HANDLE AZURE SQL AUDITING WITH EASE

Josephine Bush

She/Hers

DBA, MBA, Author

ABOUT ME

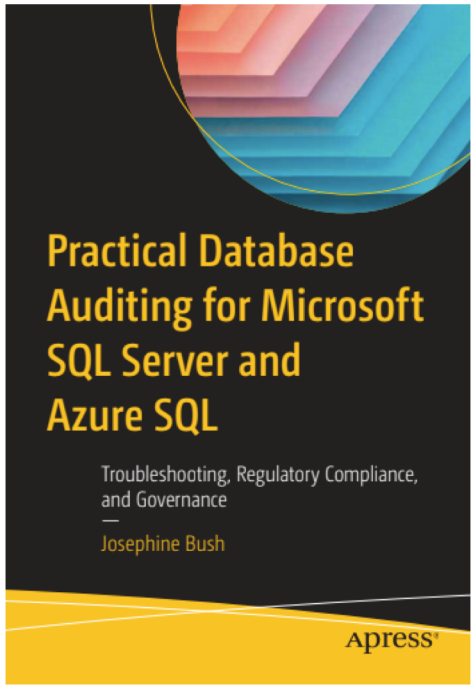
PASS Data Community SUMMIT 2022

Josephine Bush

10+ years DBA experience

MBA IT Management

MS Data Analytics

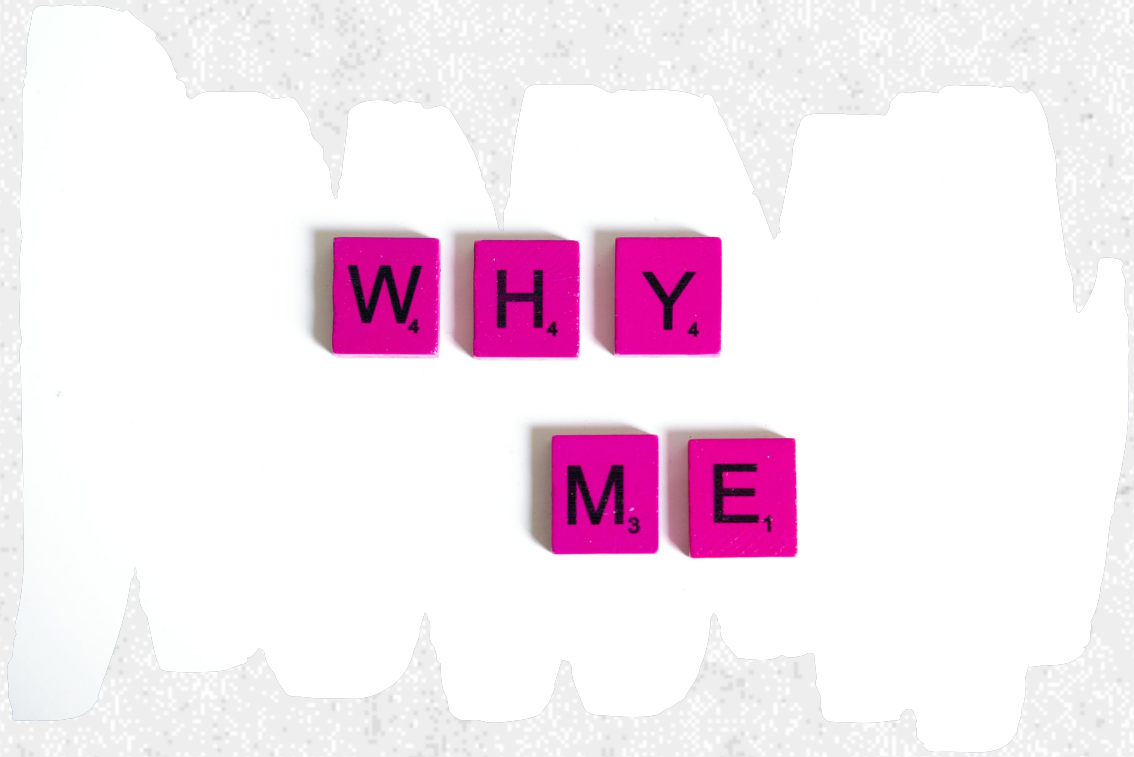




@hellosqlkitty
sqlkitty.com

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….

