

GROUPBY 2021

OCT 26-27

Free Online Training for Data Professionals.

By the Community, for the Community.



GROUPBY

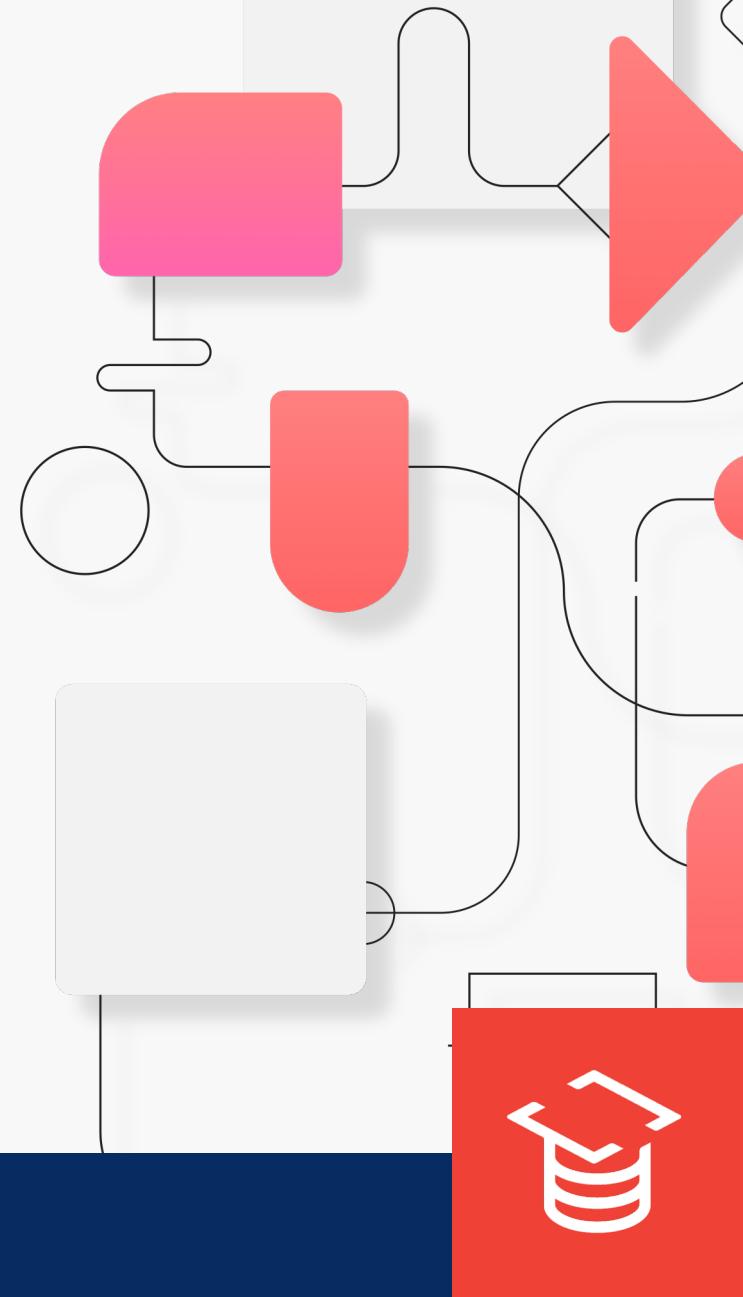
CODE OF CONDUCT

The Quick Version

We are dedicated to a harassment-free experience for everyone, regardless of who you are and what makes you *you*. We recognize the right of any individual to attend and participate. Anyone. This is included but not limited to gender identity and expression, sexual orientation, disability, physical appearance, body size, race, religion, or any other classification, affiliation, or label.

We do not tolerate harassment in any form. For the duration of your engagement with GroupBy and its programs, you are expected to act appropriately and to adhere to this Code of Conduct. This includes conduct in-person and online, at the conference itself, as well as any non-conference programs that may include participants: including talks, workshops, parties, on social media, and other online forums. GroupBy participants violating these rules may be sanctioned or expelled without a refund (if that applies) at the discretion of the conference organizers.

