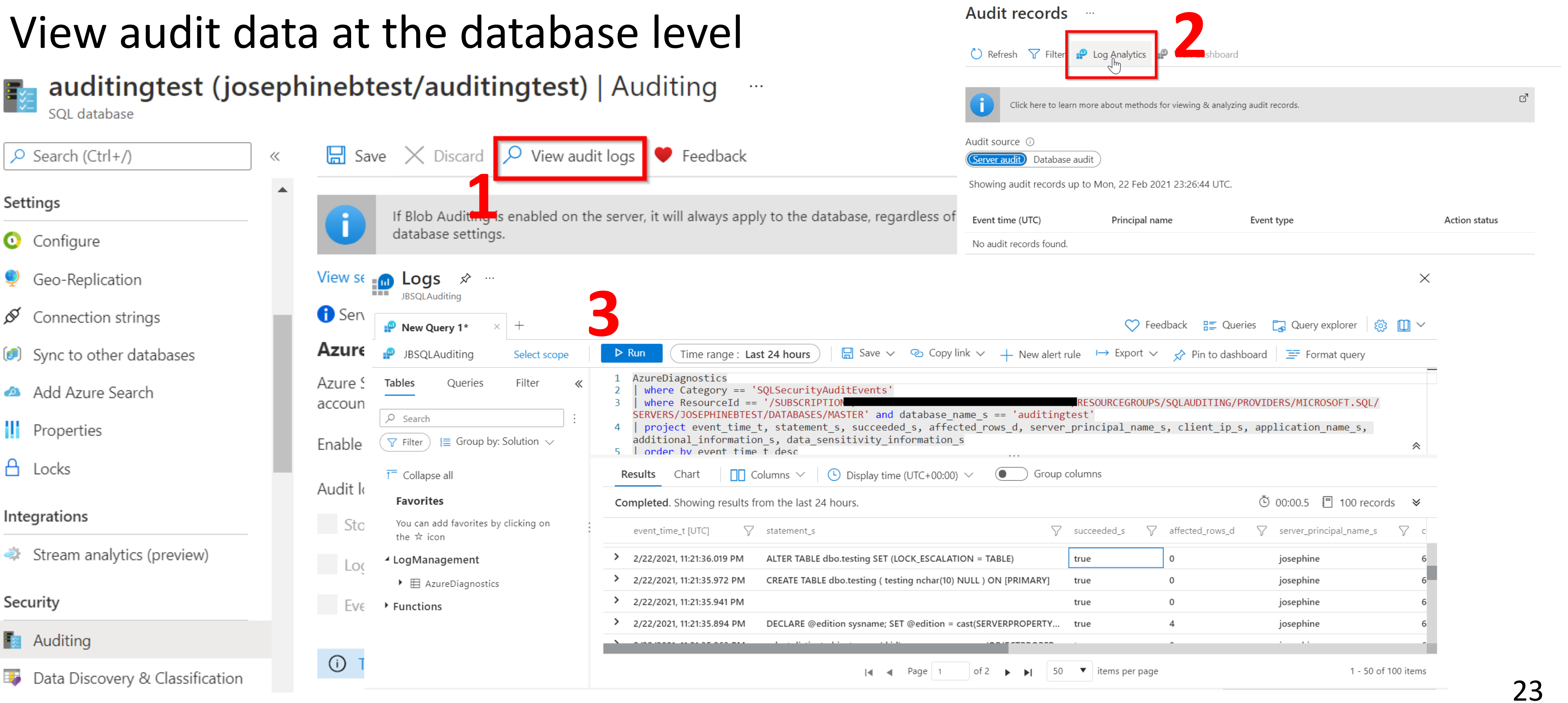
31 days of retention is included with your pricing plan. Longer retention will incur additional charges. Retention can also be configured individually for specific data types.

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.

VIEW LOG ANALYTICS AUDIT DATA

View audit data at the database level



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

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

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

No audit records found.