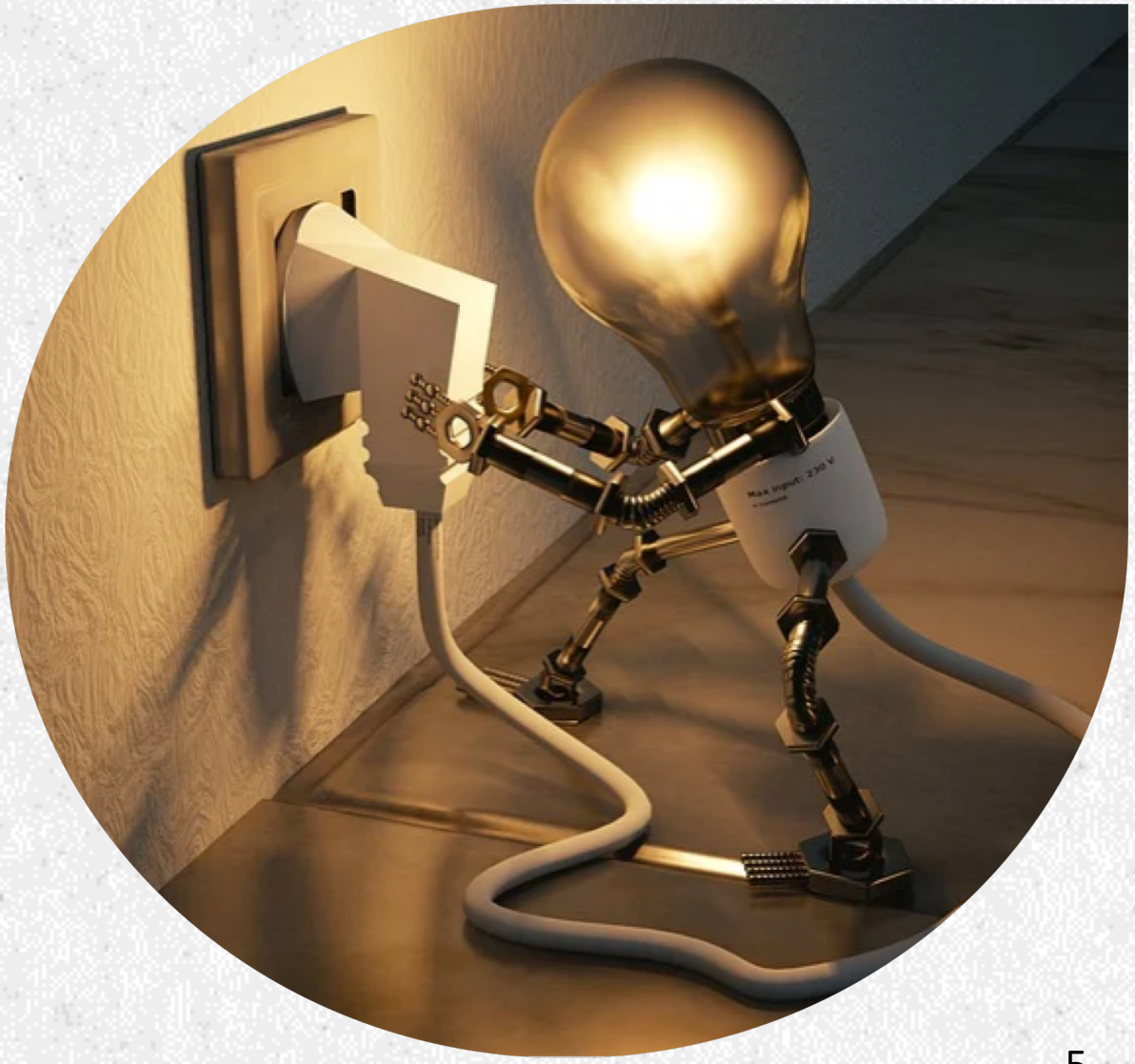
PROBLEMS AUDITING CAN SOLVE

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'

```
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

PASS Data Community SUMMIT 2022

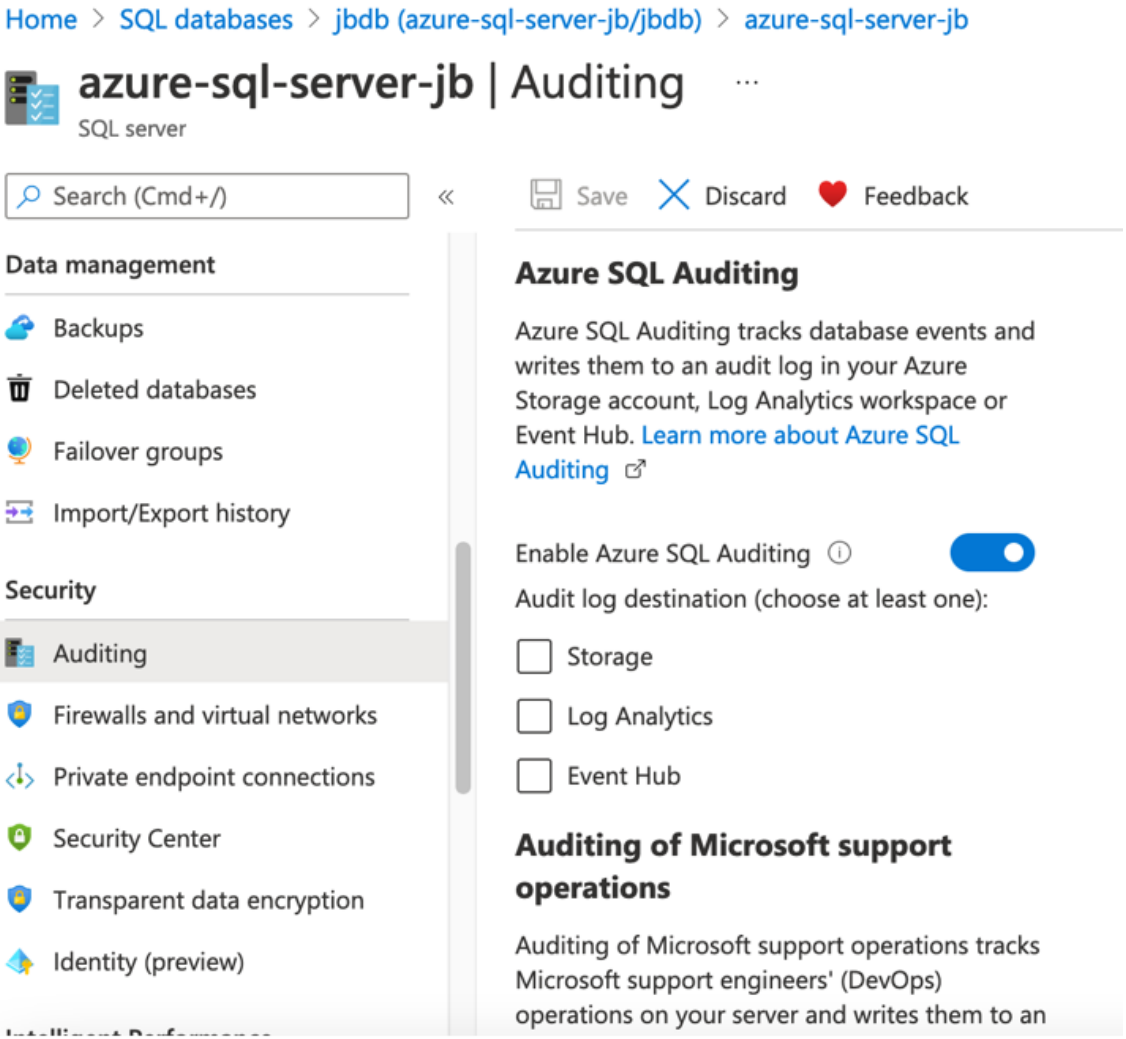
To change your current auditing policy:

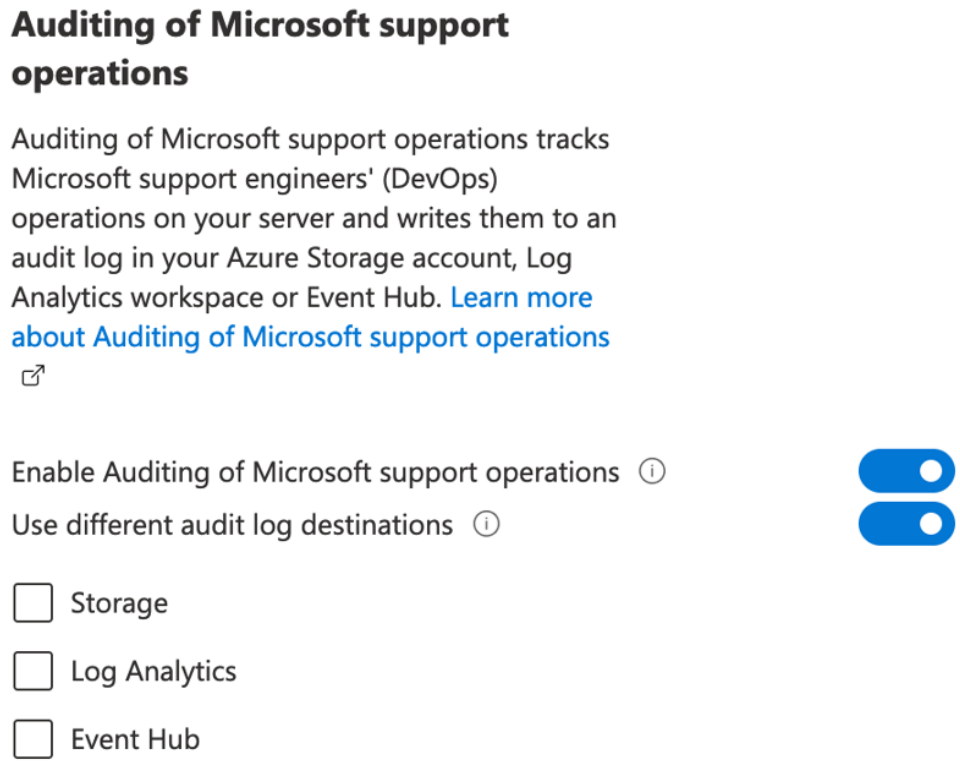
```
Set-AzSqlServerAudit -ResourceGroupName 'dbops' -ServerName 'auditingtest' `
-AuditActionGroup APPLICATION_ROLE_CHANGE_PASSWORD_GROUP,
DATABASE_CHANGE_GROUP, `
DATABASE_OBJECT_CHANGE_GROUP, DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP, `
DATABASE_OBJECT_PERMISSION_CHANGE_GROUP, DATABASE_OWNERSHIP_CHANGE_GROUP, `
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'

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



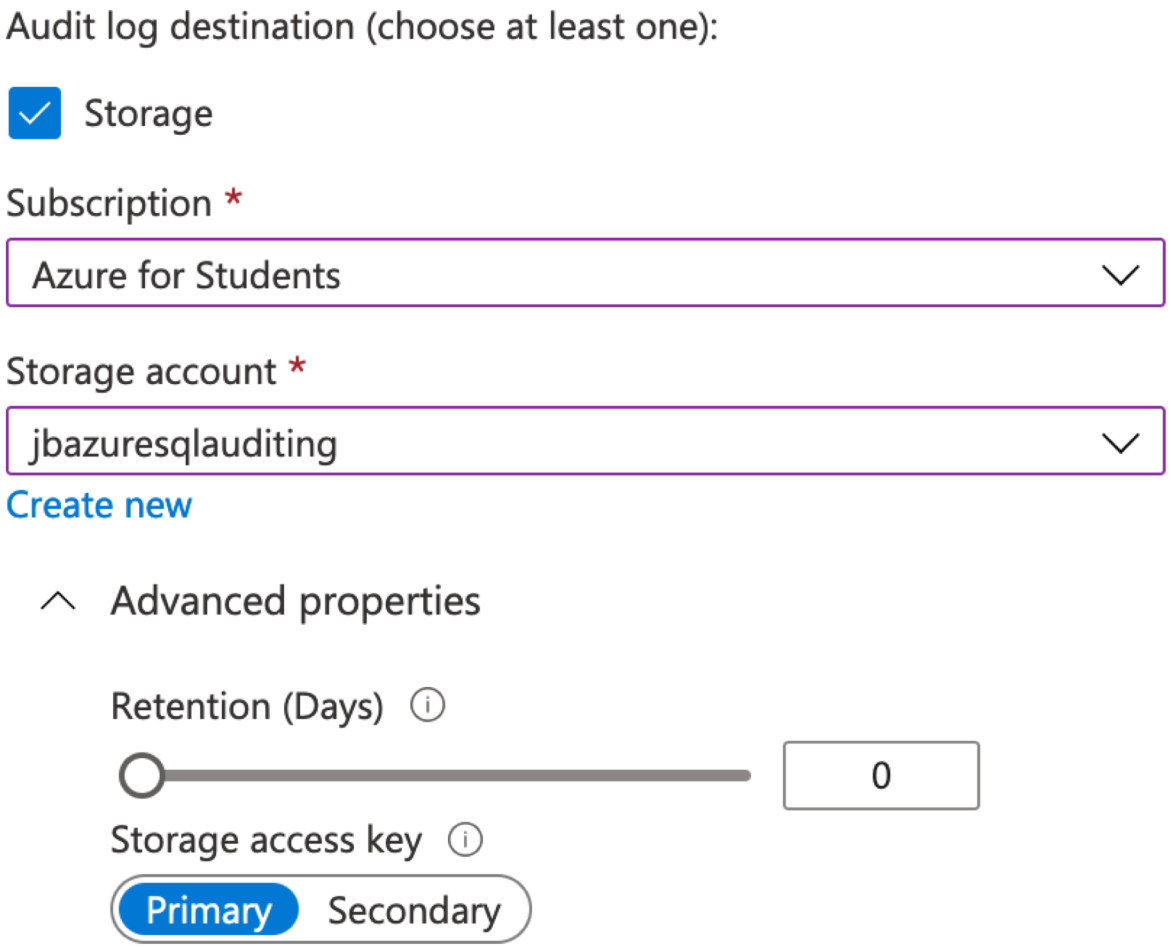


AZURE SQL AUDITING OPTIONS

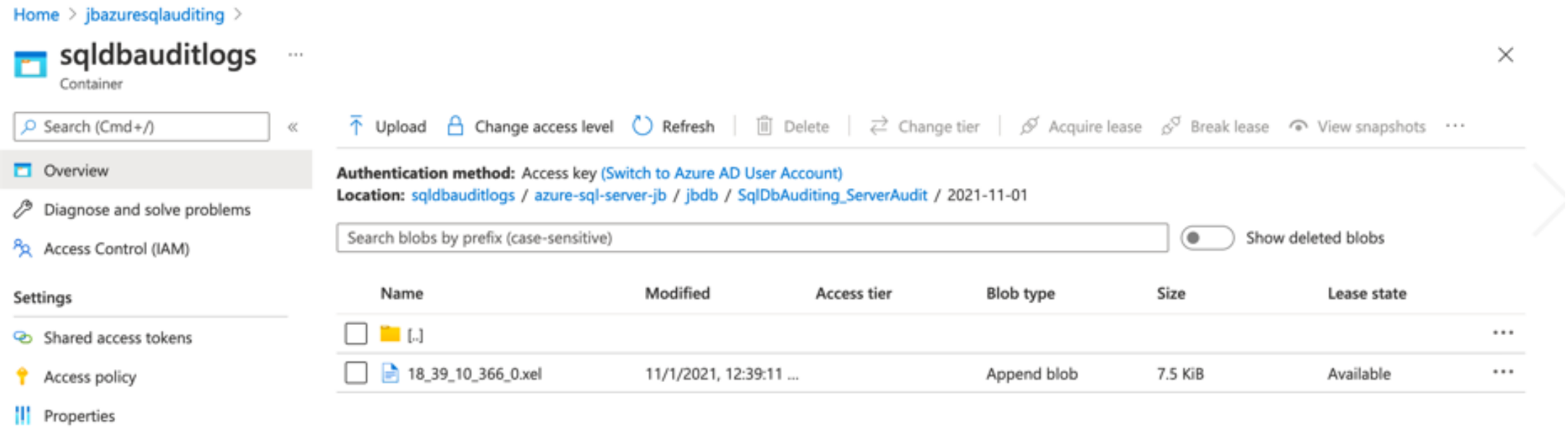
Audit log destination (choose at least one):

