HOW TO AUDIT SQL SERVER FOR FREE

ABOUT ME

Josephine Bush

20+ years IT experience

Experienced DBA

MBA IT Management

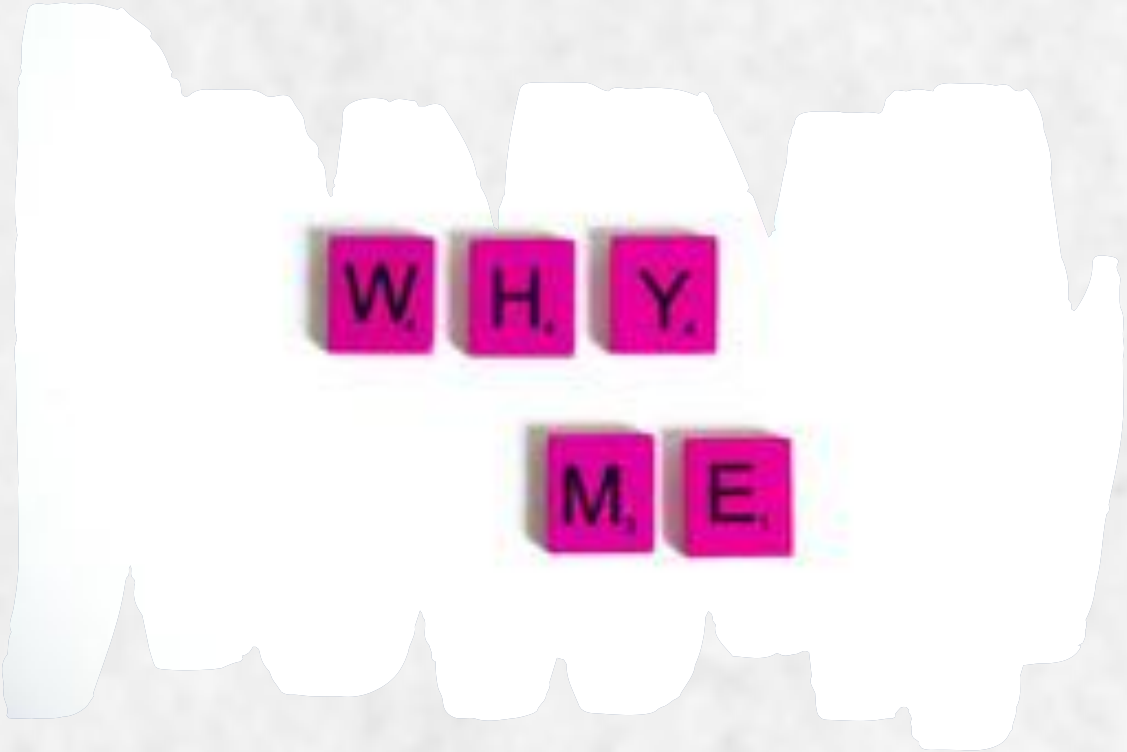
MS Data Analytics

@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….

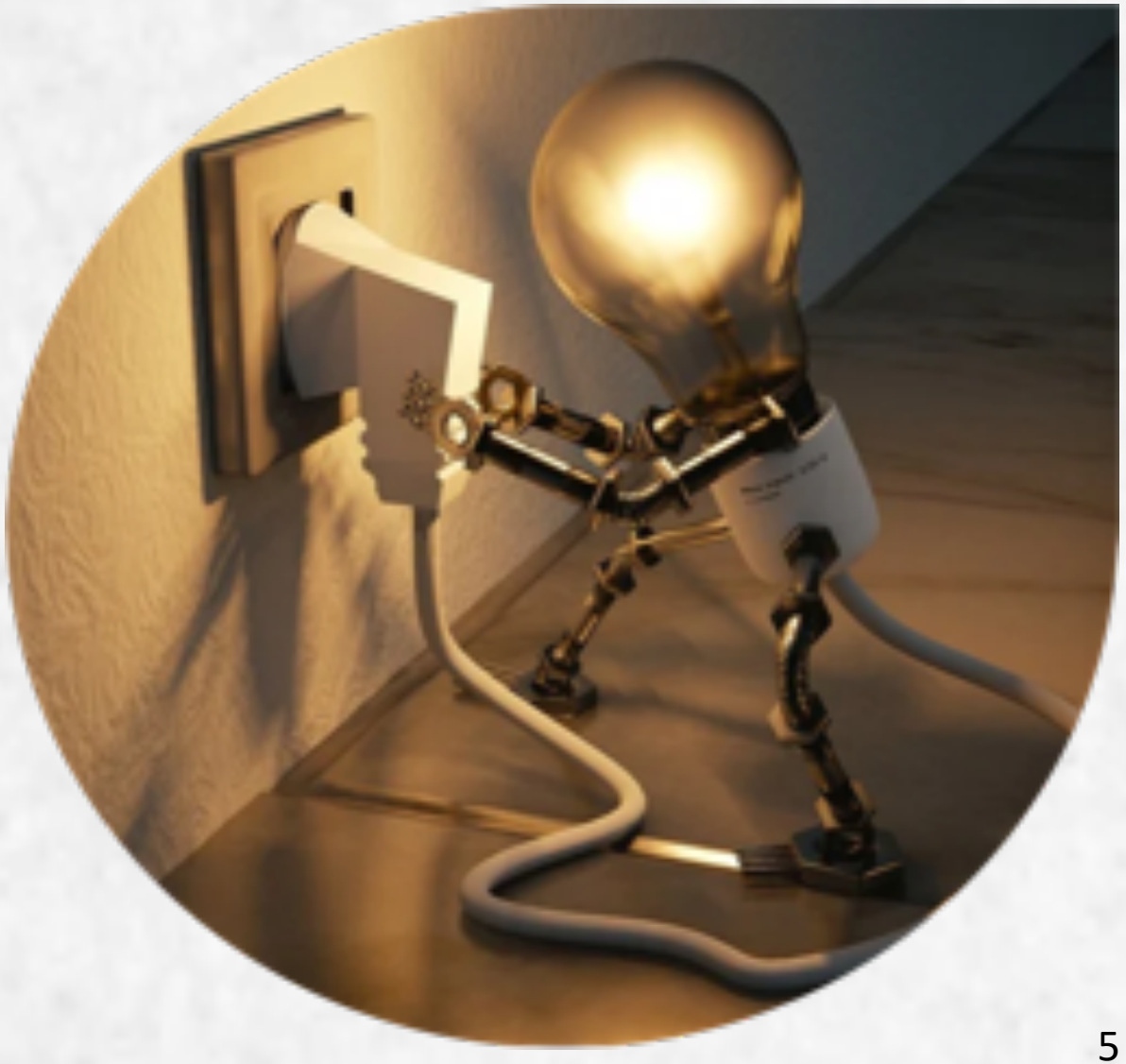
PROBLEMS AUDITING CAN SOLVE

Who broke this?