You can add favorites by clicking on the ☆ icon

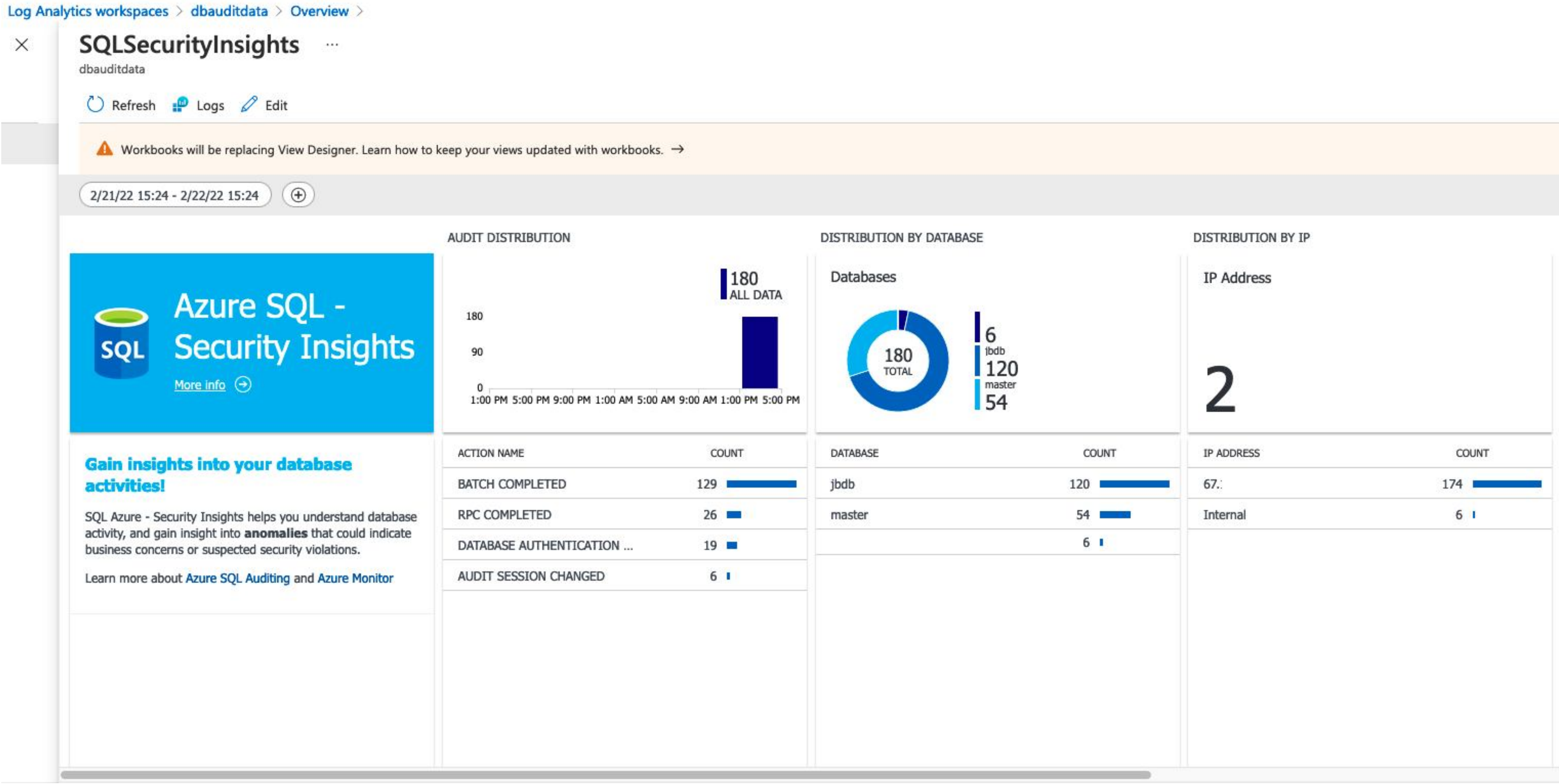
```
AzureDiagnostics
| where Category == 'SQLSecurityAuditEvents'
| where ResourceId == '/SUBSCRIPTION[redacted]RESOURCEGROUPS/SQLAUDITING/PROVIDERS/MICROSOFT.SQL/
SERVERS/JOSEPHINEBTEST/DATABASES/MASTER' and database_name_s == 'auditingtest'
| project event_time_t, statement_s, succeeded_s, affected_rows_d,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

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

VIEW LOG ANALYTICS WORKSPACE

View audit data in workspace summary – being deprecated



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
180
90
0
1:00 PM 5:00 PM 9:00 PM 1:00 AM 5:00 AM 9:00 AM 1:00 PM 5:00 PM

ACTION NAME	COUNT
BATCH COMPLETED	129
RPC COMPLETED	26
DATABASE AUTHENTICATION ...	19
AUDIT SESSION CHANGED	6

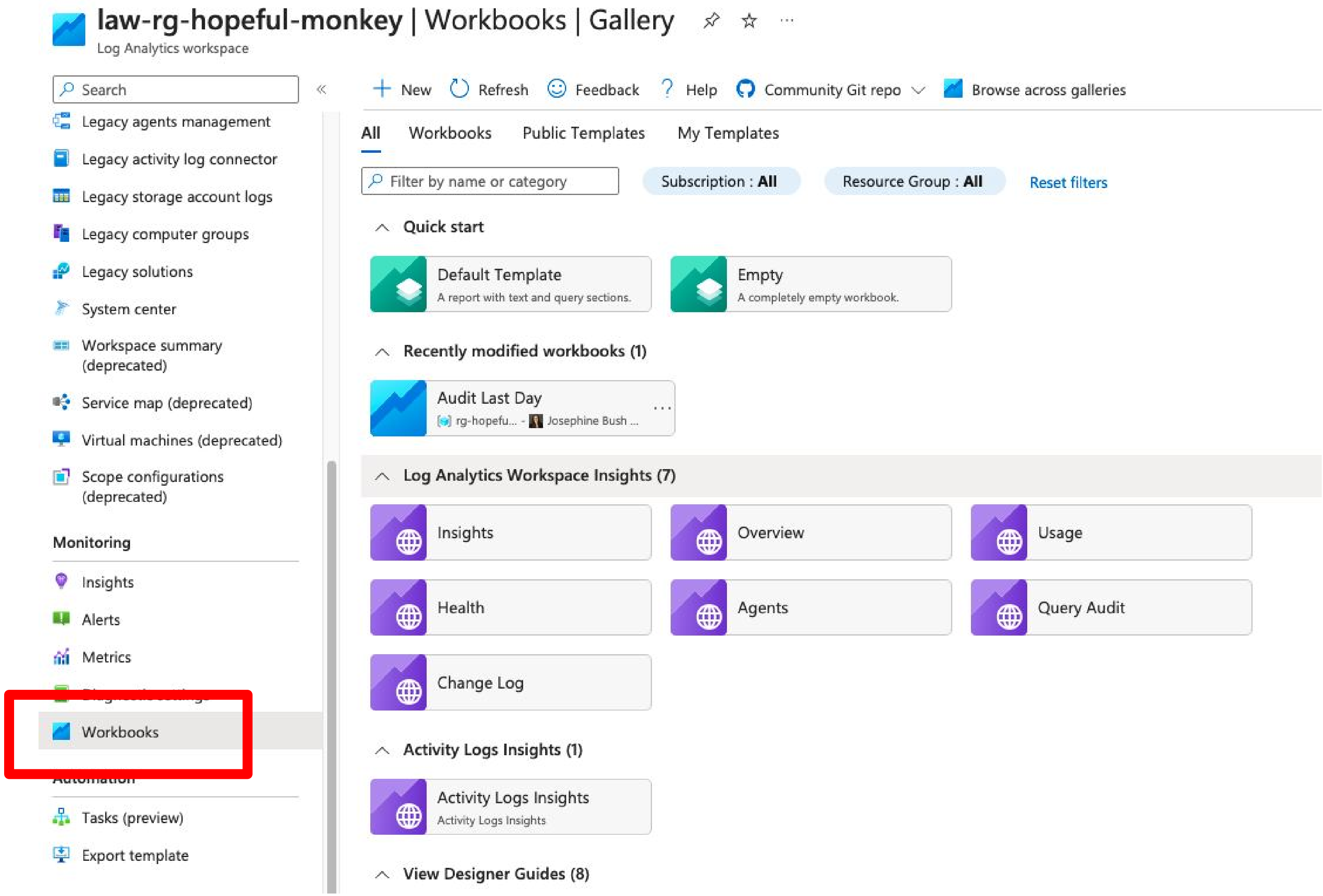
DISTRIBUTION BY DATABASE

DATABASE	COUNT
jbdb	120
master	54
	6

DISTRIBUTION BY IP

IP ADDRESS	COUNT
67.:	174
Internal	6

NEW LOG ANALYTICS WORKBOOKS



law-rg-hopeful-monkey | Workbooks | Gallery

Log Analytics workspace

Search

- Legacy agents management
- Legacy activity log connector
- Legacy storage account logs
- Legacy computer groups
- Legacy solutions
- System center
- Workspace summary (deprecated)
- Service map (deprecated)
- Virtual machines (deprecated)
- Scope configurations (deprecated)

Monitoring

- Insights
- Alerts
- Metrics
- Diagnostic settings
- Workbooks

Automation

- Tasks (preview)
- Export template

New | Refresh | Feedback | Help | Community Git repo | Browse across galleries

All | Workbooks | Public Templates | My Templates

Filter by name or category | Subscription : All | Resource Group : All | Reset filters

Quick start

- Default Template — A report with text and query sections.