- [ ] Storage
- [ ] Log Analytics
- [ ] Event Hub

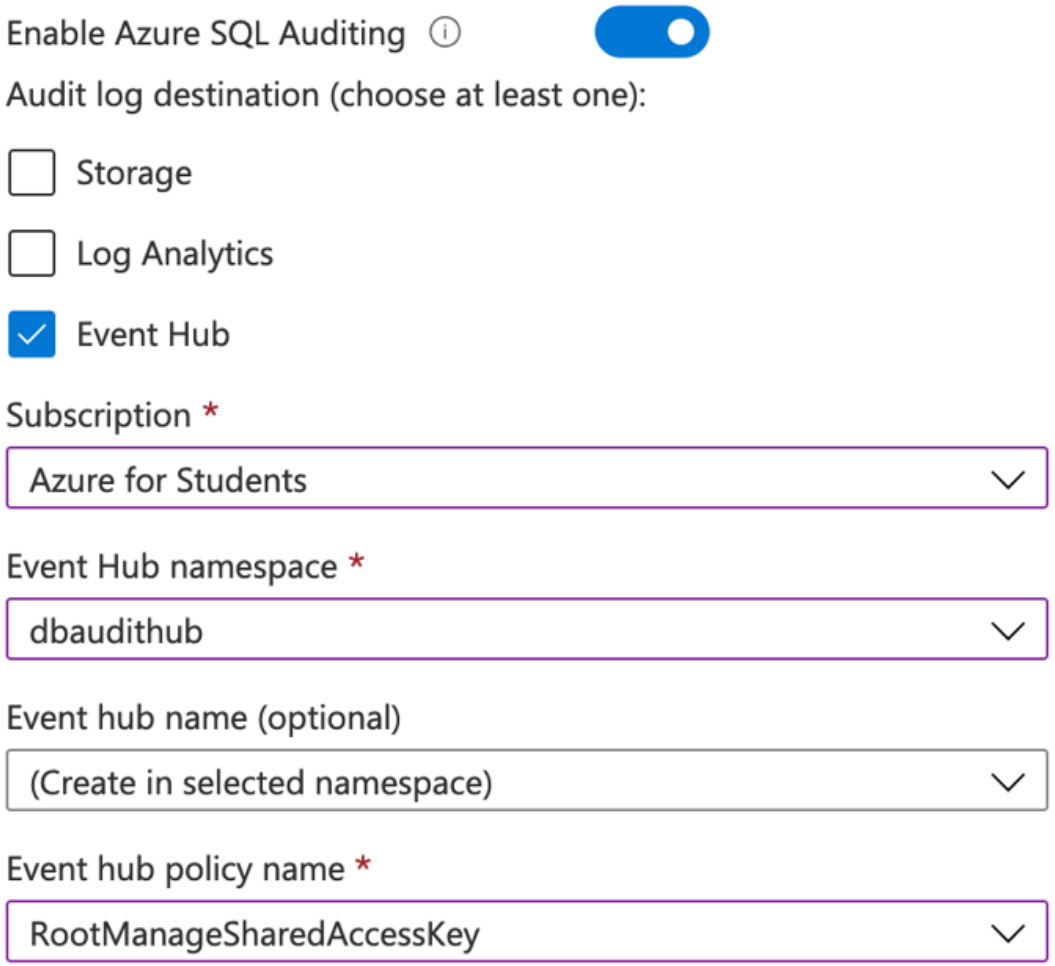
AZURE SQL AUDITING STORAGE



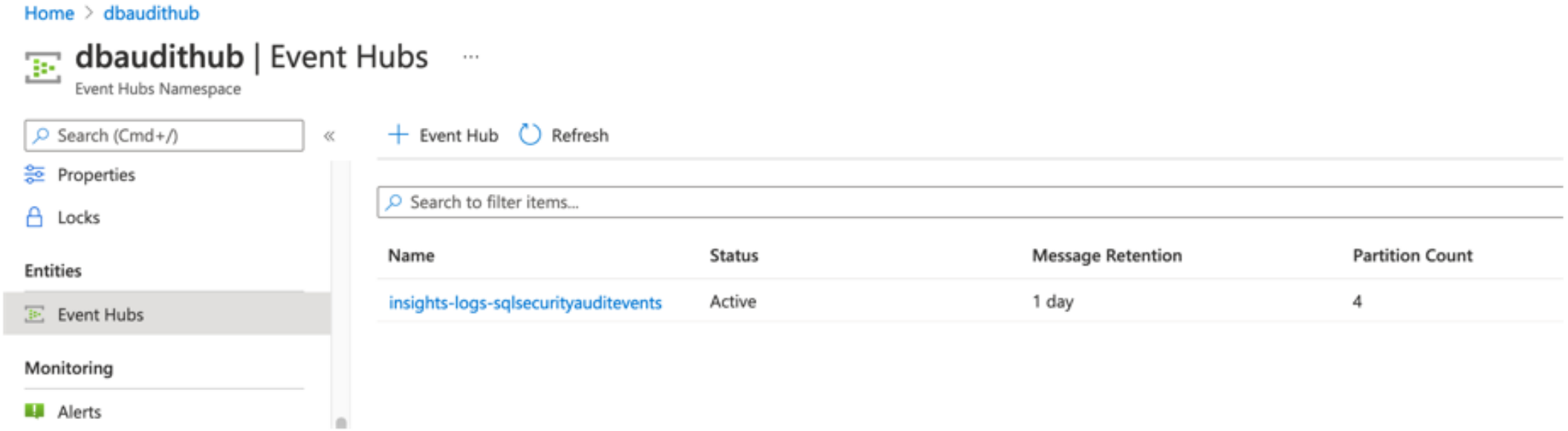
AZURE SQL AUDITING STORAGE FILES



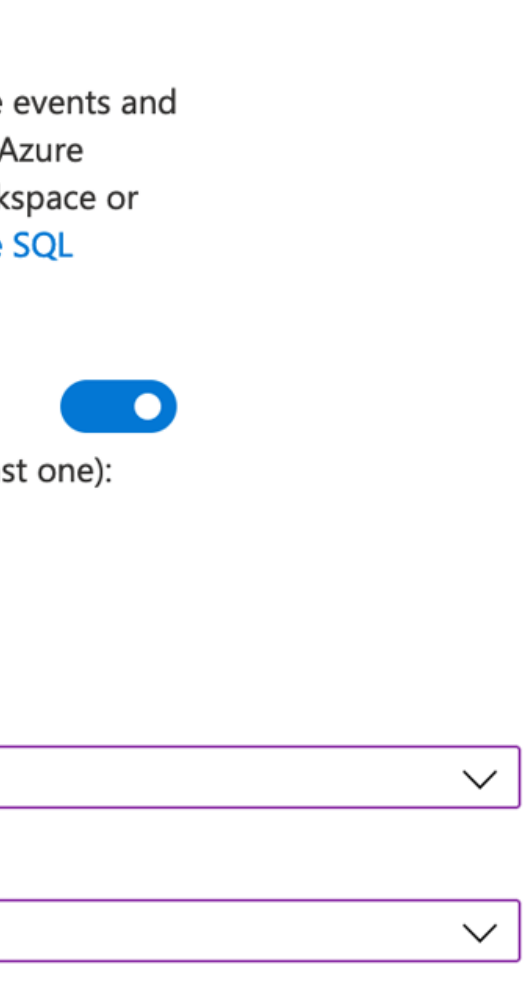
AZURE SQL AUDITING EVENT HUB



AZURE SQL AUDITING EVENT HUB DATA



AZURE SQL AUDITING LOG ANALYTICS



AZURE LOG ANALYTICS PRICING

PASS Data Community SUMMIT 2022

Ingesting data

Region: East US 2 | Currency: United States – Dollar ($) USD

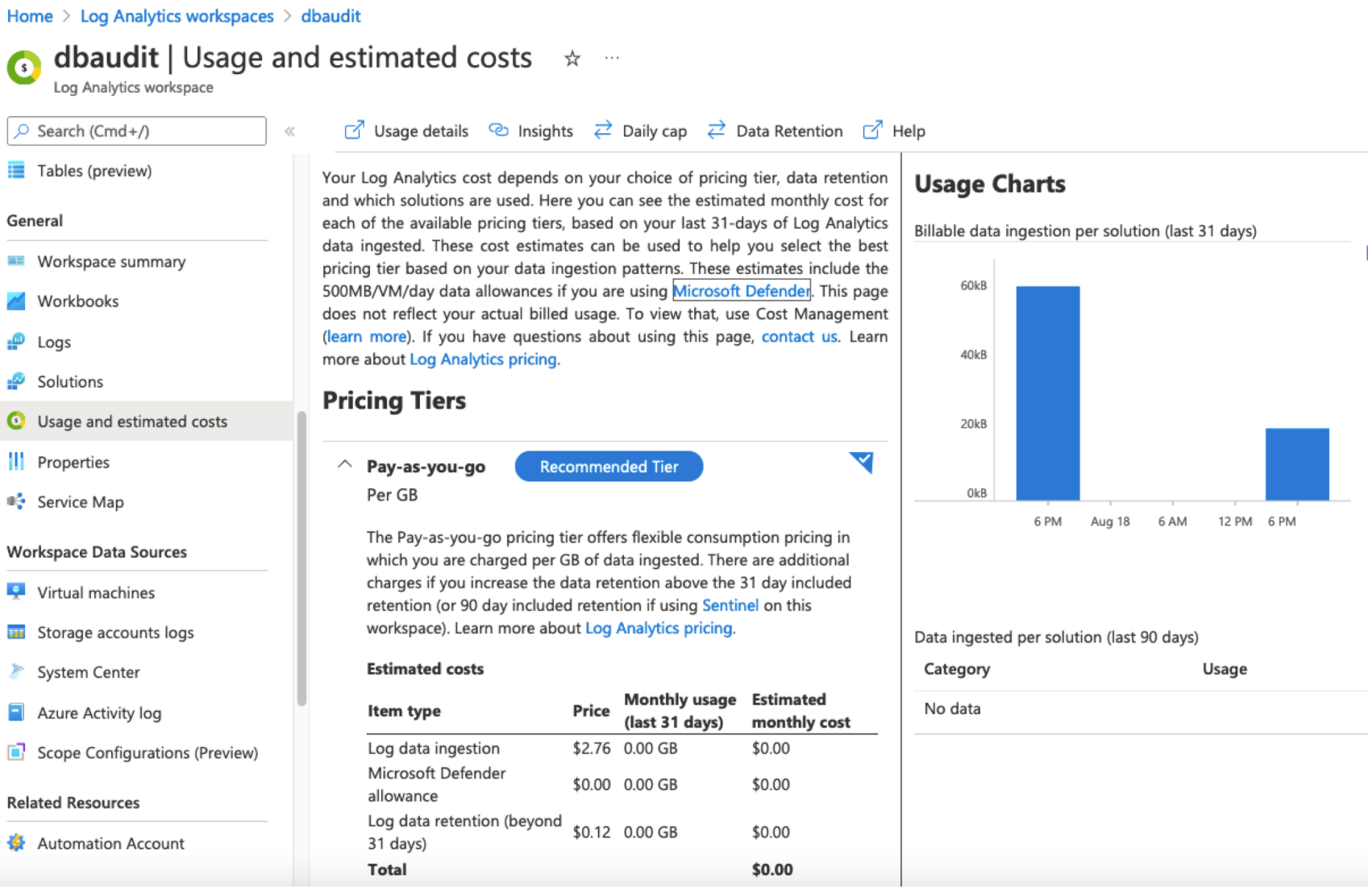
Pricing Tier	Price	Effective Per GB Price[1]	Savings Over Pay-As-You-Go
Pay-As-You-Go	**$2.76** per GB (5 GB per billing account per month included)	**$2.76** per GB	N/A
100 GB per day	**$196** per day	**$1.96** per GB	29%