Who changed this?

Who used this?

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



DISCLAIMER ON AUDITING

Be very careful how and what you audit

You can overload or freeze up a production server

Less is more

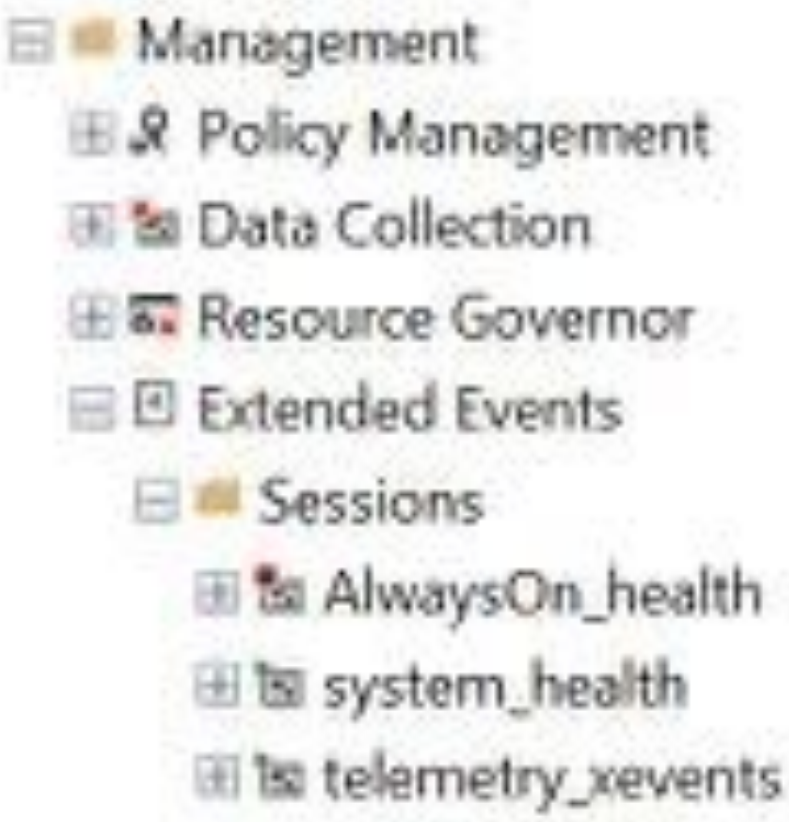
EXTENDED EVENTS (XEVENTS)

Lightweight and flexible

Good for monitoring and auditing

Collect information for troubleshooting and performance

Replacement for SQL Server Profiler and SQL Trace deprecated features



EXTENDED EVENTS AVAILABILITY

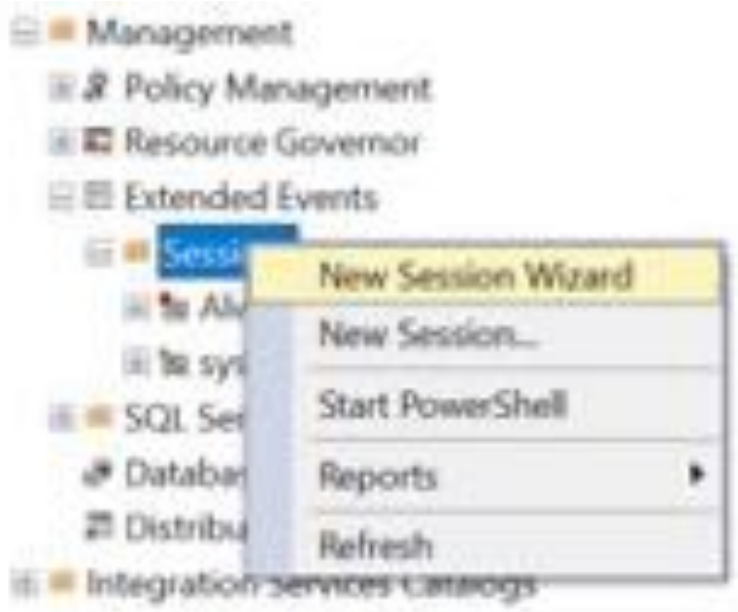
SQL Server Extended Events feature was introduced in SQL Server 2008