- Empty — A completely empty workbook.

Recently modified workbooks (1)

- Audit Last Day — rg-hopefu... · Josephine Bush ...

Log Analytics Workspace Insights (7)

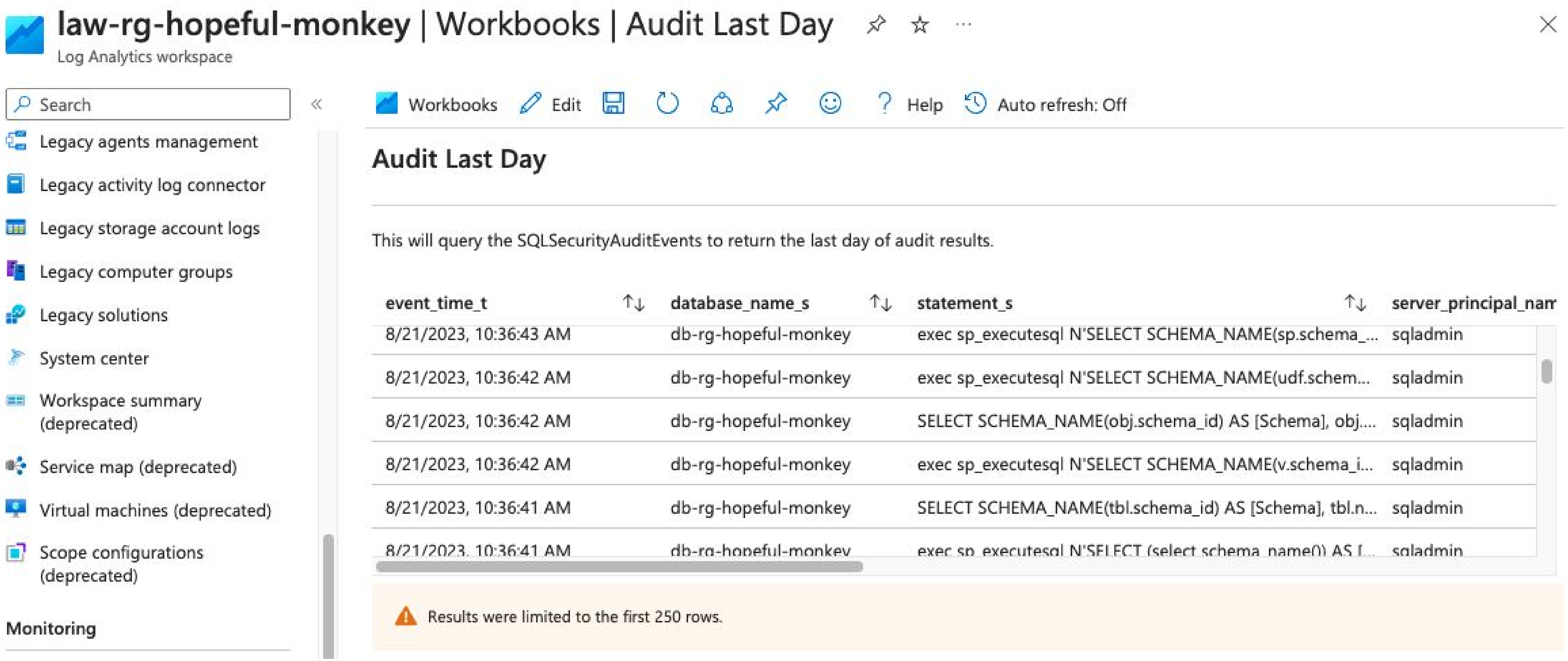
- Insights
- Overview
- Usage
- Health
- Agents
- Query Audit
- Change Log

Activity Logs Insights (1)

- Activity Logs Insights — Activity Logs Insights

View Designer Guides (8)

LOG ANALYTICS WORKBOOK EXAMPLE



law-rg-hopeful-monkey | Workbooks | Audit Last Day
Log Analytics workspace
Search
Legacy agents management
Legacy activity log connector
Legacy storage account logs
Legacy computer groups
Legacy solutions
System center
Workspace summary (deprecated)
Service map (deprecated)
Virtual machines (deprecated)
Scope configurations (deprecated)
Monitoring
Workbooks
Edit
Help
Auto refresh: Off

Audit Last Day

This will query the SQLSecurityAuditEvents to return the last day of audit results.

event_time_t	database_name_s	statement_s	server_principal_nam
8/21/2023, 10:36:43 AM	db-rg-hopeful-monkey	exec sp_executesql N'SELECT SCHEMA_NAME(sp.schema_...	sqladmin
8/21/2023, 10:36:42 AM	db-rg-hopeful-monkey	exec sp_executesql N'SELECT SCHEMA_NAME(udf.schem...	sqladmin
8/21/2023, 10:36:42 AM	db-rg-hopeful-monkey	SELECT SCHEMA_NAME(obj.schema_id) AS [Schema], obj....	sqladmin
8/21/2023, 10:36:42 AM	db-rg-hopeful-monkey	exec sp_executesql N'SELECT SCHEMA_NAME(v.schema_i...	sqladmin
8/21/2023, 10:36:41 AM	db-rg-hopeful-monkey	SELECT SCHEMA_NAME(tbl.schema_id) AS [Schema], tbl.n...	sqladmin
8/21/2023, 10:36:41 AM	db-rg-hopeful-monkey	exec sp_executesql N'SELECT (select schema_name()) AS [...	sqladmin

⚠ Results were limited to the first 250 rows.

QUERY LOG ANALYTICS AUDITING DATA

Go to your log analytics workspace

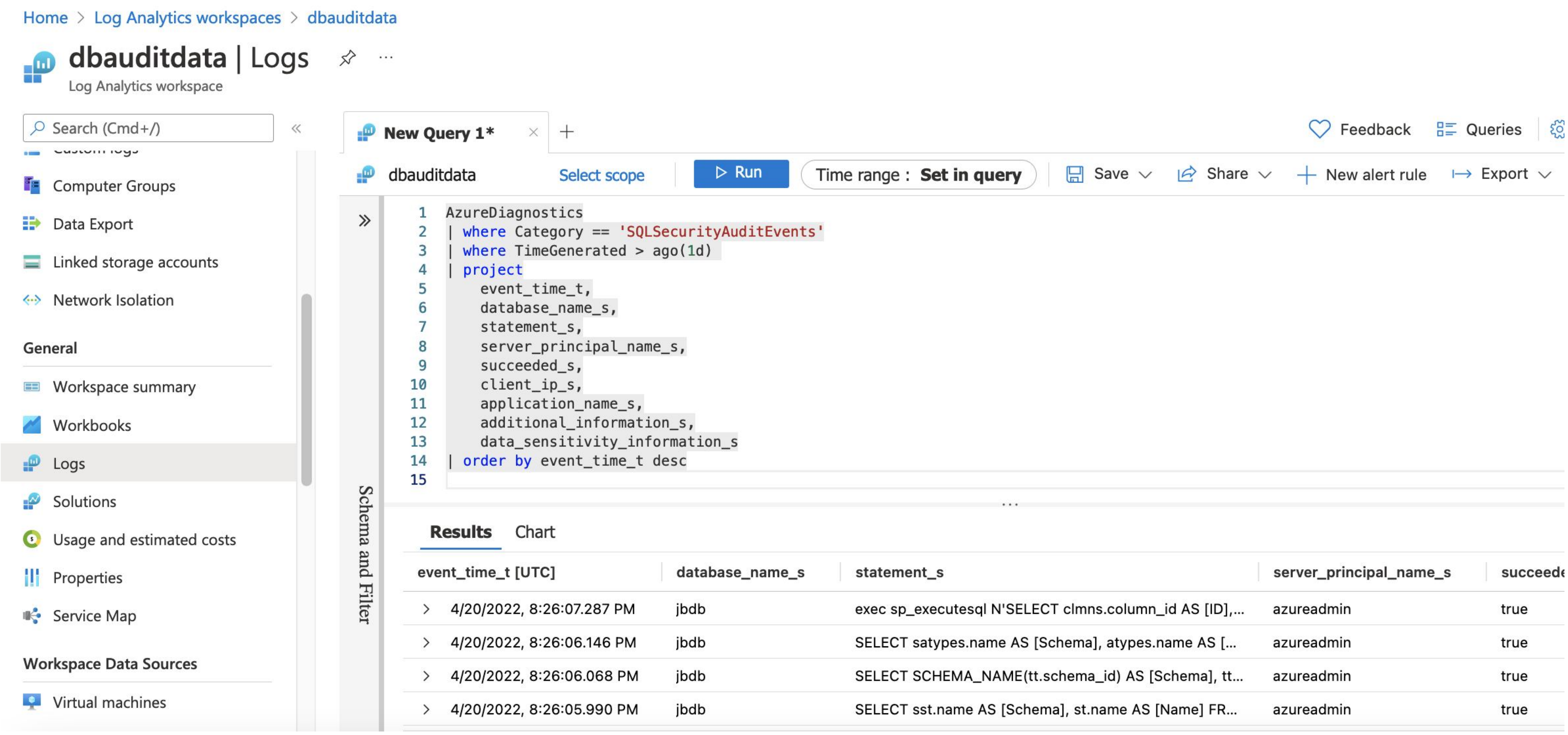
Click Logs and run a Kusto query