Retaining data

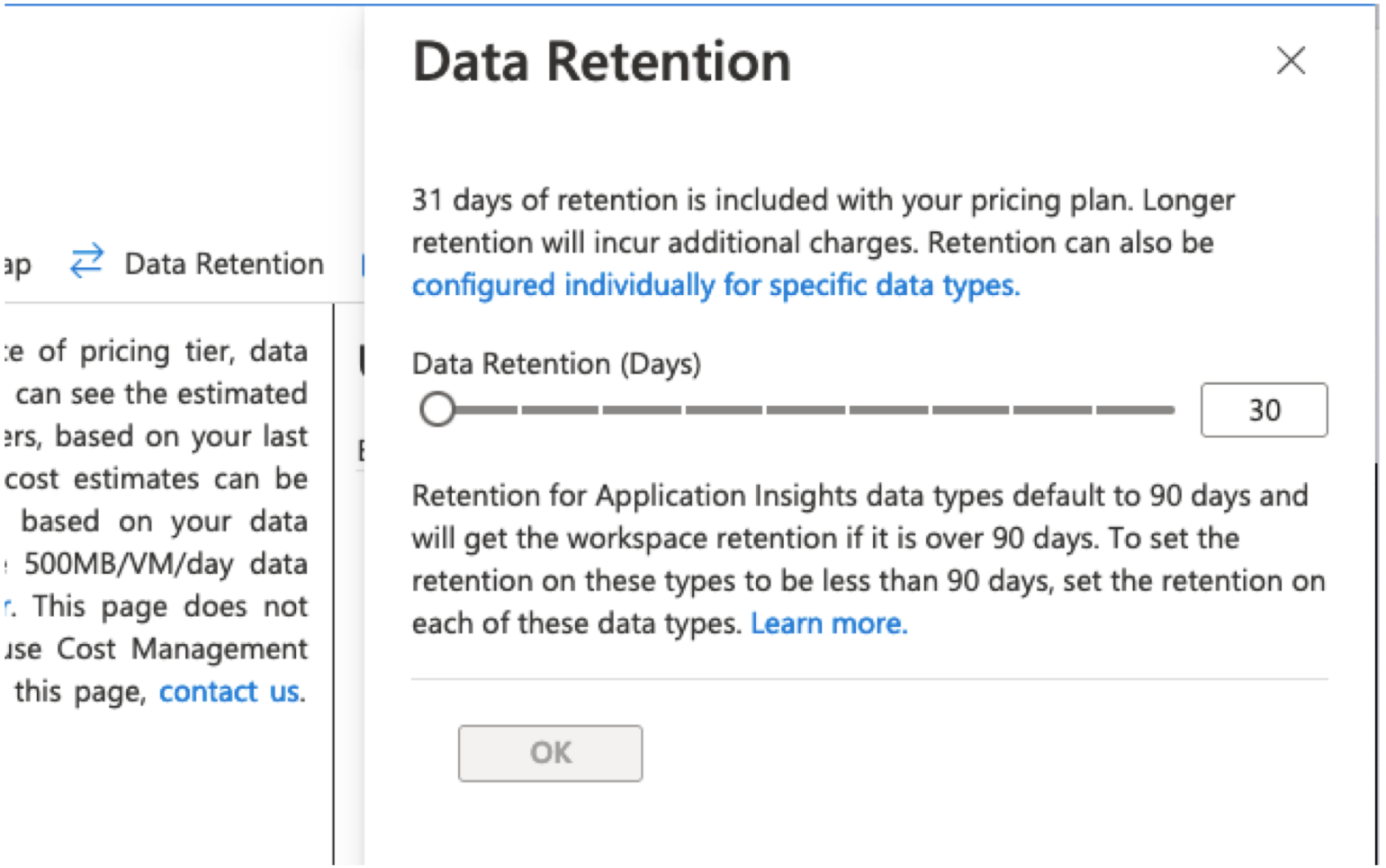
Region: East US 2 | Currency: United States – Dollar ($) USD