You can review the full policy at: GroupBy.org/Code-of-Conduct



GROUPBY 2021 | OCT 26-27

Core Sponsors



Media Sponsors



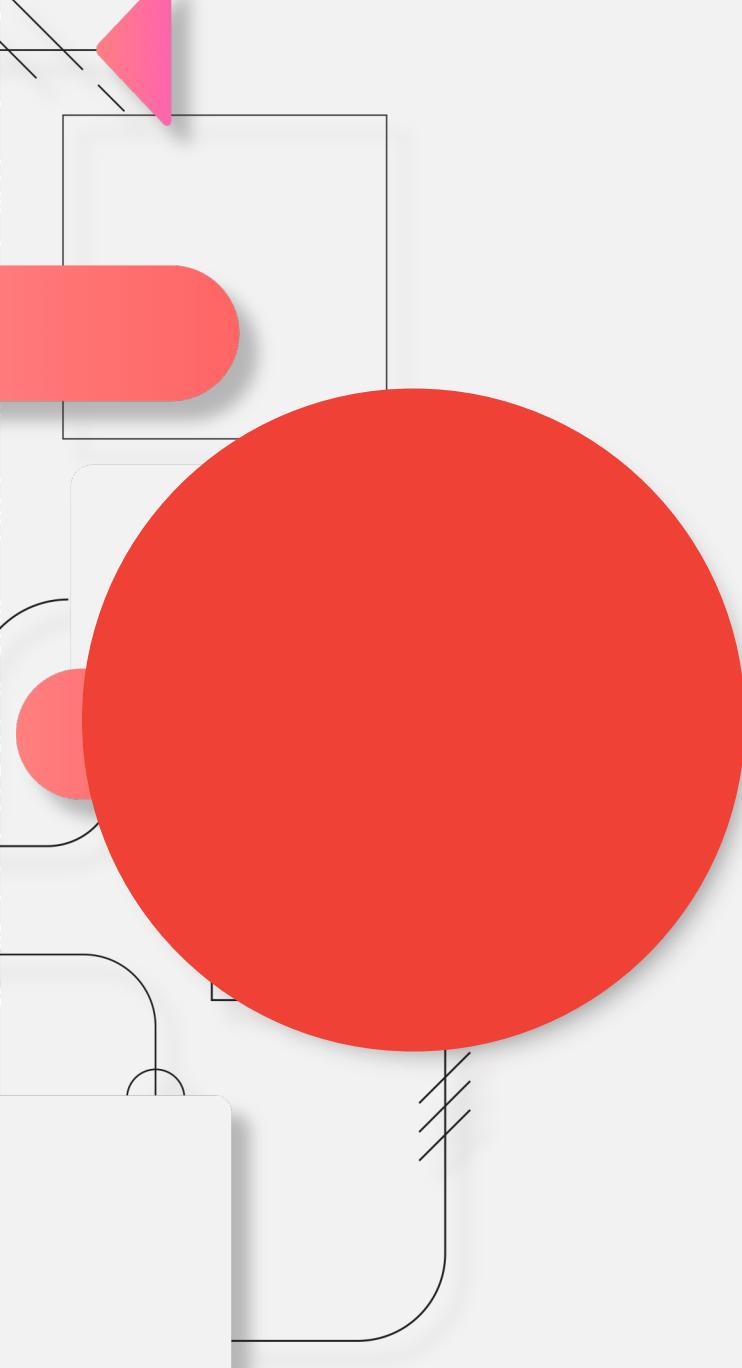
Virtual Group Sponsors



GROUPBY 2021 | OCT 26-27

Auditing SQL Server: Extended Events vs SQL Server Audit





Josephine Bush

Senior Database Administirator

sqlkitty.com

<https://twitter.com/hellosqlkitty>

Over 10 years of experience as a Database Administrator. Microsoft Certified Solutions Expert: Data Management and Analytics. BS in Information Technology, an MBA in IT Management, and an MS in Data Analytics. Author of Learn SQL Database Programming published by Packt in May 2020.

AGENDA



Why use auditing?

Problems you can solve

Extended events vs SQL

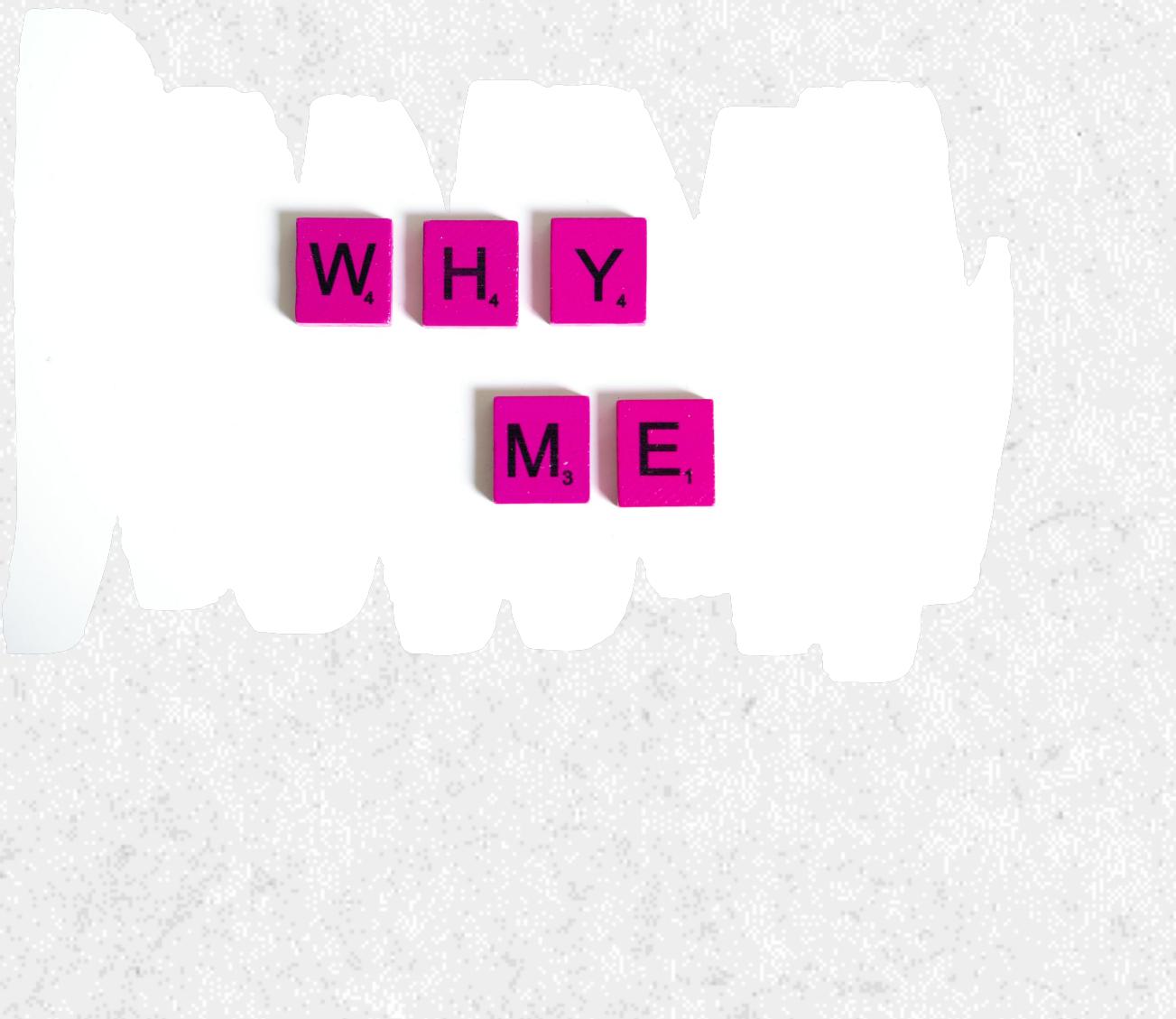
Server Audit:

- Pros and cons
- Use cases

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



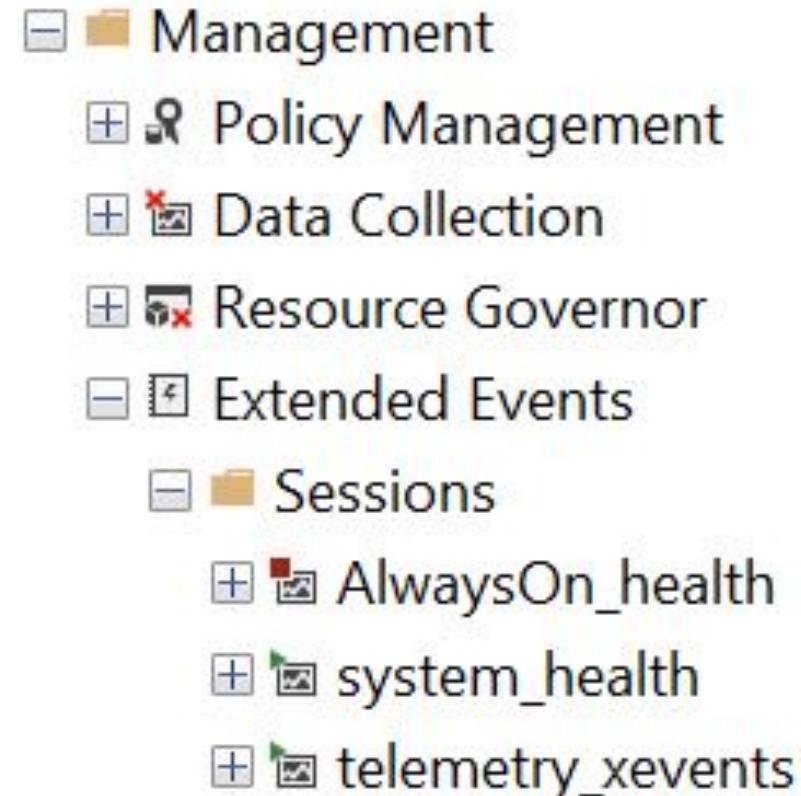
EXTENDED EVENTS (XEVENTS)

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



XEVENTS DEFAULT SESSIONS

Come with SQL Server by default

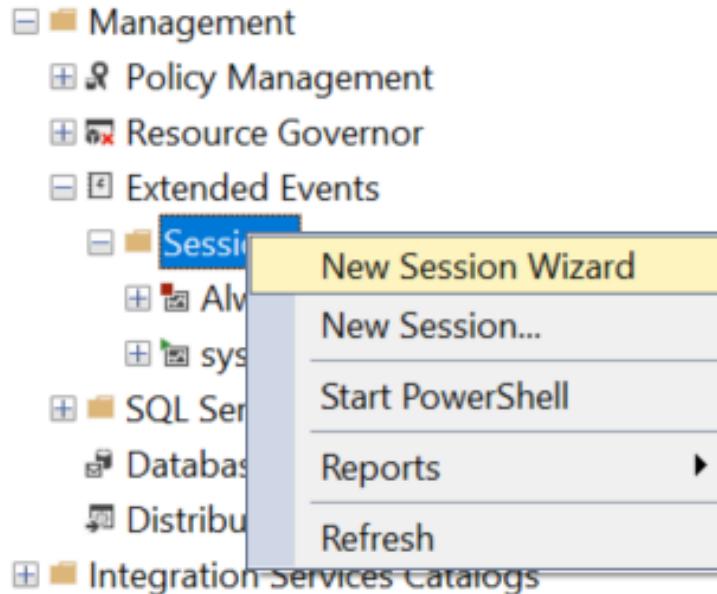
- Extended Events
- Sessions
 - AlwaysOn_health
 - package0.event_file
 - system_health
 - package0.event_file
 - package0.ring_buffer
 - telemetry_xevents
 - package0.ring_buffer