```
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
```

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'
```

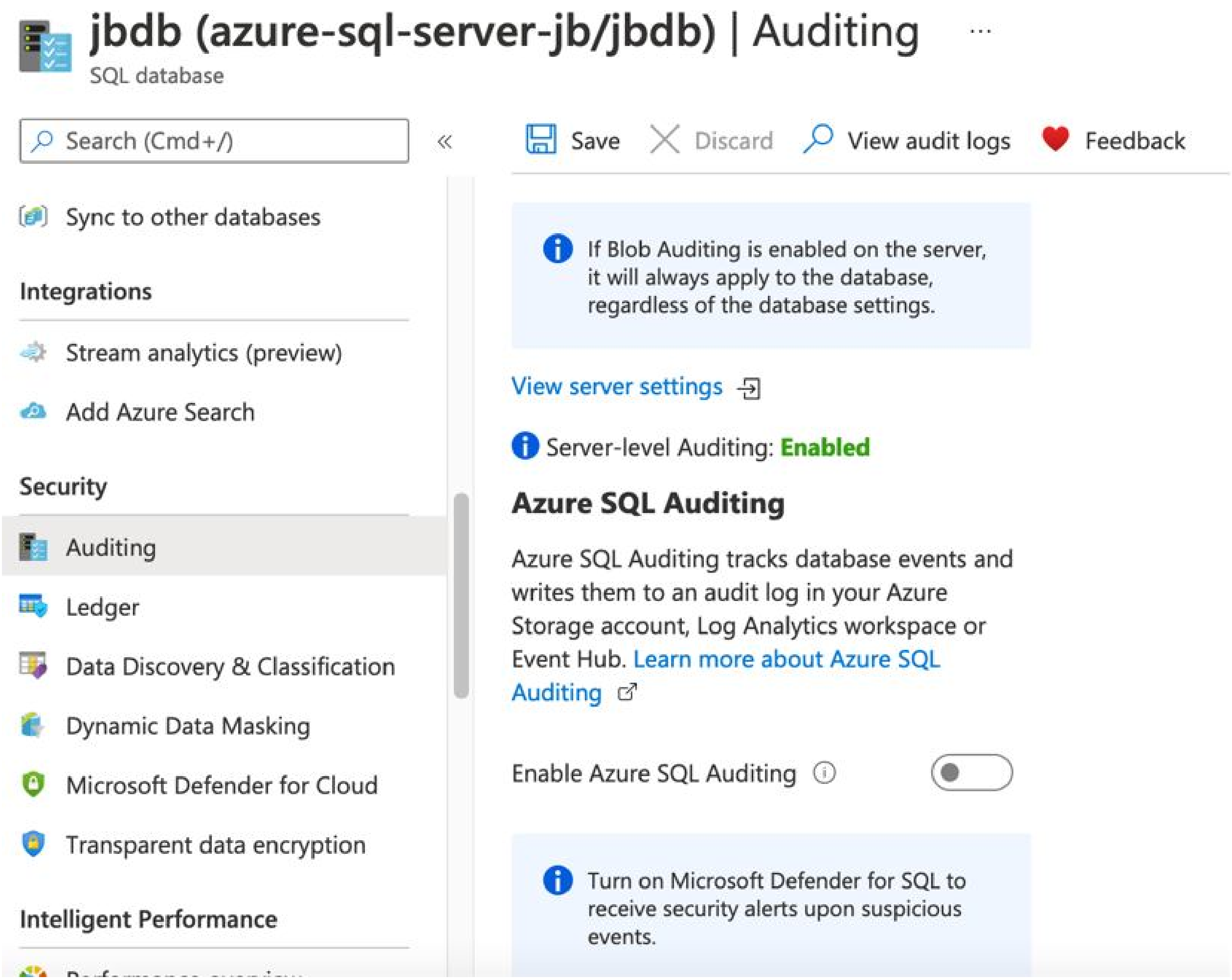
VIEW LOG ANALYTICS AUDITING DATA



```
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
```

event_time_t [UTC]	database_name_s	statement_s	server_principal_name_s	succeede
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