Graphical interface added in SQL Server 2012

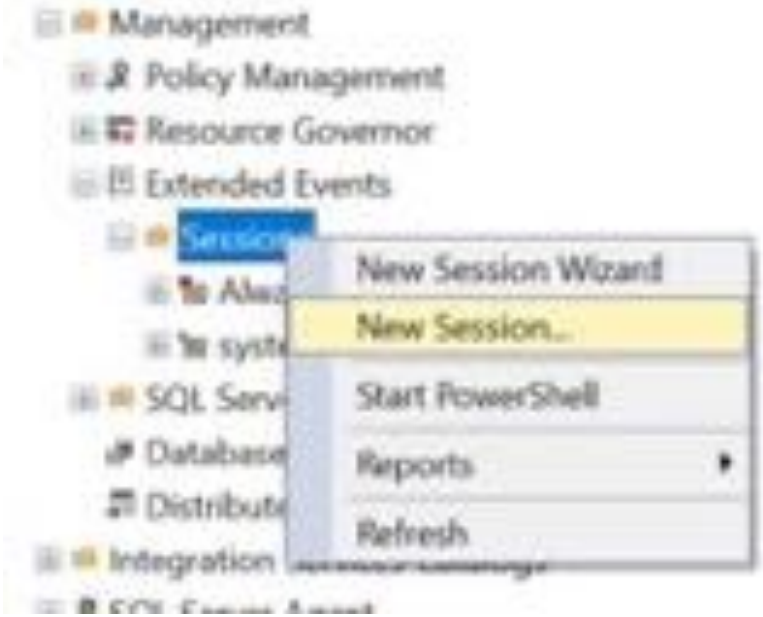
CREATE XEVENTS VIA GUI

Configure with the GUI in SSMS

New Session Wizard option

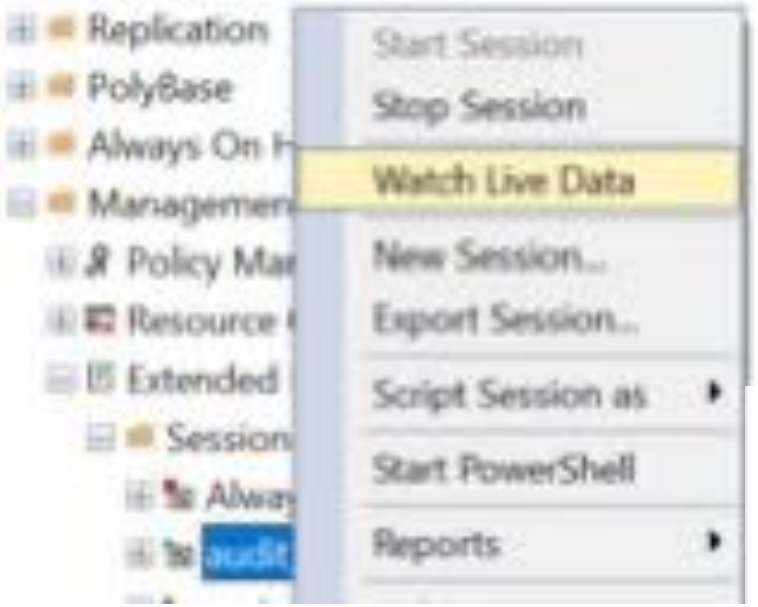


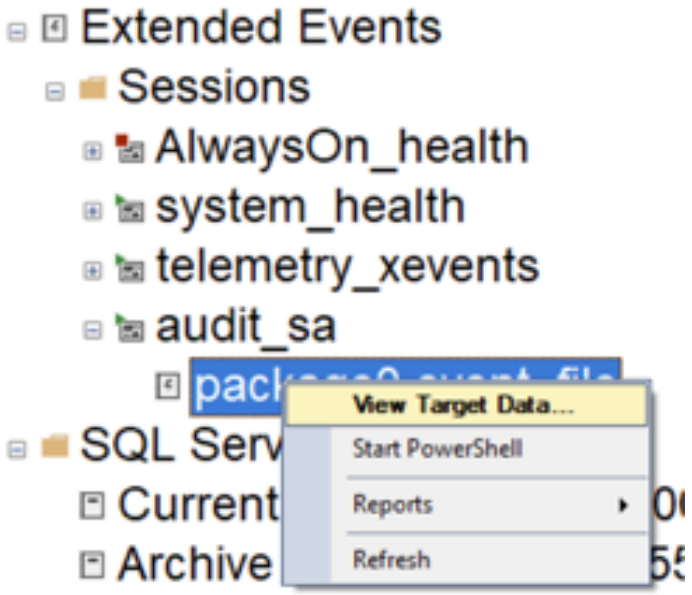
New Session option

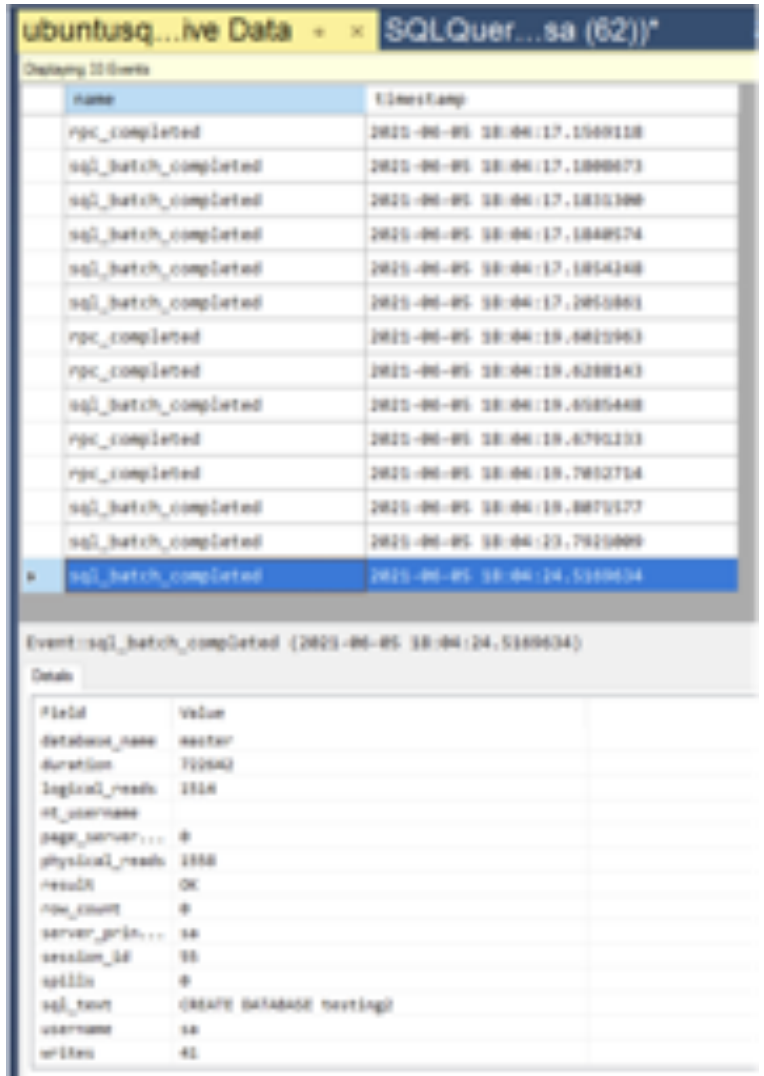


QUERY EXTENDED EVENTS VIA GUI

View extended event data via SSMS







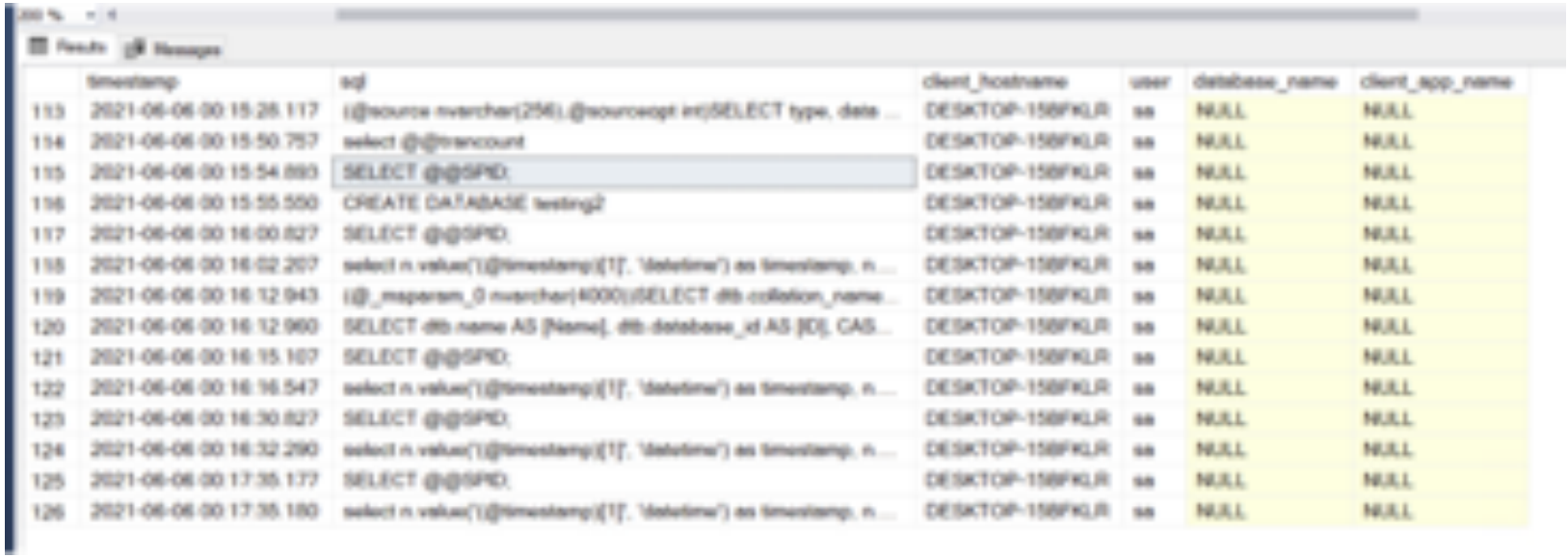
CREATE EXTENDED EVENT VIA SCRIPT

Configure with script in SSMS

```
CREATE EVENT SESSION [audit_sa] ON SERVER
ADD EVENT sqlserver.rpc_completed(
    ACTION(package0.event_sequence,sqlserver.client_hostname,sqlserver.client_pid,sqlserver.database_id,sqlserv
er.nt_username,sqlserver.query_hash,sqlserver.server_principal_name,sqlserver.session_id,sqlserver.sql_text,sql
server.username)
    WHERE (([package0].[equal_boolean]([sqlserver].[is_system],(0))) AND
([sqlserver].[session_server_principal_name]=N'sa'))),
ADD EVENT sqlserver.sql_batch_completed(
    ACTION(package0.event_sequence,sqlserver.client_hostname,sqlserver.client_pid,sqlserver.database_id,sqlserv
er.nt_username,sqlserver.query_hash,sqlserver.server_principal_name,sqlserver.session_id,sqlserver.sql_text,sql
server.username)
    WHERE (([package0].[equal_boolean]([sqlserver].[is_system],(0))) AND