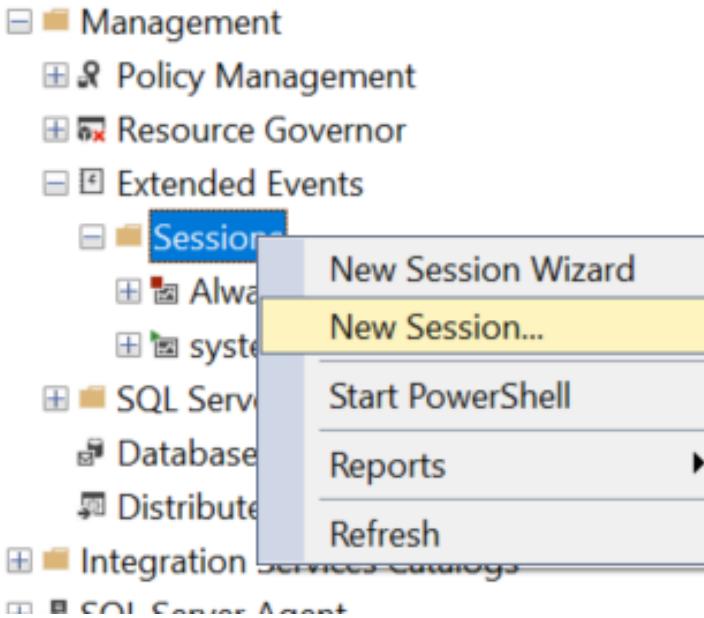
CREATE XEVENTS VIA GUI

Configure with the GUI in SSMS

New Session Wizard option



New Session option



XEVENTS NAMING

New Session Wizard: Set Session Properties

Set Session Properties



Introduction Help

Set Session Properties

Choose Template

Select Events To Capture

Capture Global Fields

Set Session Event Filters

Specify Session Data Storage

Summary

Create Event Session

Enter a name for the event session and the time when you want the session to start.

Session name:

Schedule:

Start the event session at server startup.

< Previous Next > Finish Cancel



XEVENTS TEMPLATES

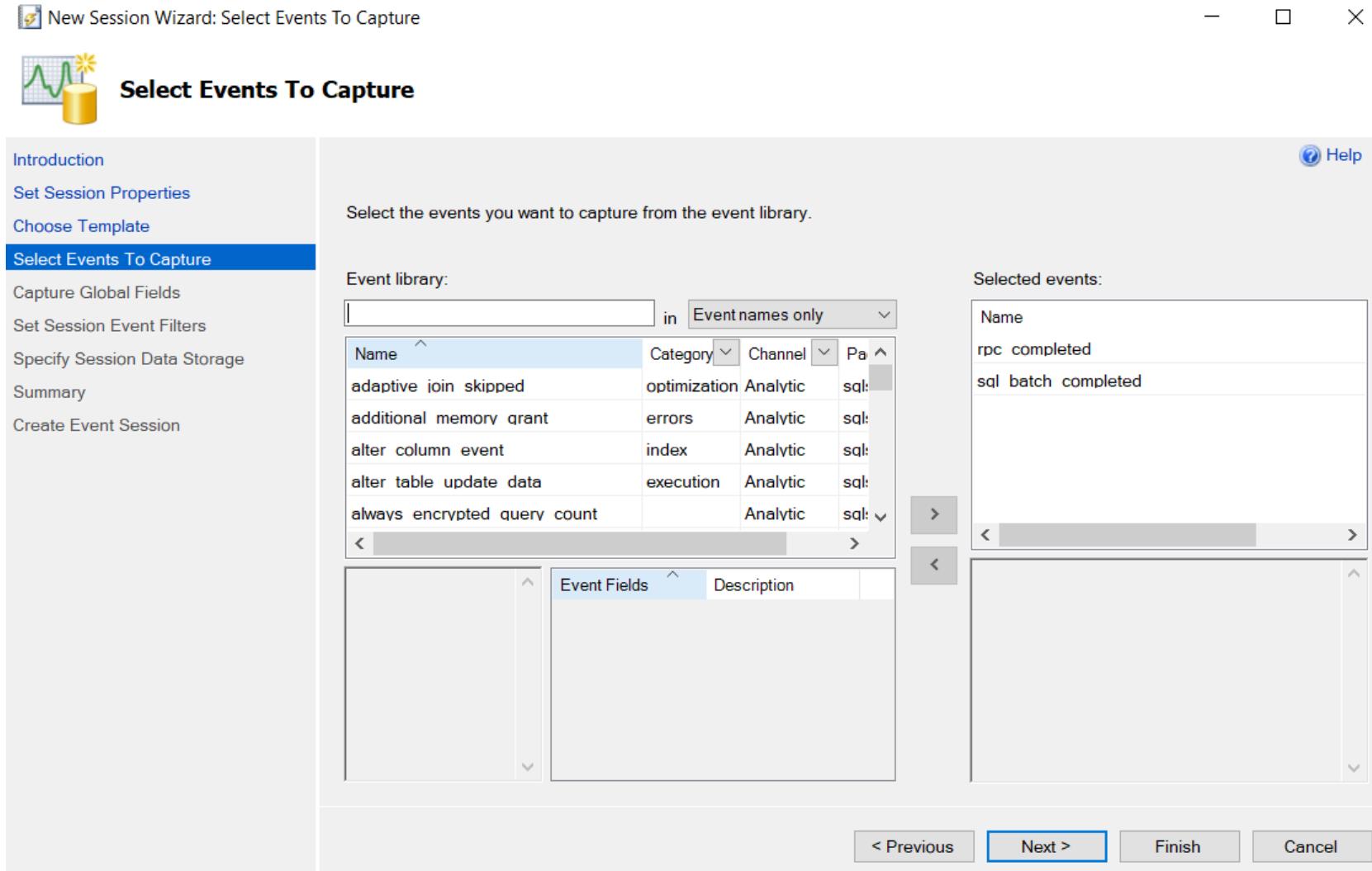
The screenshot shows the 'New Session Wizard: Choose Template' dialog box. On the left, a sidebar lists steps: Introduction, Set Session Properties, **Choose Template**, Select Events To Capture, Capture Global Fields, Set Session Event Filters, Specify Session Data Storage, Summary, and Create Event Session. The 'Choose Template' step is selected. The main area has two radio button options: 'Use this event session template:' (selected) and 'Do not use a template.' Below the first option, a dropdown menu is open, showing a list of templates categorized by color:

- Count Query Locks** (highlighted in blue)
- Profiler Equivalents**
- SP_Counts
- Standard
- TSQL
- TSQL SPs
- TSQL_Duration
- TSQL_Locks
- TSQL_Replay
- Tuning
- Query Execution**
- Query Batch Sampling** (highlighted in blue)
- Query Batch Tracking
- Query Detail Sampling
- Query Detail Tracking
- Query Wait Statistic
- System Monitoring**
- Activity Tracking
- Connection Tracking
- Database Log File IO Tracking

At the bottom of the dialog are buttons: < Previous, Next >, Finish, and Cancel.



XEVENTS SELECT EVENTS

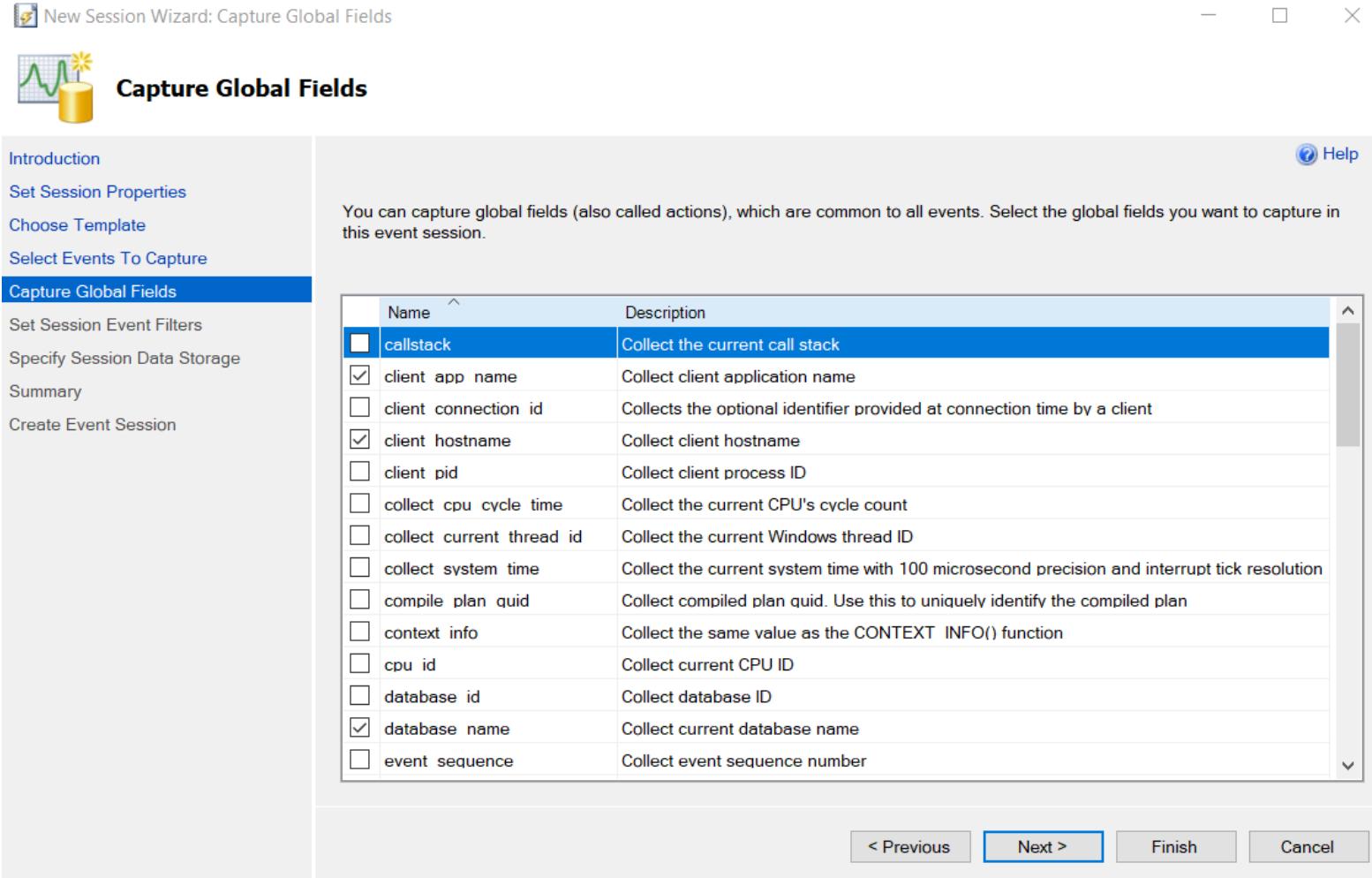


**When auditing with
xevents I use these
events:**

**rpc_completed
sql_batch_completed**



XEVENTS GLOBAL FIELDS



**When auditing with
xevents I use these
global fields:**

`client_app_name`
`client_hostname`
`database_name`
`server_instance_name`
`server_principal_name`
`sql_text`



XEVENTS APPLYING FILTERS

New Session Wizard: Set Session Event Filters

Set Session Event Filters



Introduction
Set Session Properties
Choose Template
Select Events To Capture
Capture Global Fields
Set Session Event Filters
Specify Session Data Storage
Summary
Create Event Session

You can apply filters (also called predicates) on events to limit the data you want to capture. You can specify filter options for the entire session.

Help

And/Or	Field	Operator	Value
And	sqlserver.server_principal_name	=	sa
Or	sqlserver.username	=	sa