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



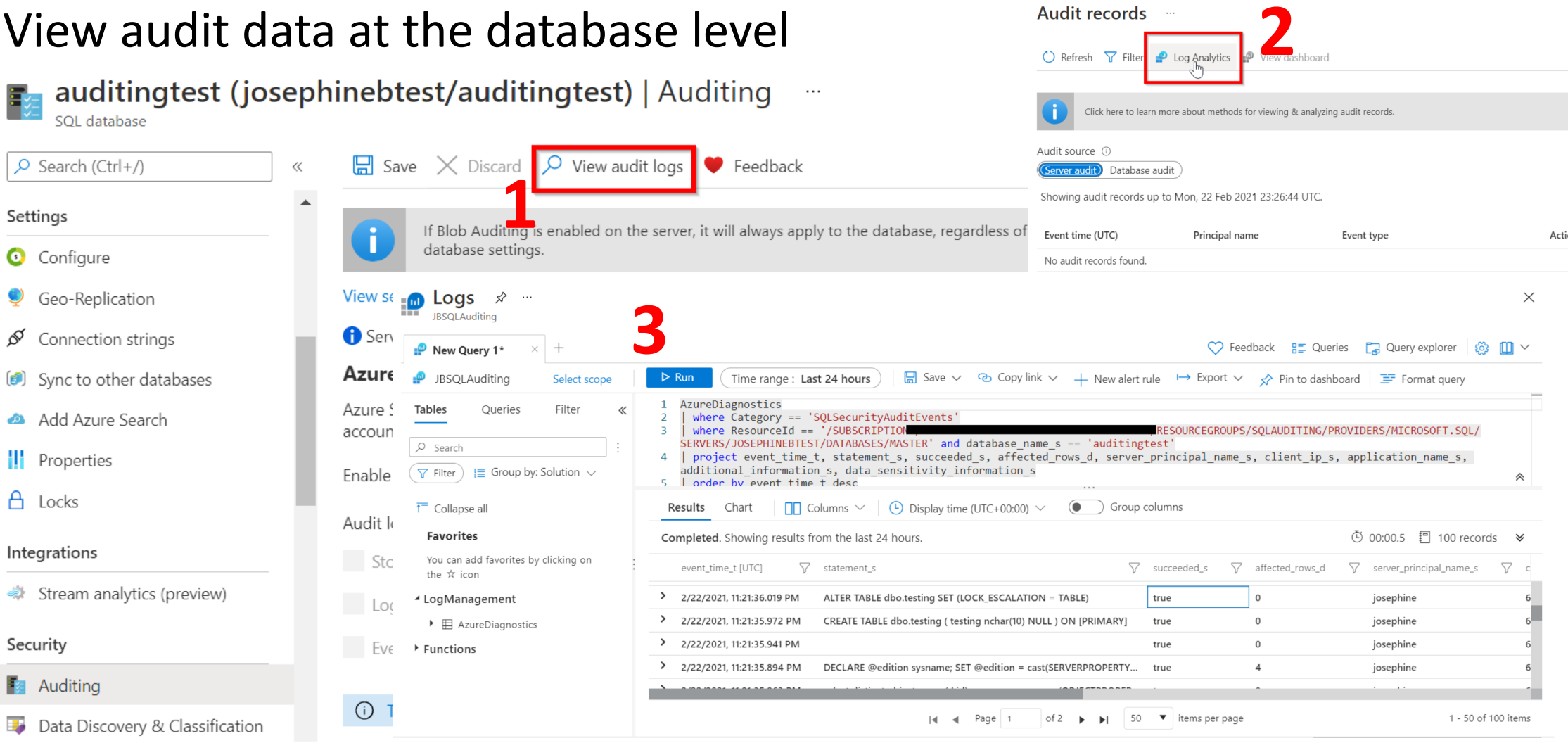
AZURE LOG ANALYTICS RETENTION



VIEW LOG ANALYTICS AUDIT DATA

PASS Data Community SUMMIT 2022

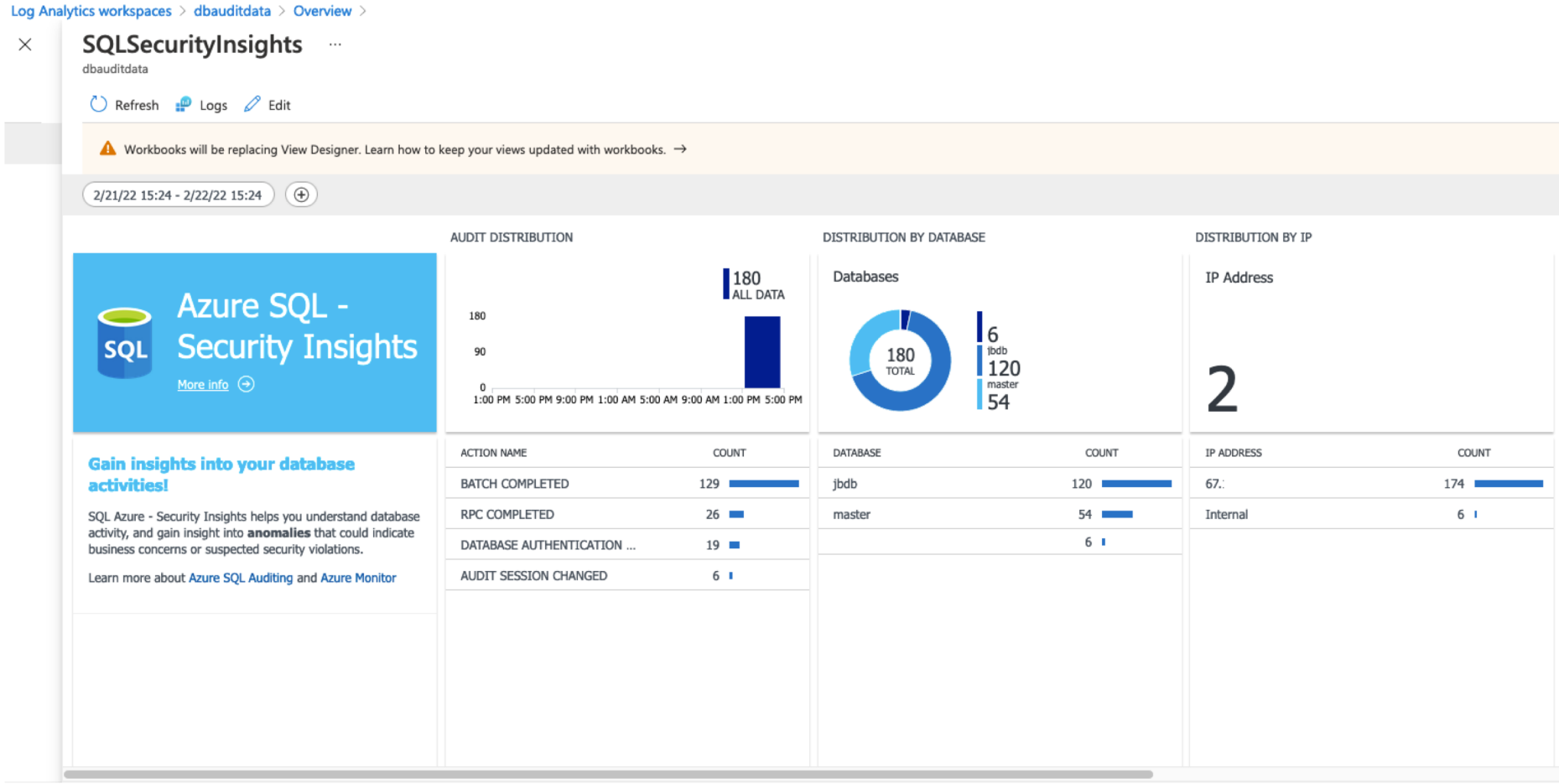
View audit data at the database level



VIEW LOG ANALYTICS WORKSPACE

PASS Data Community SUMMIT 2022

View audit data in workspace summary



QUERY LOG ANALYTICS AUDITING DATA

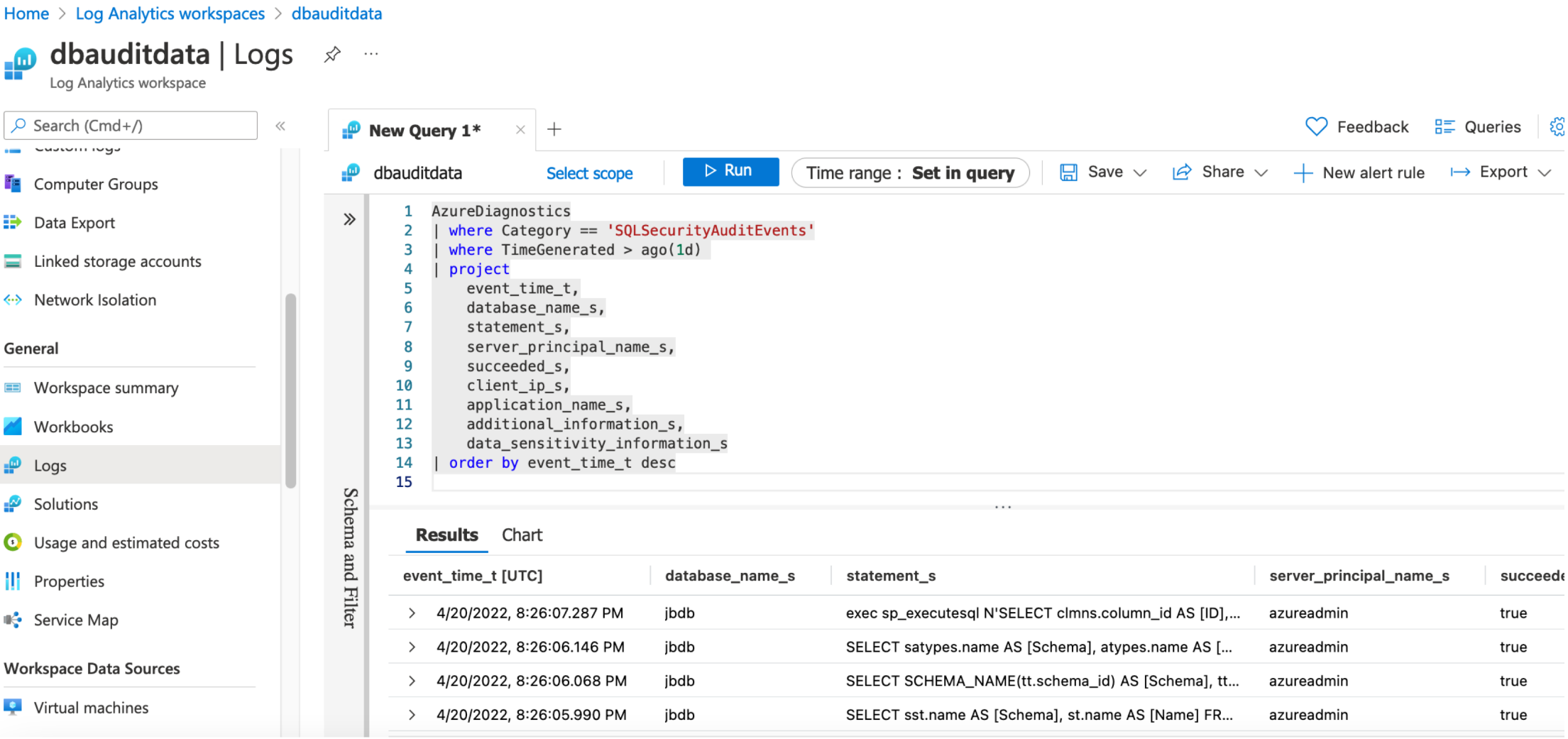
Go to your log analytics workspace
Click Logs and run a Kusto query

```
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
```

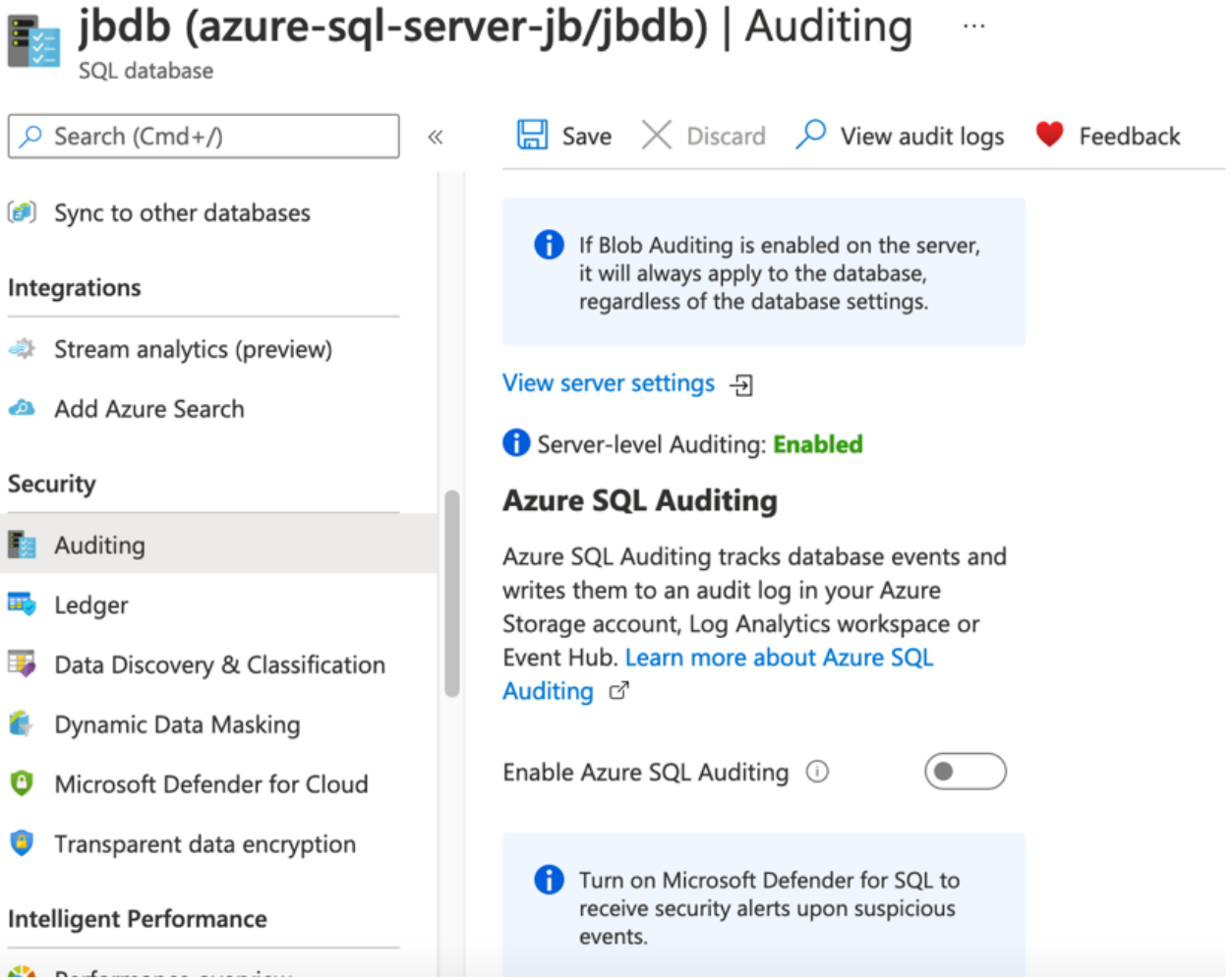
You may need to filter on this if you are seeing a lot of entries for this user:

```
and server_principal_name_s !=
'NT AUTHORITY\\SYSTEM'
```