([sqlserver].[session_server_principal_name]=N'sa')))
ADD TARGET package0.event_file(SET
filename=N'/var/opt/mssql/audit_sa.xel',max_file_size=(50),max_rollover_files=(4))
WITH (MAX_MEMORY=8192 KB,EVENT_RETENTION_MODE=ALLOW_SINGLE_EVENT_LOSS,MAX_DISPATCH_LATENCY=5
SECONDS,MAX_EVENT_SIZE=0 KB,MEMORY_PARTITION_MODE=PER_CPU,TRACK_CAUSALITY=ON,STARTUP_STATE=ON)
GO
ALTER EVENT SESSION [audit_sa]
ON SERVER STATE = START;
GO
```

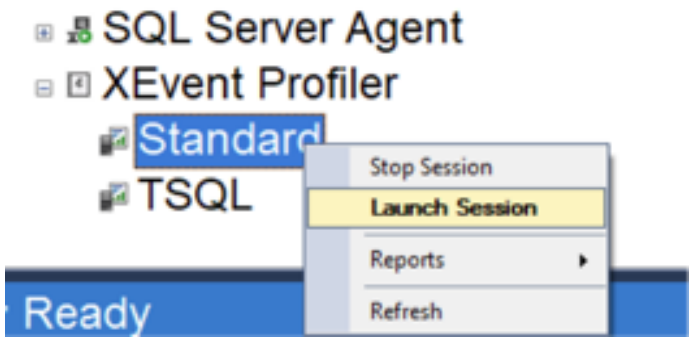
QUERY EXTENDED EVENTS VIA SCRIPT

```sql
SELECT n.value('(@timestamp)[1]', 'datetime') as timestamp,
       n.value('(action[@name="sql_text"]/value)[1]', 'nvarchar(max)') as [sql],
       n.value('(action[@name="client_hostname"]/value)[1]', 'nvarchar(50)') as [client_hostname],
       n.value('(action[@name="server_principal_name"]/value)[1]', 'nvarchar(50)') as [user],
       n.value('(action[@name="database_name"]/value)[1]', 'nvarchar(50)') as [database_name],
       n.value('(action[@name="client_app_name"]/value)[1]', 'nvarchar(50)') as [client_app_name]
FROM (select cast(event_data as XML) as event_data
FROM sys.fn_xe_file_target_read_file(N'/var/opt/mssql/*.xel', NULL, NULL, NULL)) ed
CROSS APPLY ed.event_data.nodes('event') as q(n)
WHERE n.value('(@timestamp)[1]', 'datetime') >= DATEADD(HOUR, -1, GETDATE())
ORDER BY timestamp desc
```