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

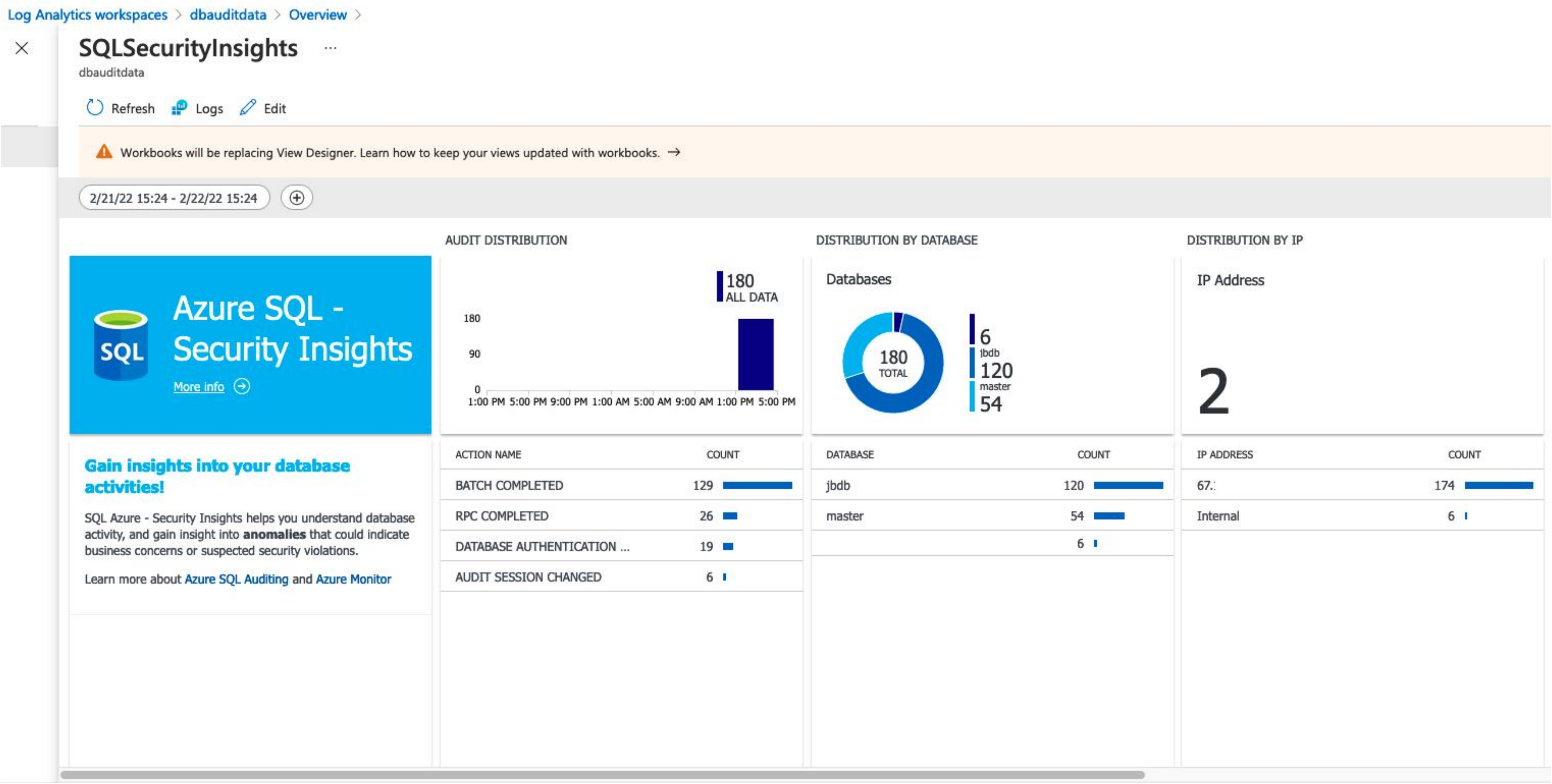
Enabling at database level instead of server level to audit only one database