VIEW LOG ANALYTICS AUDITING DATA



ENABLING AZURE SQL AUDITING



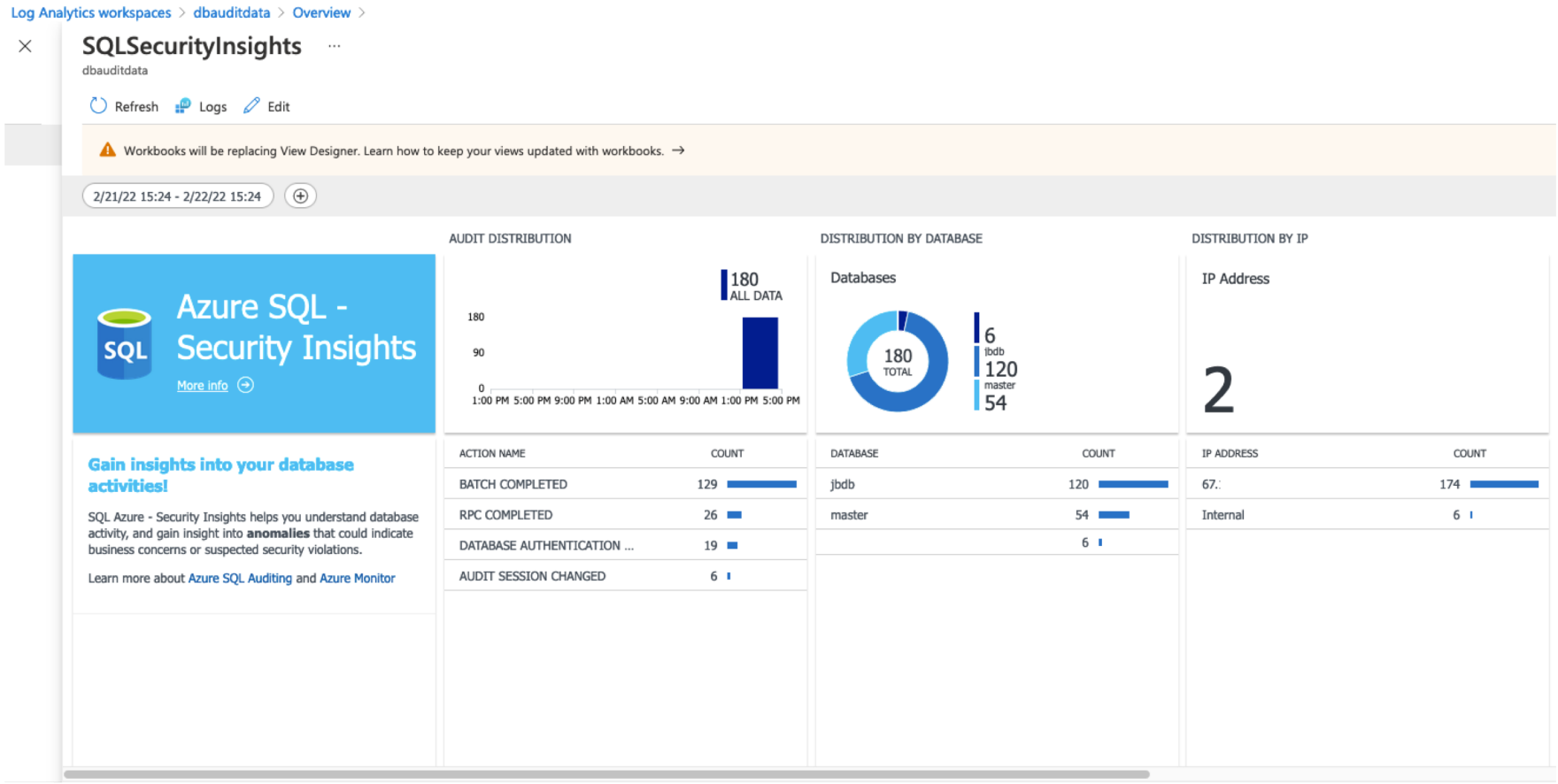
Enabling at database level instead of server level to audit only one database