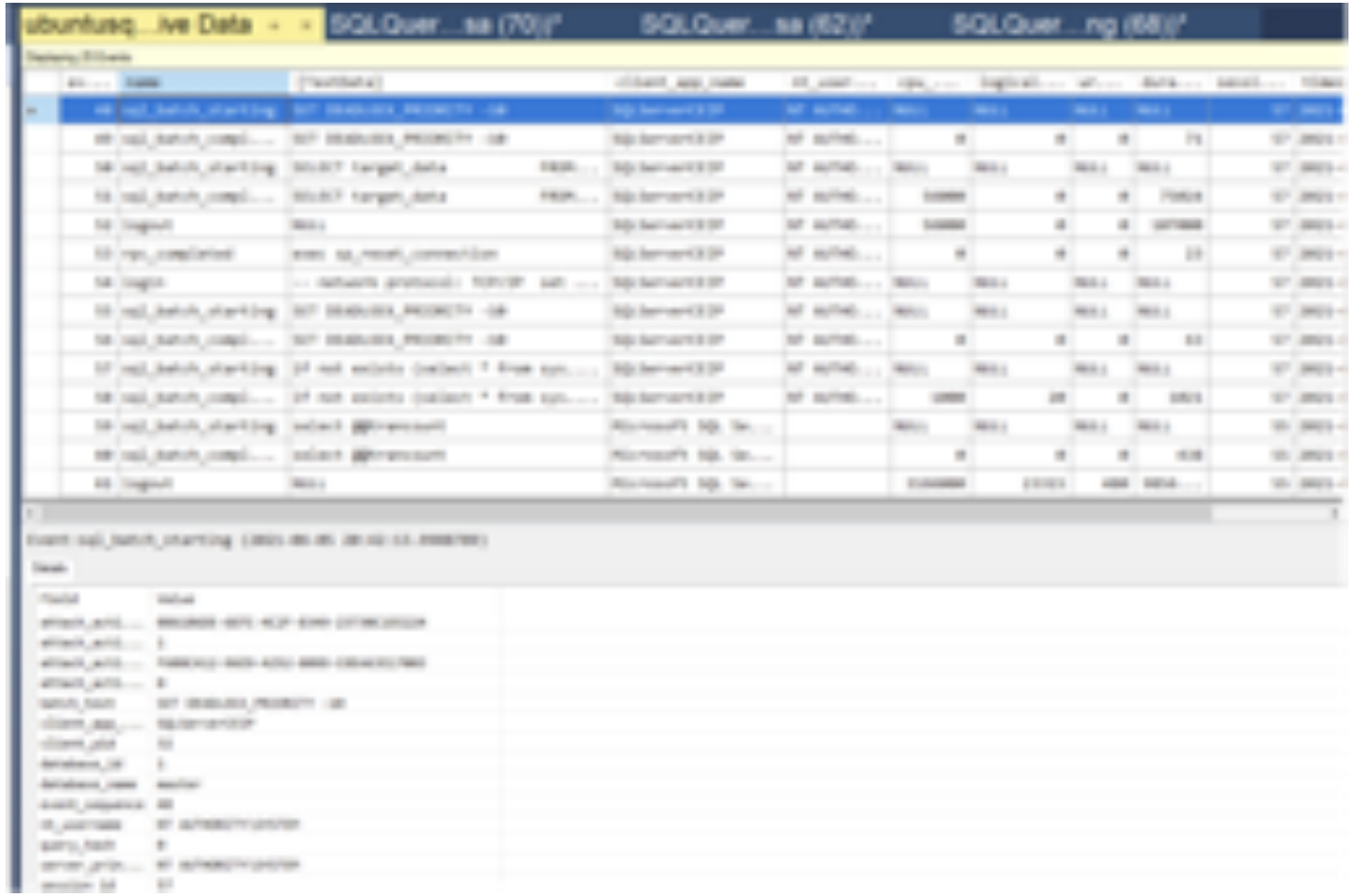


	timestamp	sql	client_hostname	user	database_name	client_app_name
113	2021-06-06 00:15:28.117	i@source nvarchar(256),@sourceopt int)SELECT type, date ...	DESKTOP-158FKLR	sa	NULL	NULL
114	2021-06-06 00:15:50.757	select @@trancount	DESKTOP-158FKLR	sa	NULL	NULL
115	2021-06-06 00:15:54.893	SELECT @@SPID;	DESKTOP-158FKLR	sa	NULL	NULL
116	2021-06-06 00:15:55.550	CREATE DATABASE testing2	DESKTOP-158FKLR	sa	NULL	NULL
117	2021-06-06 00:16:00.827	SELECT @@SPID;	DESKTOP-158FKLR	sa	NULL	NULL
118	2021-06-06 00:16:02.207	select n.value('(@timestamp)[1]', 'datetime') as timestamp, n....	DESKTOP-158FKLR	sa	NULL	NULL
119	2021-06-06 00:16:12.943	i@_msparam_0 nvarchar(4000))SELECT dtb.collation_name...	DESKTOP-158FKLR	sa	NULL	NULL
120	2021-06-06 00:16:12.960	SELECT dtb.name AS [Name], dtb.database_id AS [ID], CAS...	DESKTOP-158FKLR	sa	NULL	NULL
121	2021-06-06 00:16:15.107	SELECT @@SPID;	DESKTOP-158FKLR	sa	NULL	NULL
122	2021-06-06 00:16:16.547	select n.value('(@timestamp)[1]', 'datetime') as timestamp, n....	DESKTOP-158FKLR	sa	NULL	NULL
123	2021-06-06 00:16:30.827	SELECT @@SPID;	DESKTOP-158FKLR	sa	NULL	NULL
124	2021-06-06 00:16:32.290	select n.value('(@timestamp)[1]', 'datetime') as timestamp, n....	DESKTOP-158FKLR	sa	NULL	NULL
125	2021-06-06 00:17:35.177	SELECT @@SPID;	DESKTOP-158FKLR	sa	NULL	NULL
126	2021-06-06 00:17:35.180	select n.value('(@timestamp)[1]', 'datetime') as timestamp, n....	DESKTOP-158FKLR	sa	NULL	NULL

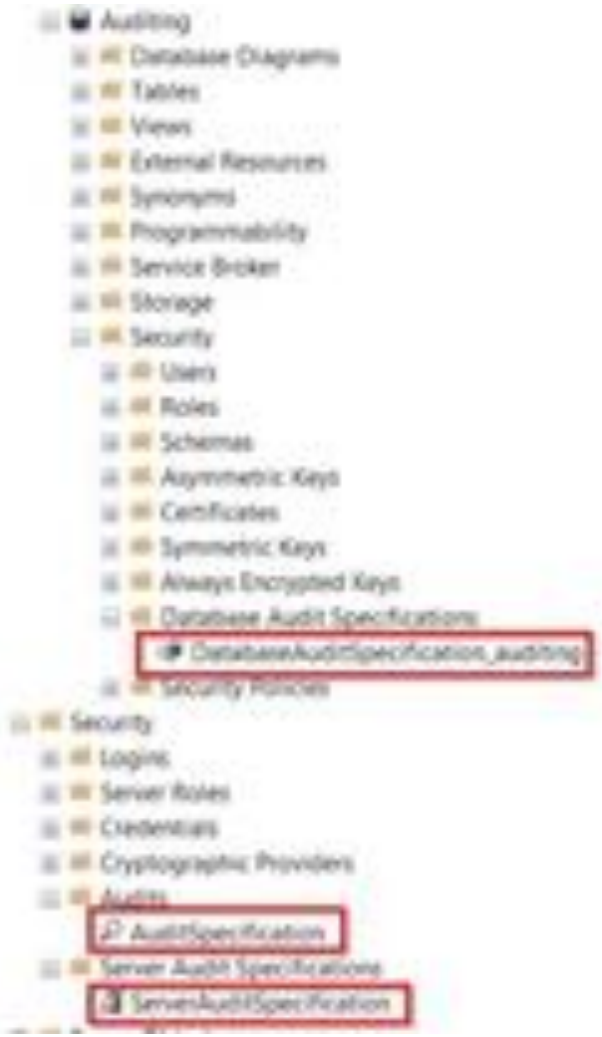
QUICK VIEW XEVENTS VIA GUI



Make sure to stop it when you are done



SQL SERVER AUDIT



Lightweight and flexible

Good for auditing user actions

Uses extended events under the hood

SQL SERVER AUDIT AVAILABILITY

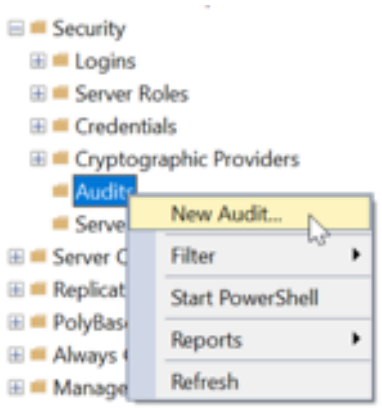
Version	Server audit edition	Database audit edition
2008	Only available in enterprise	Only available in enterprise
2012 and 2014	Available in all editions	Only available in enterprise
2016, 2017, 2019	Available in all editions	Available in all editions