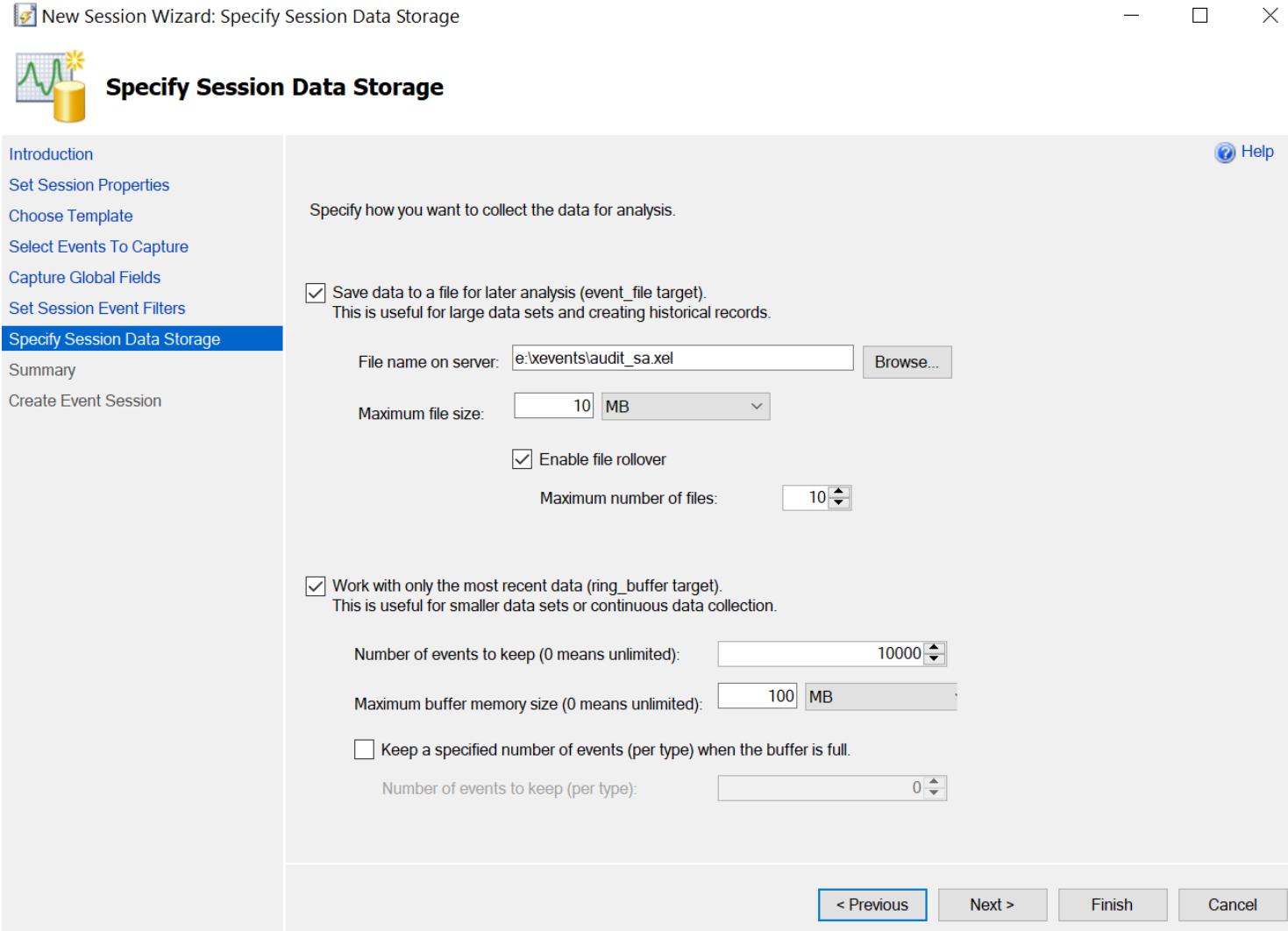
Click here to add a clause

sqlserver.username (package0.unicode_string)
Get the current username