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

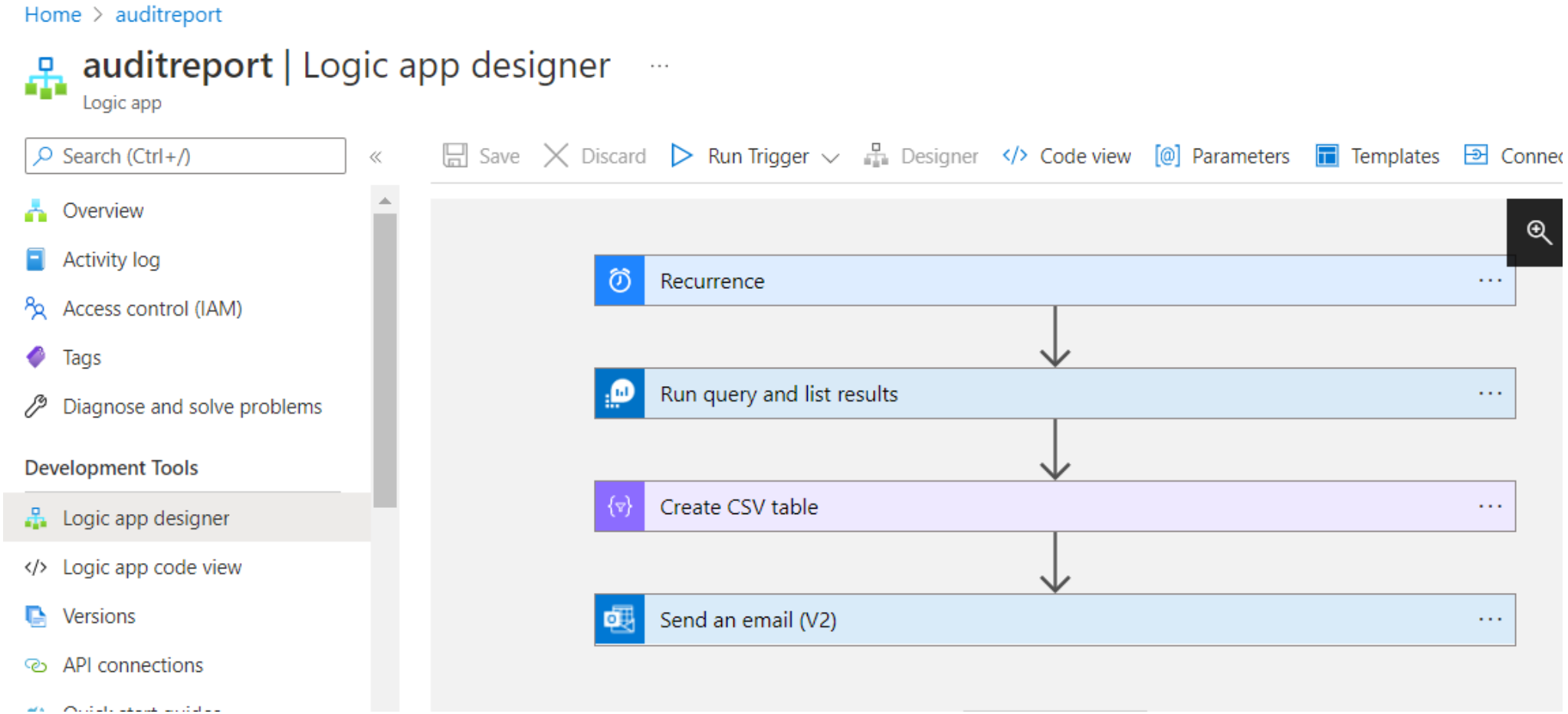
AZURE SQL AUDITING DEMO

CENTRALIZING AUDITING DATA

Store Azure SQL audit data in the same log analytics workspace



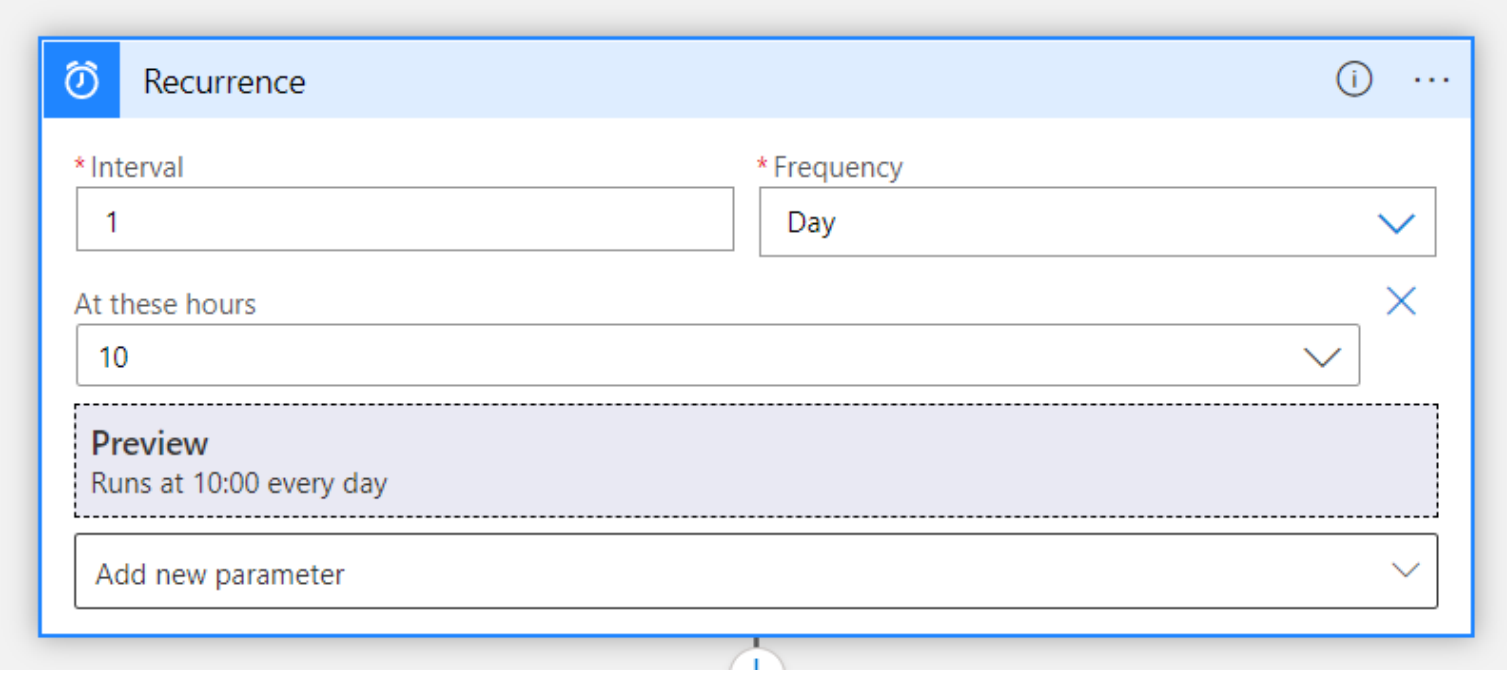
REPORTING ON AUDITING DATA



SETUP LOGIC APP - RECURRENCE

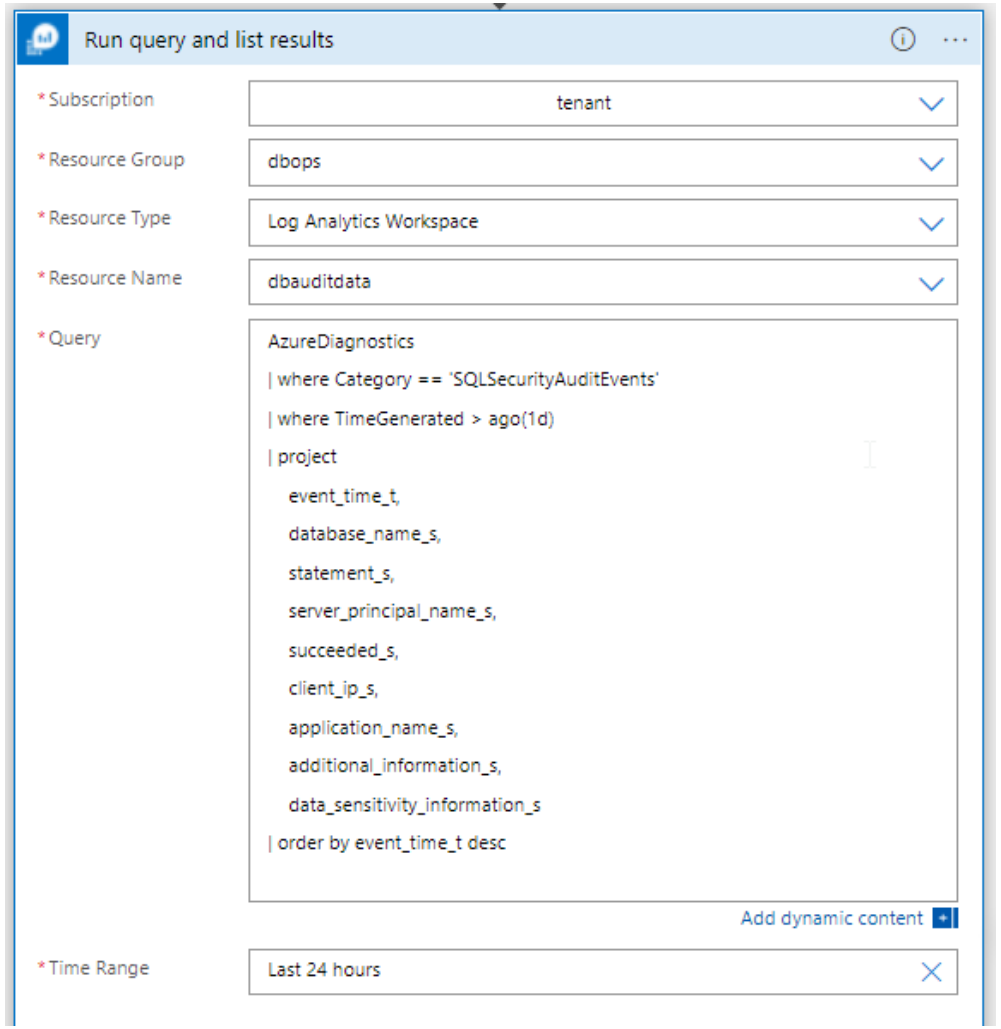
PASS Data Community SUMMIT 2022

Setup a schedule with Recurrence step



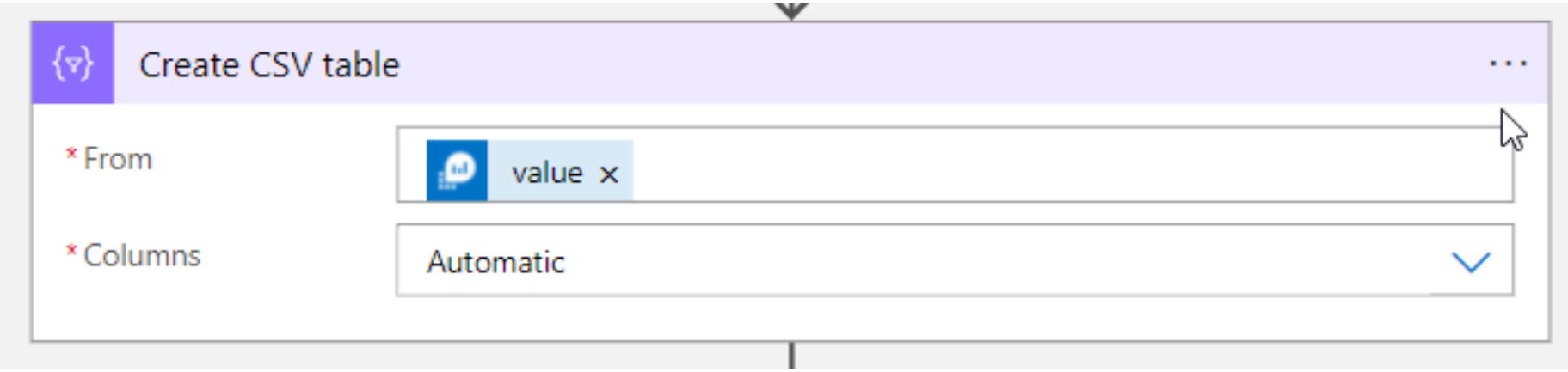
SETUP LOGIC APP –KUSTO QUERY

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

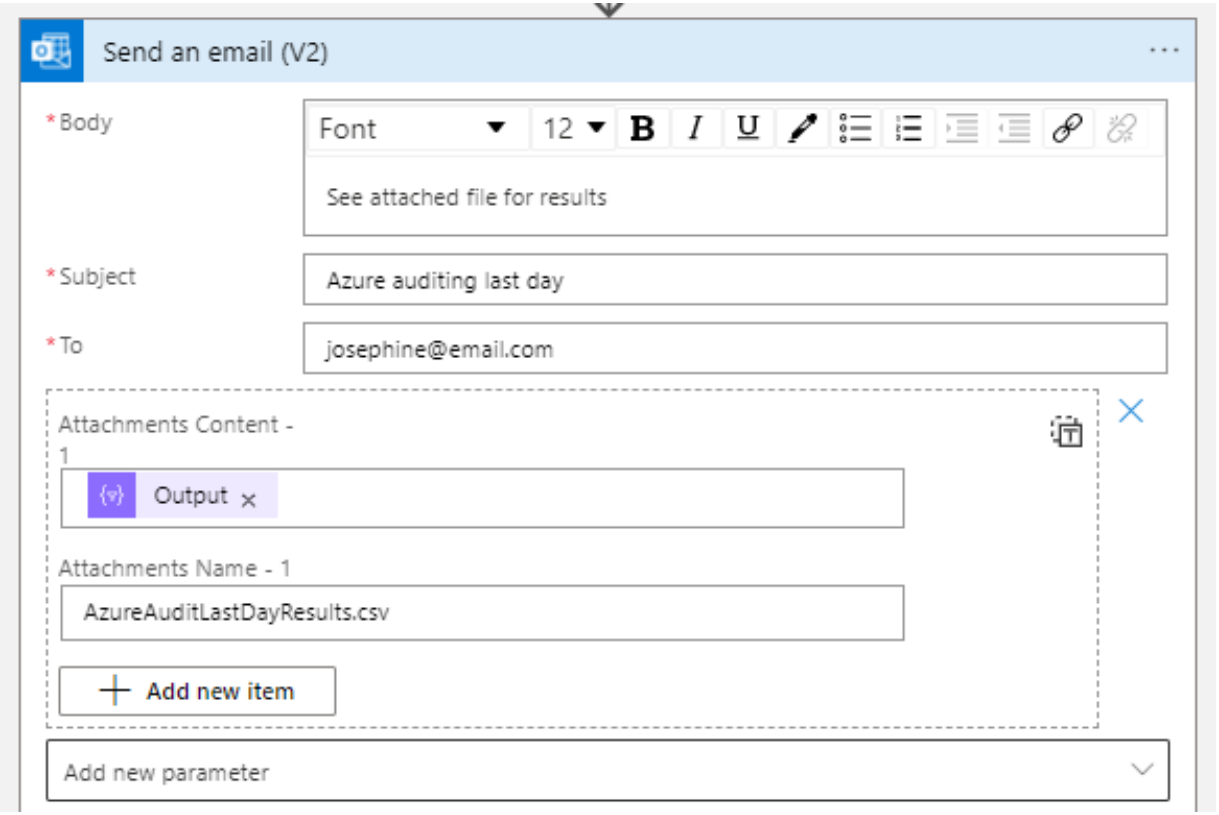


SETUP LOGIC APP – CSV FILE

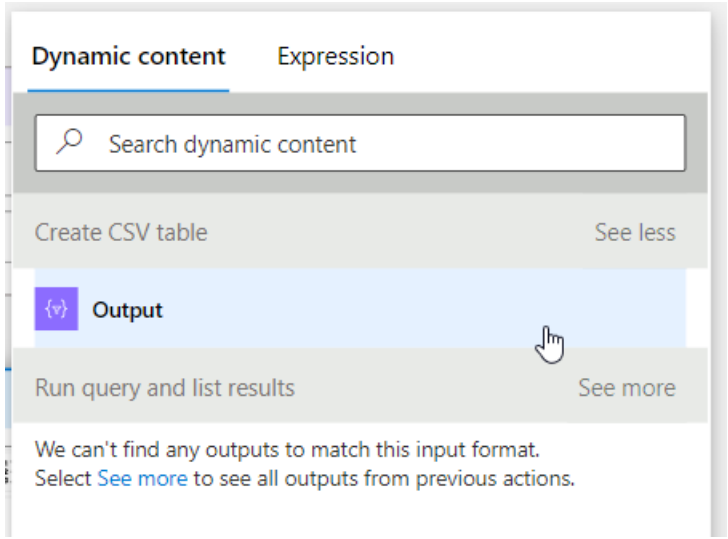
Create CSV table step to create a CSV file attachment