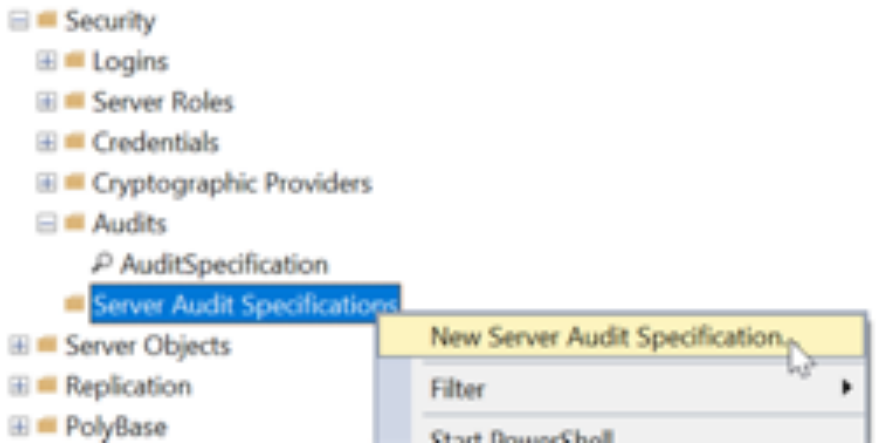
SQL SERVER AUDIT USE CASES

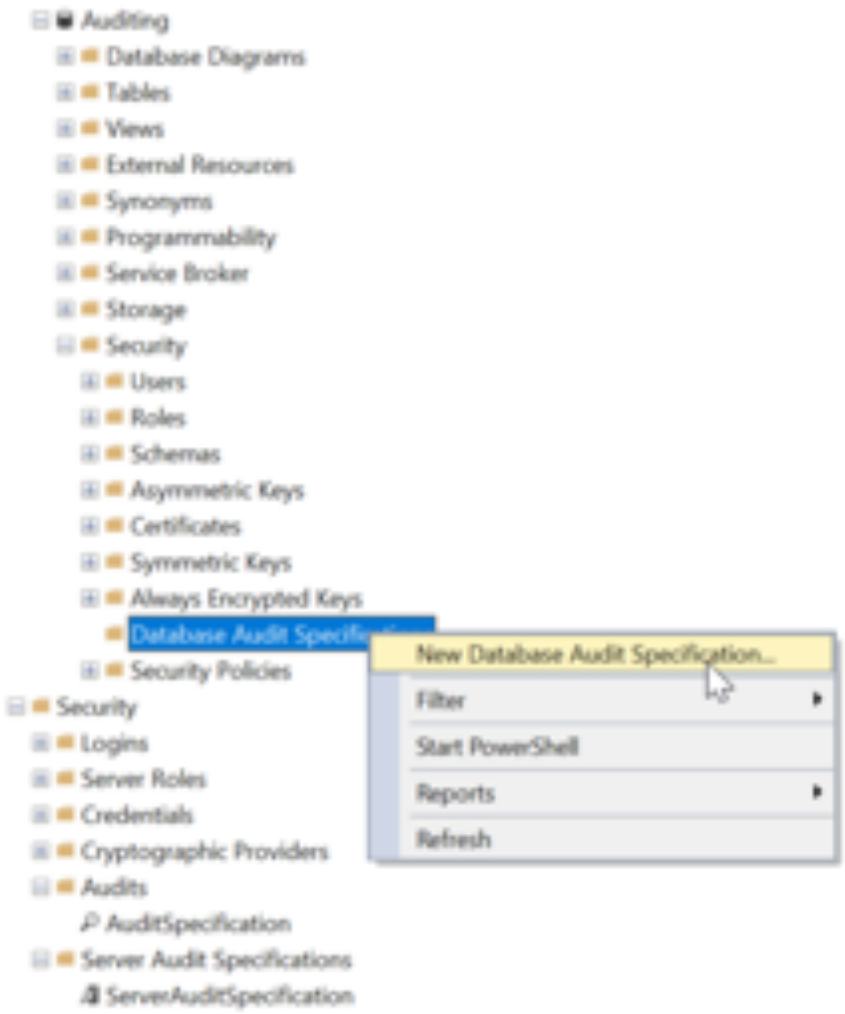
A server audit specification is good for auditing server level and/or all databases at the same time

A database audit specification is good for auditing one database or a subset of activities in one database

CREATE AUDIT VIA GUI







CREATE AUDIT VIA SCRIPT

Creating an audit specification via script

```
USE [master]
GO
CREATE SERVER AUDIT [AuditSpecification]
TO FILE
(FILEPATH = N'E:\sqlaudit'
,MAXSIZE = 50 MB
,MAX_FILES = 4
,RESERVE_DISK_SPACE = OFF
) WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
ALTER SERVER AUDIT [AuditSpecification] WITH (STATE = ON)
GO
```