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



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

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

ACTION NAME	COUNT
BATCH COMPLETED	129
RPC COMPLETED	26
DATABASE AUTHENTICATION ...	19
AUDIT SESSION CHANGED	6

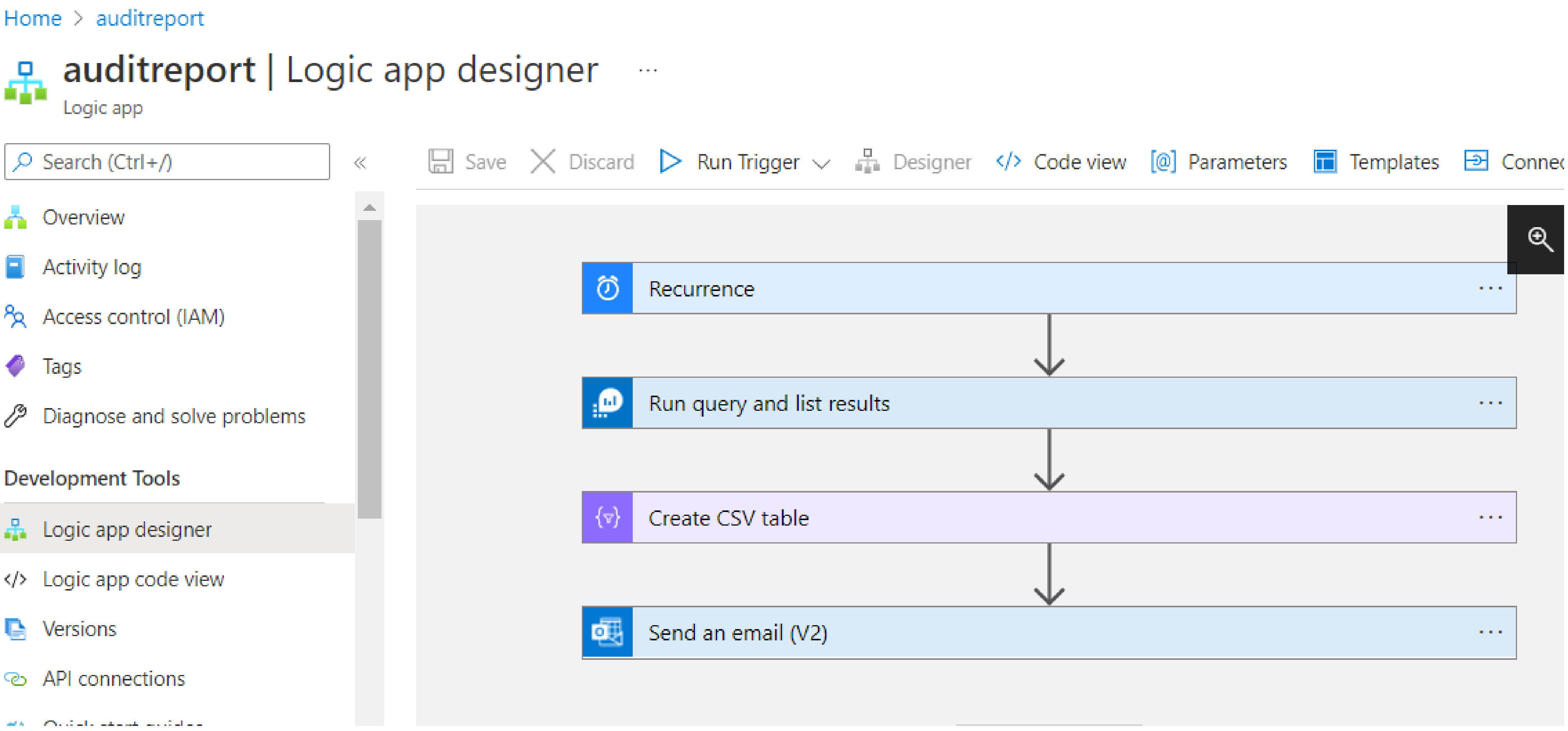
DISTRIBUTION BY DATABASE

DATABASE	COUNT
jbdb	120
master	54
	6

DISTRIBUTION BY IP

IP ADDRESS	COUNT
67.:	174
Internal	6

REPORTING ON AUDITING DATA



Recurrence

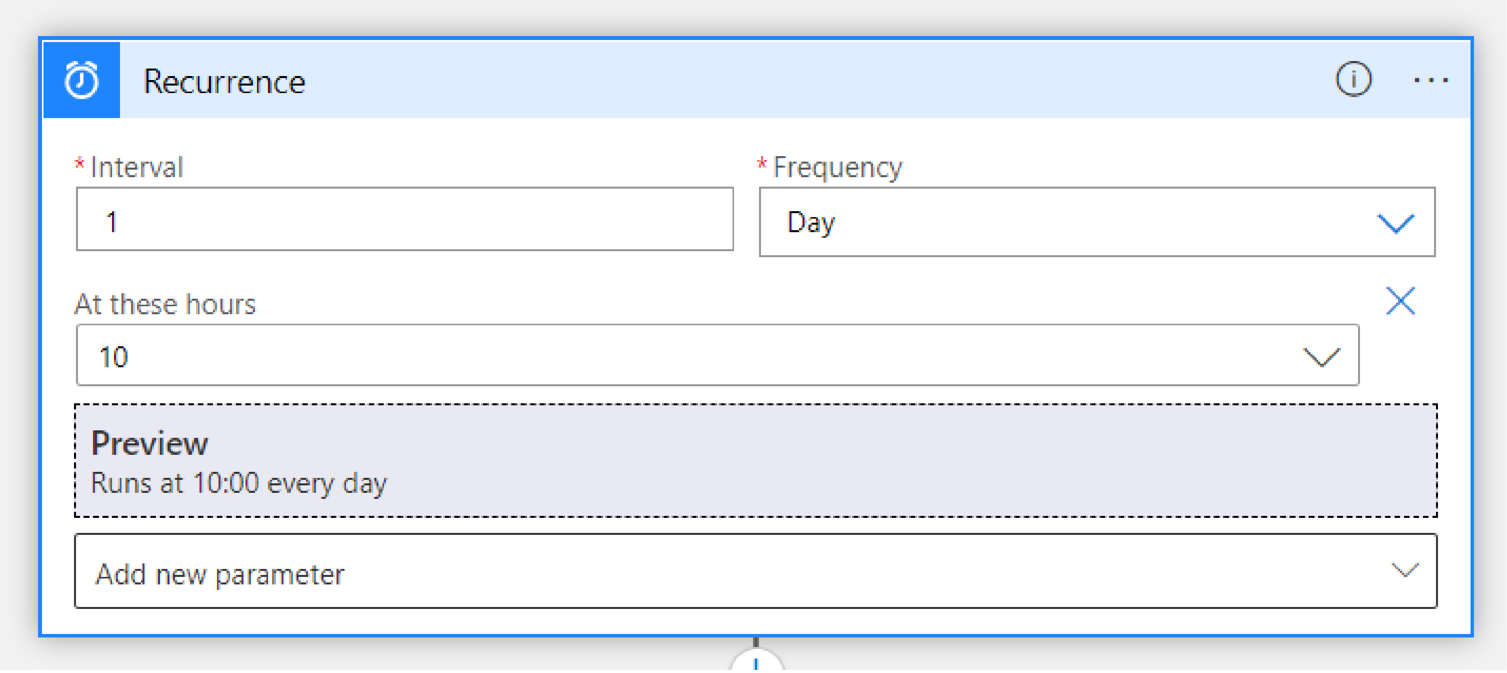
Run query and list results

Create CSV table

Send an email (V2)