SETUP LOGIC APP – SEND EMAIL



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



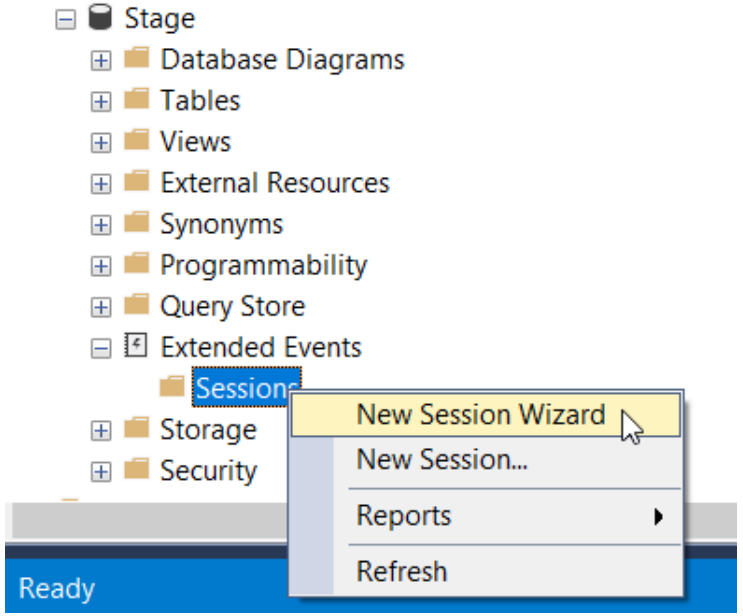
AZURE SQL AUDITING EXTENDED EVENTS

PASS Data Community SUMMIT 2022

Script

```
CREATE EVENT SESSION [audit] ON DATABASE
ADD EVENT sqlserver.rpc_completed(
ACTION(sqlserver.client_app_name,sqlserver.client_hostna
me,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_hostna
me,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

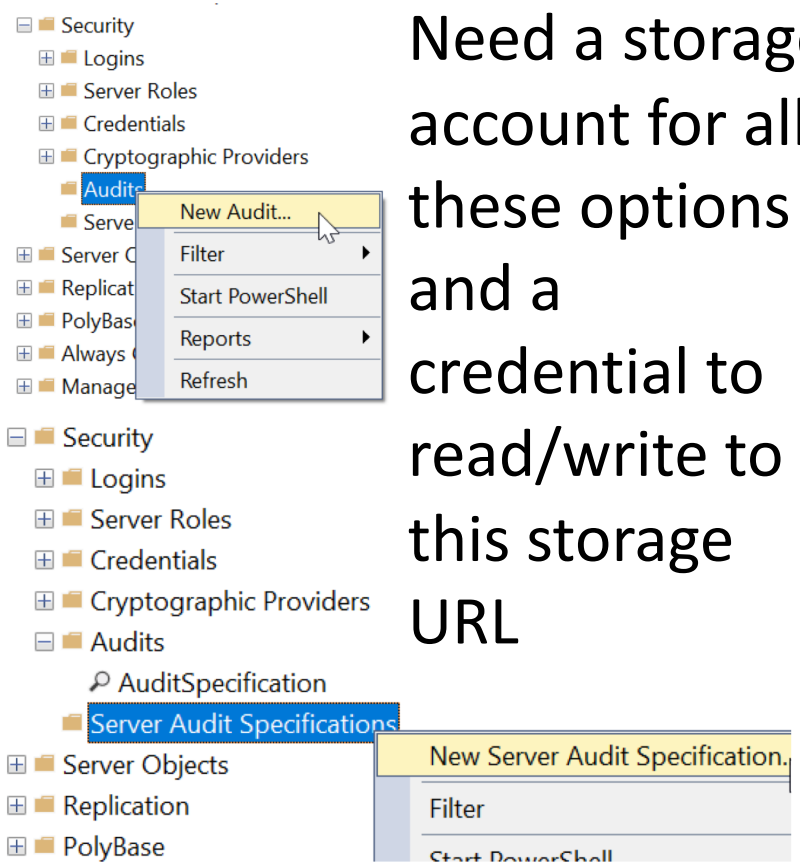


You need a credential setup to use the URL to the storage account in the filename

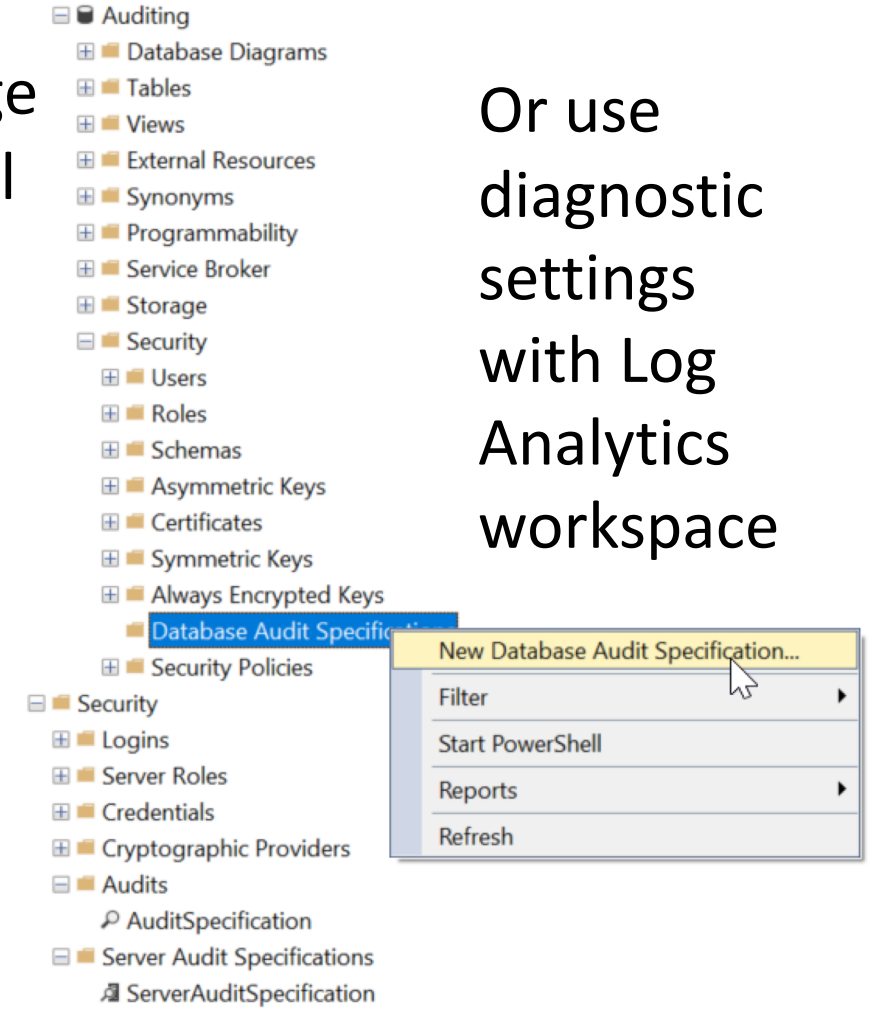
MANAGED INSTANCE AUDITING

PASS Data Community SUMMIT 2022

SQL Server Audit

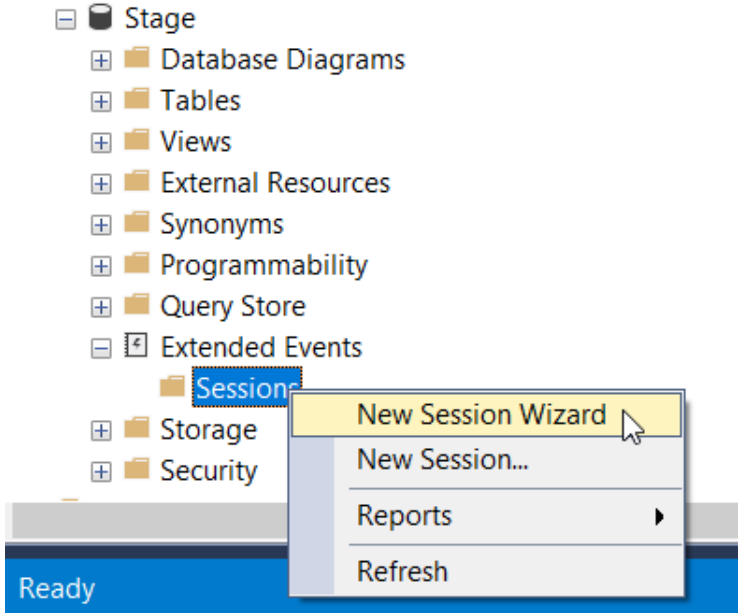


Need a storage account for all these options and a credential to read/write to this storage URL



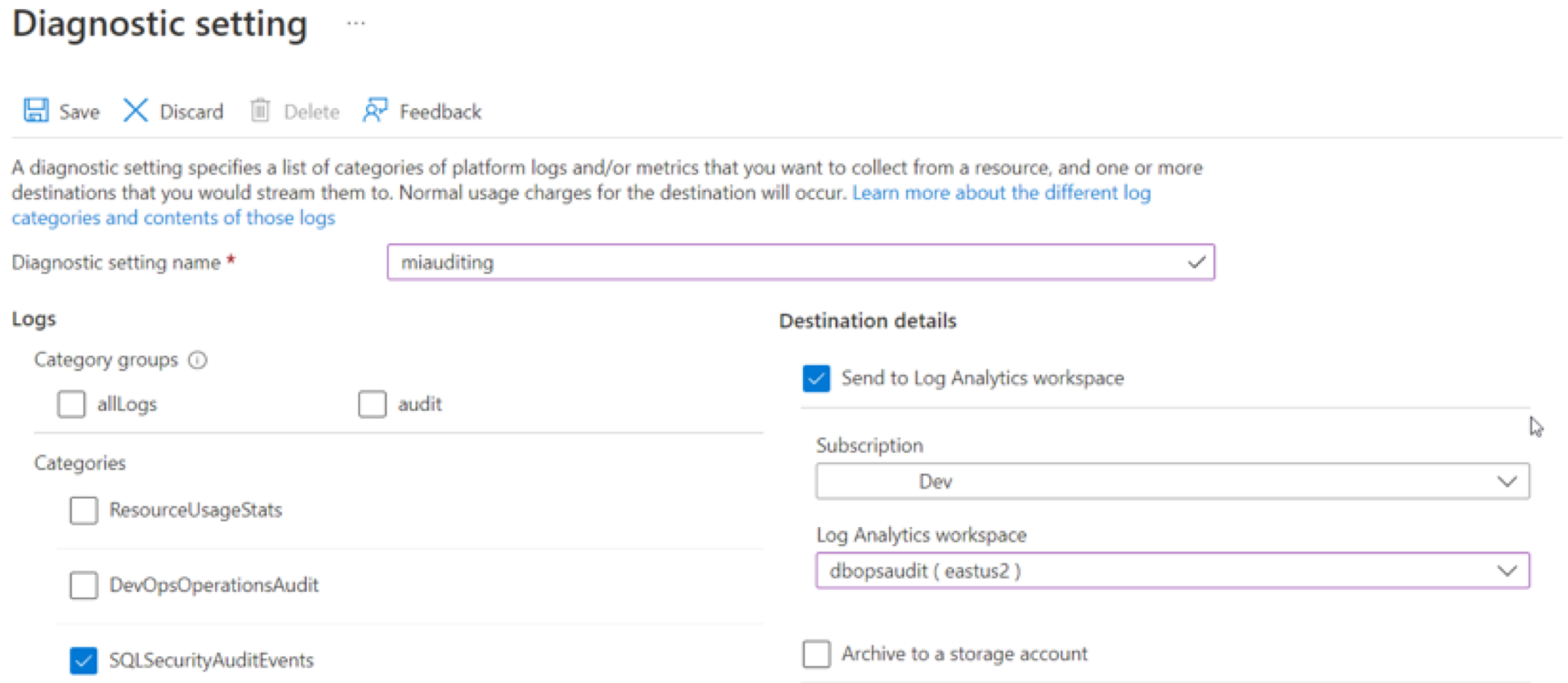
Or use diagnostic settings with Log Analytics workspace

Extended Events



DIAGNOSTIC SETTINGS

Diagnostic setting to store audit events in a Log Analytics workspace



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

PASS Data Community SUMMIT 2022

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.

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

```
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');
```

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