CREATE SERVER AUDIT VIA SCRIPT

Creating a server audit specification via script

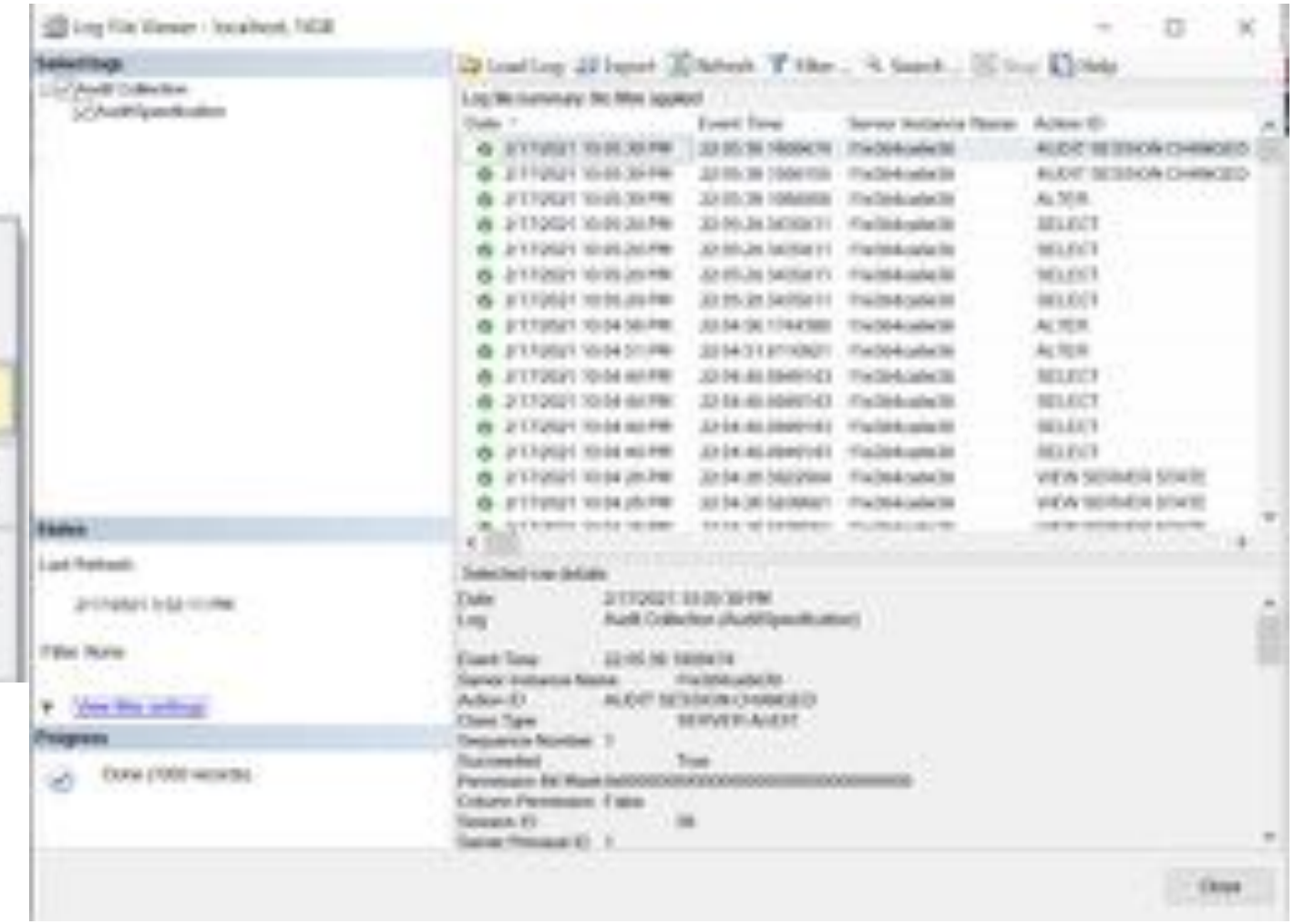
```
USE [master]
CREATE SERVER AUDIT SPECIFICATION [ServerAuditSpecification]
FOR SERVER AUDIT [AuditSpecification]
ADD (DATABASE_ROLE_MEMBER_CHANGE_GROUP),
ADD (SERVER_ROLE_MEMBER_CHANGE_GROUP),
ADD (AUDIT_CHANGE_GROUP),
ADD (DATABASE_PERMISSION_CHANGE_GROUP),
ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
ADD (SERVER_OBJECT_PERMISSION_CHANGE_GROUP),
ADD (SERVER_PERMISSION_CHANGE_GROUP),
ADD (DATABASE_CHANGE_GROUP),
ADD (DATABASE_OBJECT_CHANGE_GROUP),
ADD (DATABASE_PRINCIPAL_CHANGE_GROUP),
ADD (SCHEMA_OBJECT_CHANGE_GROUP),
ADD (SERVER_OBJECT_CHANGE_GROUP),
ADD (SERVER_PRINCIPAL_CHANGE_GROUP),
ADD (SERVER_OPERATION_GROUP),
ADD (APPLICATION_ROLE_CHANGE_PASSWORD_GROUP),
ADD (LOGIN_CHANGE_PASSWORD_GROUP),
ADD (SERVER_STATE_CHANGE_GROUP),
ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
ADD (SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP),
ADD (SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP),
ADD (USER_CHANGE_PASSWORD_GROUP)
WITH (STATE = ON)
```

CREATE DATABASE AUDIT VIA SCRIPT

Creating a database audit specification via script

```
USE [auditing]
CREATE DATABASE AUDIT SPECIFICATION [DatabaseAuditSpecification_Auditing]
FOR SERVER AUDIT [AuditSpecification]
ADD (DATABASE_ROLE_MEMBER_CHANGE_GROUP),
ADD (AUDIT_CHANGE_GROUP),
ADD (DBCC_GROUP),
ADD (DATABASE_PERMISSION_CHANGE_GROUP),
ADD (DATABASE_OBJECT_PERMISSION_CHANGE_GROUP),
ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
ADD (DATABASE_CHANGE_GROUP),
ADD (DATABASE_OBJECT_CHANGE_GROUP),
ADD (DATABASE_PRINCIPAL_CHANGE_GROUP),
ADD (SCHEMA_OBJECT_CHANGE_GROUP),
ADD (APPLICATION_ROLE_CHANGE_PASSWORD_GROUP),
ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
ADD (DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP),
ADD (SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP),
ADD (USER_CHANGE_PASSWORD_GROUP)
WITH (STATE = ON)
```

QUERYING AUDIT VIA GUI



QUERYING AUDIT VIA SCRIPT

```
SELECT distinct DATEADD(mi, DATEPART(TZ, SYSDATETIMEOFFSET()), event_time) as event_time,
aa.name as audit_action,statement,succeeded, server_instance_name,
database_name, schema_name, session_server_principal_name, server_principal_name,
object_Name, file_name, client_ip, application_name, host_name, file_name
FROM sys.fn_get_audit_file ('/var/opt/mssql/*.sqlaudit',default,default) af
INNER JOIN sys.dm_audit_actions aa ON aa.action_id = af.action_id
where  DATEADD(mi, DATEPART(TZ, SYSDATETIMEOFFSET()), event_time) > DATEADD(HOUR, -24, GETDATE())
order by DATEADD(mi, DATEPART(TZ, SYSDATETIMEOFFSET()), event_time) desc
```