SETUP LOGIC APP - RECURRENCE

Setup a schedule with Recurrence step



Recurrence

* Interval

1

* Frequency

Day

At these hours

10

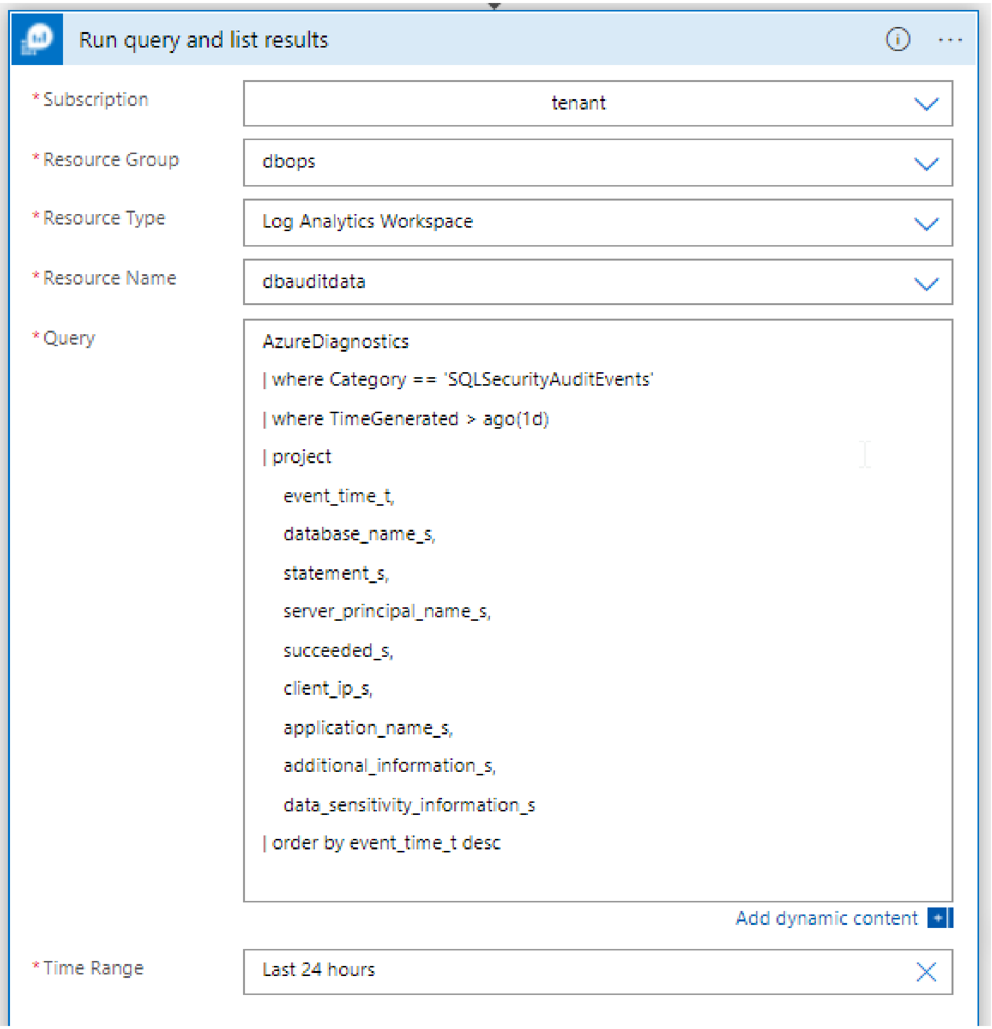
Preview

Runs at 10:00 every day

Add new parameter

SETUP LOGIC APP –KUSTO QUERY

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



Run query and list results

*Subscription: tenant

*Resource Group: dbops

*Resource Type: Log Analytics Workspace

*Resource Name: dbauditdata

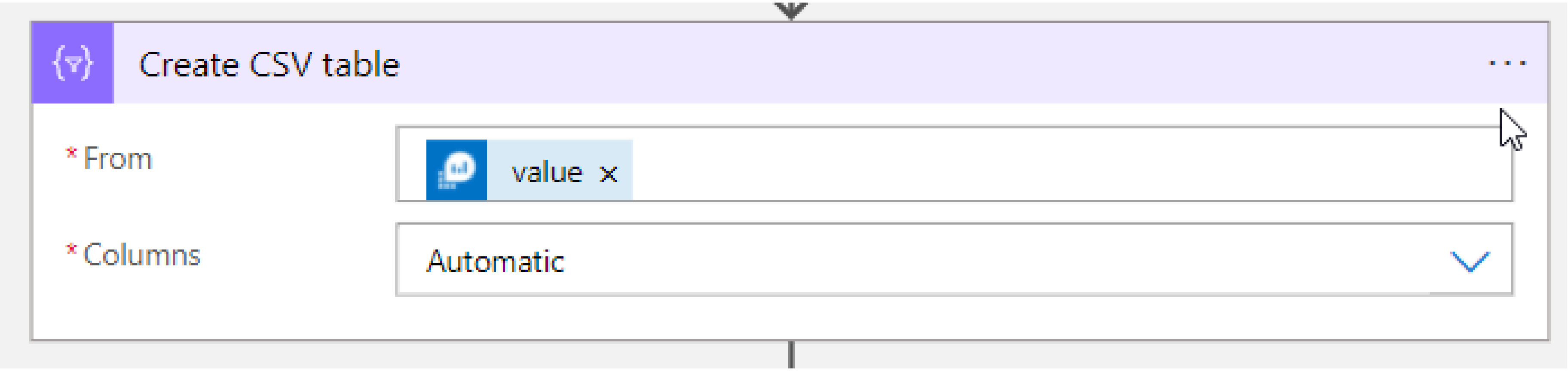
*Query

```
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

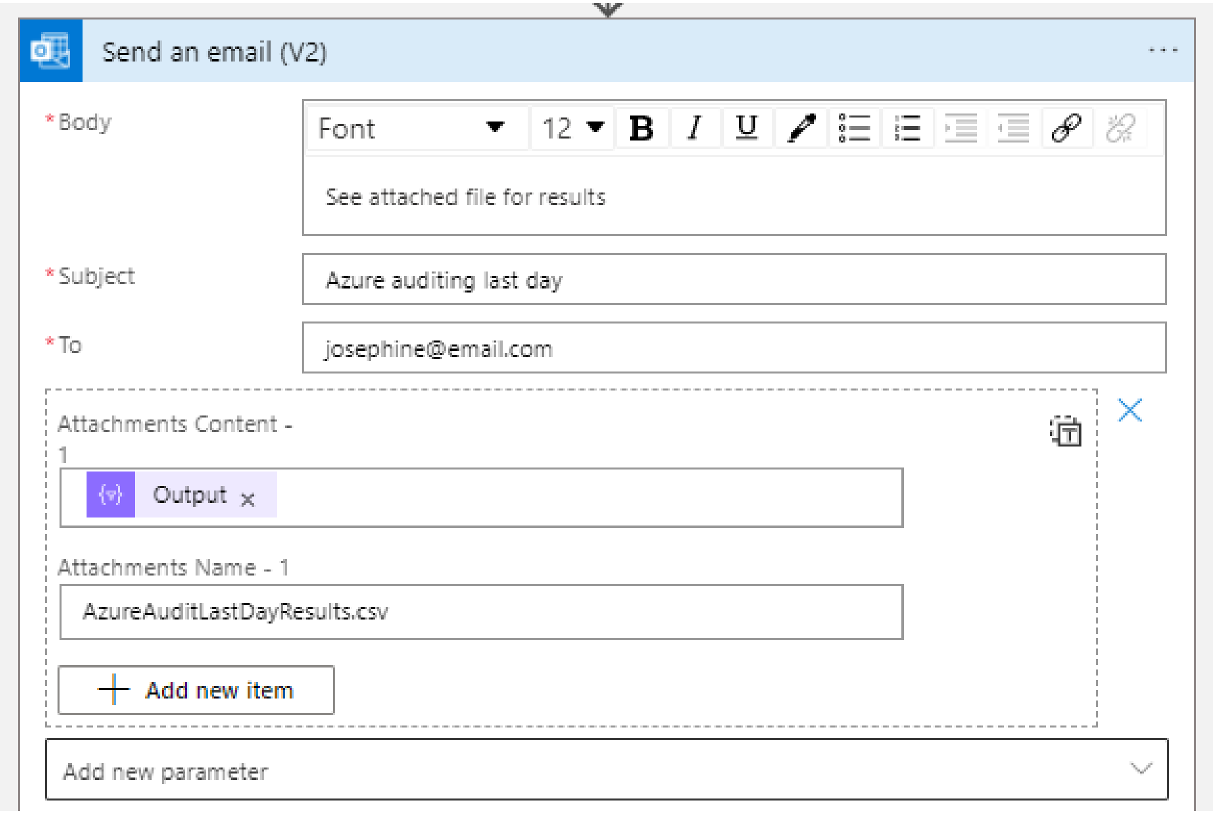


Create CSV table

* From: value

* Columns: Automatic

SETUP LOGIC APP – SEND EMAIL



Send an email (V2)

*Body

See attached file for results

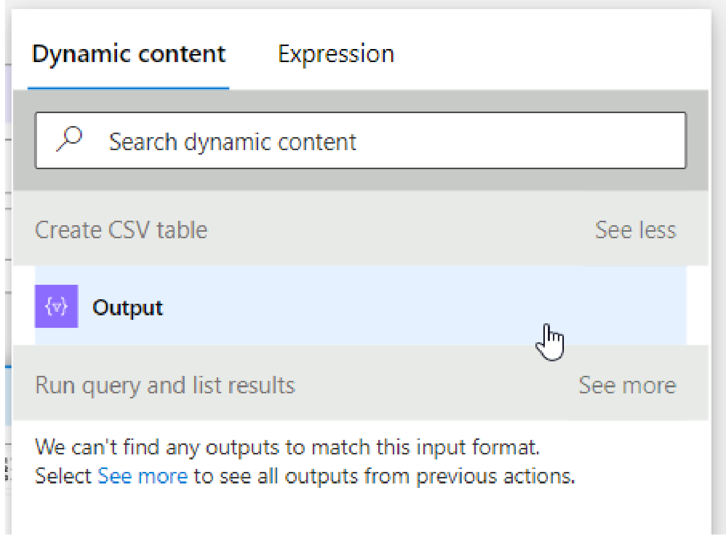
*Subject: Azure auditing last day

*To: josephine@email.com

Attachments Content - 1: Output

Attachments Name - 1: AzureAuditLastDayResults.csv

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



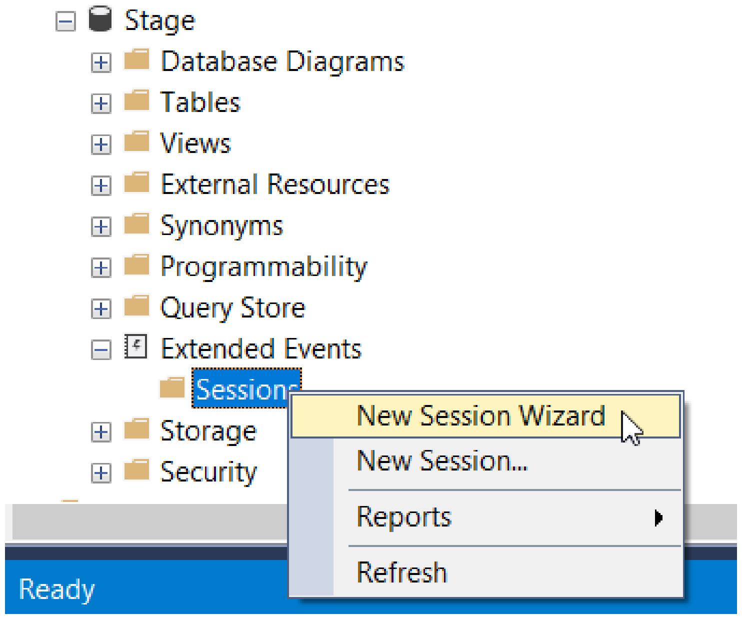
We can't find any outputs to match this input format.
Select See more to see all outputs from previous actions.

AZURE SQL AUDITING EXTENDED EVENTS

Script