event_time	audit_action	statement	succeeded	server_instance_name	database_name	schema_name	session_server_princi
2021-03-10 16:56:43.2172217	VIEW SERVER STATE	SELECT se.is_admin_endpoint AS N'AdminConnection', ...	1	ubuntusql1	master		sa
2021-03-10 00:14:46.0174361	ALTER	ALTER SERVER AUDIT SPECIFICATION [ServerAuditSpe...	1	ubuntusql1	master		sa
2021-03-10 00:14:43.2910458	ALTER	ALTER SERVER AUDIT SPECIFICATION [ServerAuditSpe...	1	ubuntusql1	master		sa
2021-03-10 00:13:49.0498994	DROP	DROP TABLE [dbo].[testing]	1	ubuntusql1	testing	dbo	sa
2021-03-10 00:13:12.5602091	ALTER	ALTER SERVER AUDIT SPECIFICATION [ServerAuditSpe...	1	ubuntusql1	master		sa
2021-03-10 00:12:47.8445646	ADD MEMBER	ALTER ROLE [db_datawriter] ADD MEMBER [testing]	1	ubuntusql1	testing		sa
2021-03-10 00:12:47.8364041	ADD MEMBER	ALTER ROLE [db_datareader] ADD MEMBER [testing]	1	ubuntusql1	testing		sa
2021-03-10 00:12:47.7993722	CREATE	CREATE USER [testing] FOR LOGIN [testing] WITH DEFA...	1	ubuntusql1	testing		sa
2021-03-10 00:12:44.9579663	CREATE	CREATE LOGIN [testing] WITH PASSWORD=N'******, DEF...	1	ubuntusql1	master		sa
2021-03-10 00:12:39.7804485	CREATE	CREATE TABLE [dbo].[testing]([testing] [nchar](10) NUL...	1	ubuntusql1	testing	dbo	sa
2021-03-10 00:12:39.7763430	ALTER	CREATE TABLE [dbo].[testing]([testing] [nchar](10) NUL...	1	ubuntusql1	testing		sa
2021-03-10 00:12:38.0592305	CREATE	CREATE DATABASE testing	1	ubuntusql1	master		sa

SQL SERVER AUDITING A USER

Audit specification

```
USE [master]
CREATE SERVER AUDIT [Audit_AuditingUser]
TO FILE
(FILEPATH = N'E:\sqlaudit\auditinguser\'
,MAXSIZE = 100 MB
,MAX_FILES = 4
,RESERVE_DISK_SPACE = OFF
) WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
WHERE ([server_principal_name]='sa' AND [schema_name]<>'sys')
ALTER SERVER AUDIT [Audit-AuditingUser] WITH (STATE = ON)
```

Server audit specification

```
USE [master]
CREATE SERVER AUDIT SPECIFICATION
[ServerAudit_Auditinguser]
FOR SERVER AUDIT [Audit-AuditingUser]
ADD (DATABASE_OBJECT_ACCESS_GROUP),
ADD (SCHEMA_OBJECT_ACCESS_GROUP),
ADD (DATABASE_ROLE_MEMBER_CHANGE_GROUP),
ADD (SERVER_ROLE_MEMBER_CHANGE_GROUP),
ADD (AUDIT_CHANGE_GROUP),
ADD (DATABASE_PERMISSION_CHANGE_GROUP),
ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
ADD (SERVER_OBJECT_PERMISSION_CHANGE_GROUP),
ADD (SERVER_PERMISSION_CHANGE_GROUP),
ADD (DATABASE_CHANGE_GROUP),
ADD (DATABASE_OBJECT_CHANGE_GROUP),
ADD (DATABASE_PRINCIPAL_CHANGE_GROUP),
ADD (SCHEMA_OBJECT_CHANGE_GROUP),
ADD (SERVER_OBJECT_CHANGE_GROUP),
ADD (SERVER_PRINCIPAL_CHANGE_GROUP),
ADD (SERVER_OPERATION_GROUP),
ADD (APPLICATION_ROLE_CHANGE_PASSWORD_GROUP),
ADD (LOGIN_CHANGE_PASSWORD_GROUP),
ADD (SERVER_STATE_CHANGE_GROUP),
ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
ADD (SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP),
ADD (SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP),
ADD (USER_CHANGE_PASSWORD_GROUP)
WITH (STATE = ON)
```

Be very careful with these audit actions

They can overload your audit and/or server

EXTENDED EVENTS PROS AND CONS

Pros

Easy to get started with a templates

Will feel familiar if you used SQL Trace or Profiler

Easy to view live events in SSMS GUI

Cons

Need to know how to query XML if you want to use a SQL query instead of SSMS live event viewer

SQL SERVER AUDIT PROS AND CONS

Pros

Easy to view audit log in SSMS GUI

You don’t need to know how to query XML to query events with a SQL query

Easy to capture specific auditable events or capture all auditable events

Cons

More complicated to setup than Extended Events

No templates to guide you

XEVENTS VS SQL AUDIT

Feature	Extended events	SQL Server audit
Setup via GUI or scripts	Yes	Yes
Query via GUI or scripts	Yes	Yes
Delete in GUI or script and it deletes history	No, xel files are left on disk if disk location is configured	No, audit files are left on disk if disk location is configured
Can delete and modify it while it's enabled and running	Yes	No
Save to locations	event_file as .xel file on disk ring_buffer event_counter histogram pair_matching etw_classic_sync_target	.sqlaudit file on disk Application Log Security Log
Ability to customize number, location, and size of files	Yes	Yes

XEVENTS VS SQL AUDIT

Feature	Extended events	SQL Server audit
Query without parsing XML	No	Yes
Gives you host info about changes made	Yes	Only in SQL Server 2017 and later versions
Templates	Yes	No
Ability to filter what is captured	Yes	Yes
Ability to audit what a user does	Yes	Yes
Ability to capture server metrics like waits stats or connection tracking	Yes	No
Setup multiple on a server	Yes	Yes
Number of items required to make it work	One	Two to three

DISCLAIMER ON AUDITING

Be very careful how and what you audit

You can overload or freeze up a production server

Less is more

RESOURCES

SQL Server Audit Overview

https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-database-engine?view=sql-server-ver15

Using SQL Server Auditing Full Length Presentation

https://www.youtube.com/watch?v=Iv62qowczDk&list=PLLq_tkpMFDU7UzoBMSi0BmRF09CKy182Q&index=13

Extended events quickstart

https://docs.microsoft.com/en-us/sql/relational-databases/extended-events/quick-start-extended-events-in-sql-server?view=sql-server-ver15

Extended events overview

https://docs.microsoft.com/en-us/sql/relational-databases/extended-events/extended-events?view=sql-server-ver15

THANK YOU FOR ATTENDING

Contact me @hellosqlkitty

Visit me at sqlkitty.com

Email me hellosqlkitty@gmail.com