```
CREATE EVENT SESSION [audit] ON DATABASE
ADD EVENT
sqlserver.rpc_completed(  ACTION(sqlserver.client_app_na
me,sqlserver.client_hostname,sqlserver.database_name,sql
server.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_n
ame,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)
```

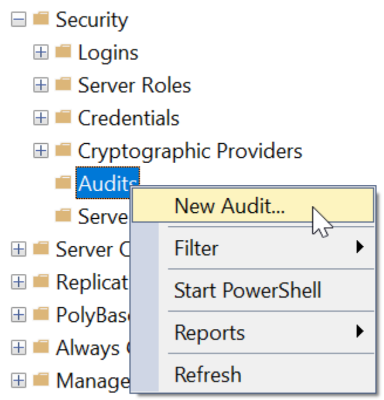
GUI

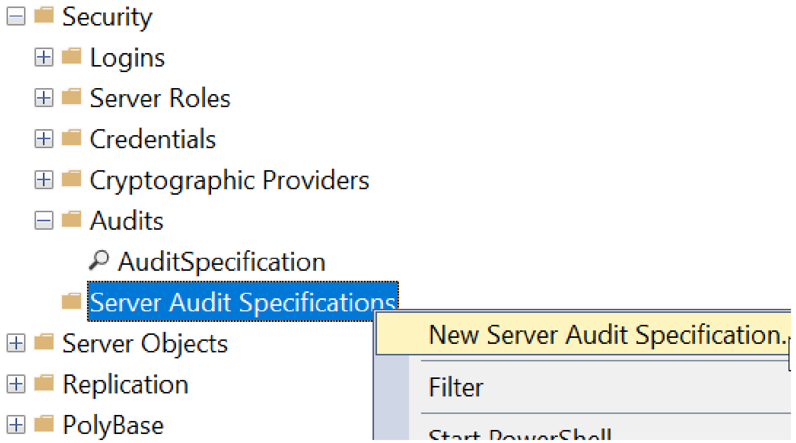


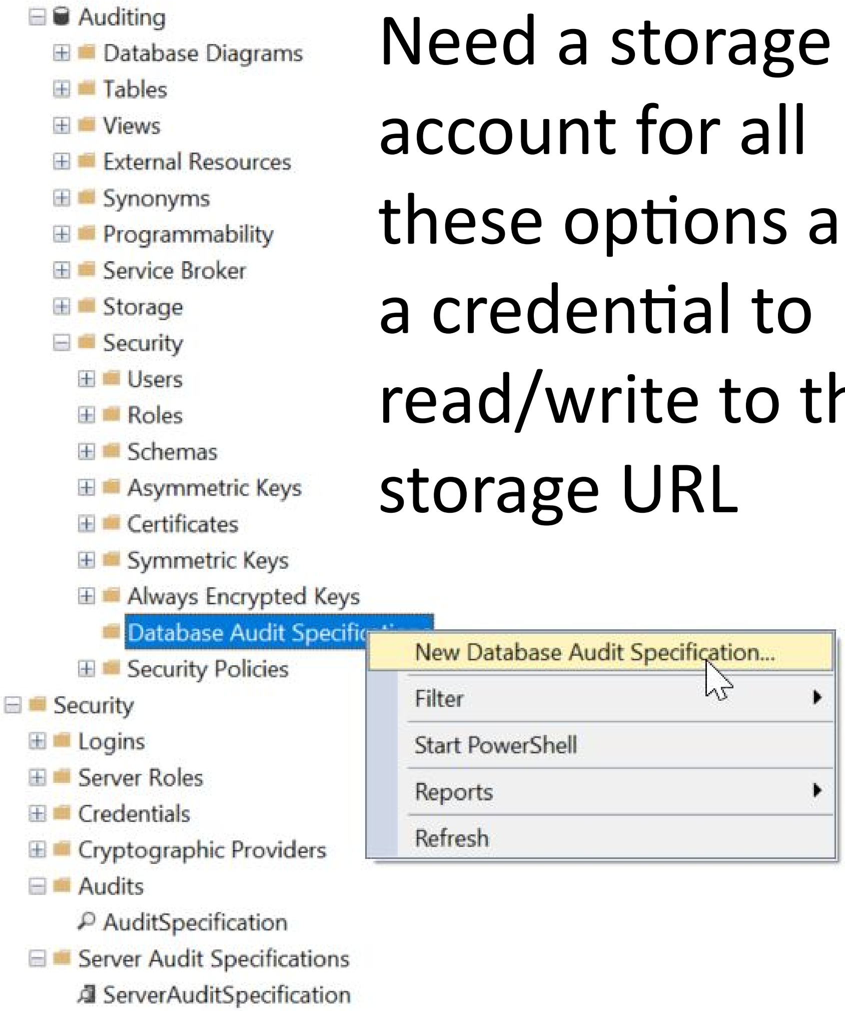
You need a credential setup to use the URL to the storage account in the filename

MANAGED INSTANCE AUDITING

SQL Server Audit

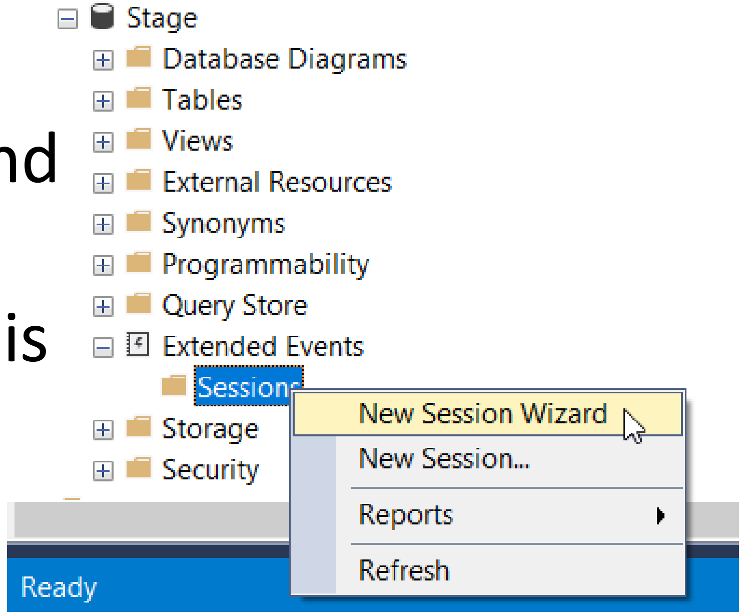






Need a storage account for all these options and a credential to read/write to this storage URL

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

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

THANK YOU FOR ATTENDING

Contact me @hellosqlkitty

or visit me at sqlkitty.com