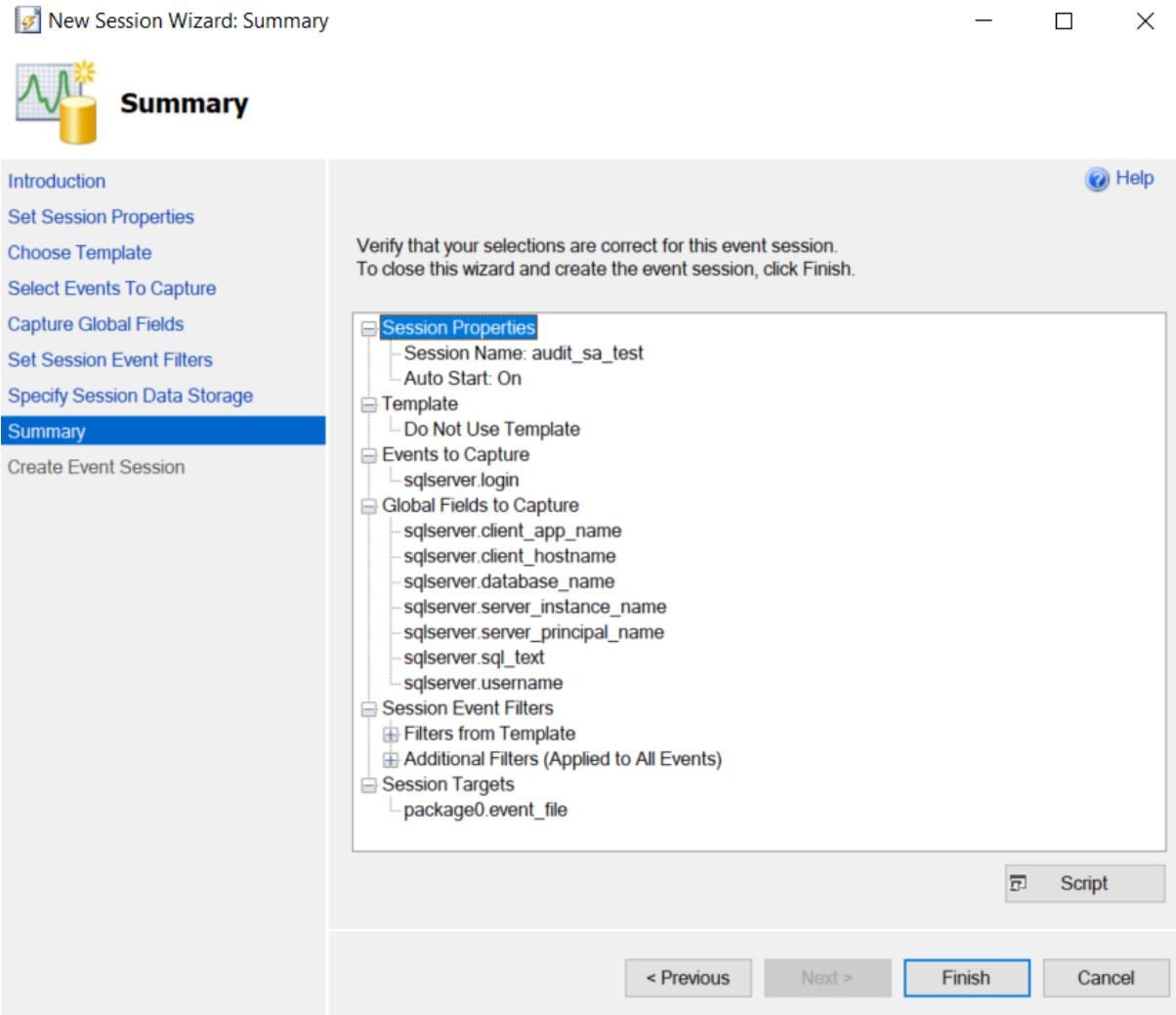
< Previous **Next >** Finish Cancel



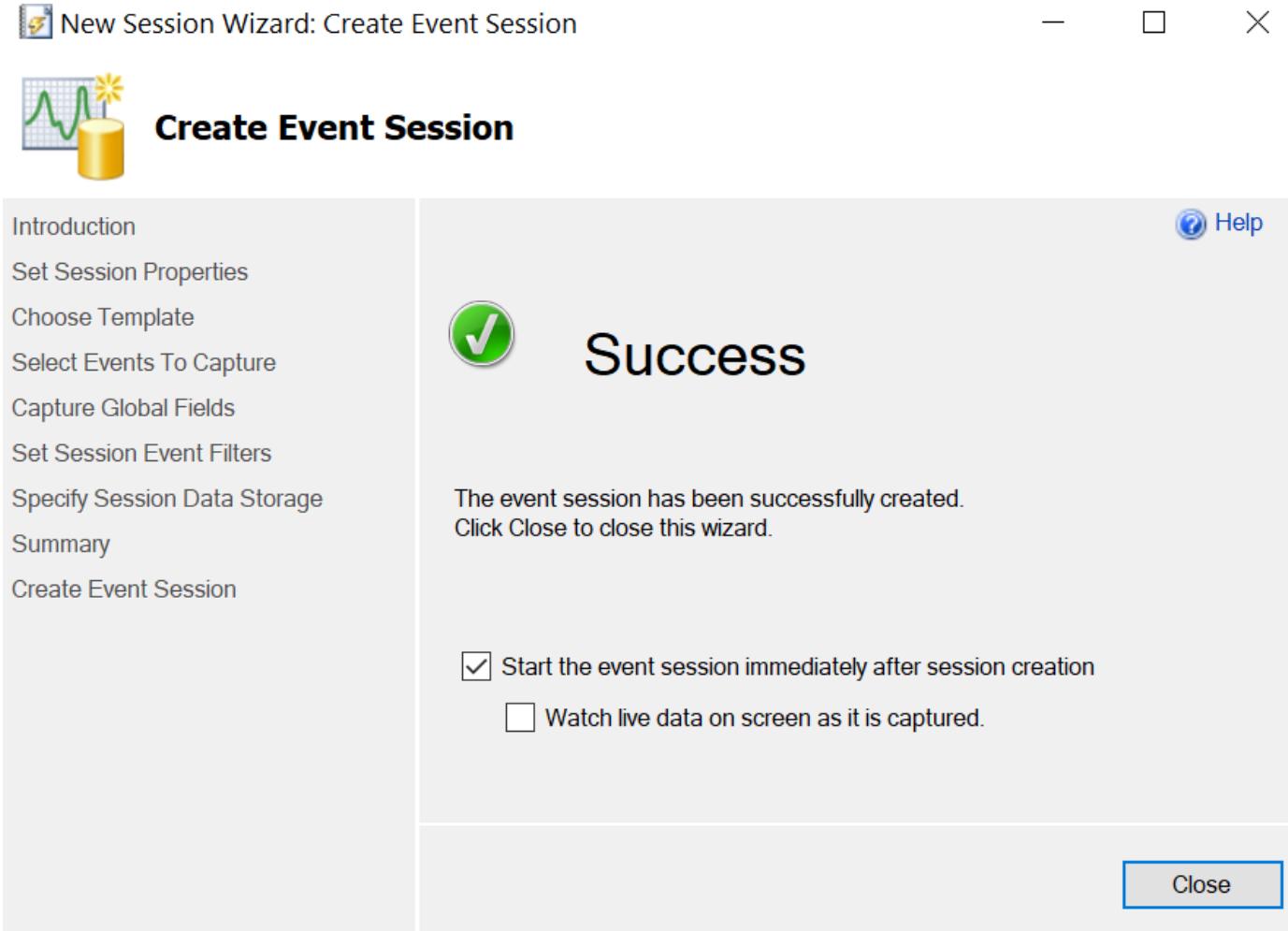
XEVENTS STORING EVENTS



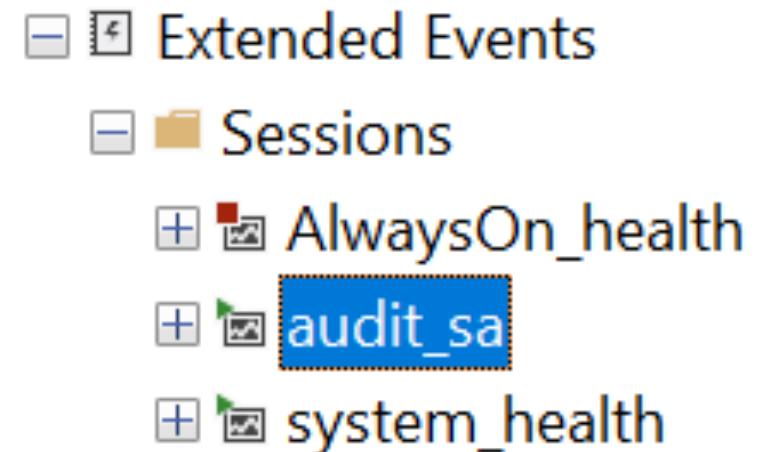
XEVENTS SUMMARY



XEVENTS CREATED



When you refresh extended events in SSMS, you will see your new xevent



XEVENT FILES ON DISK

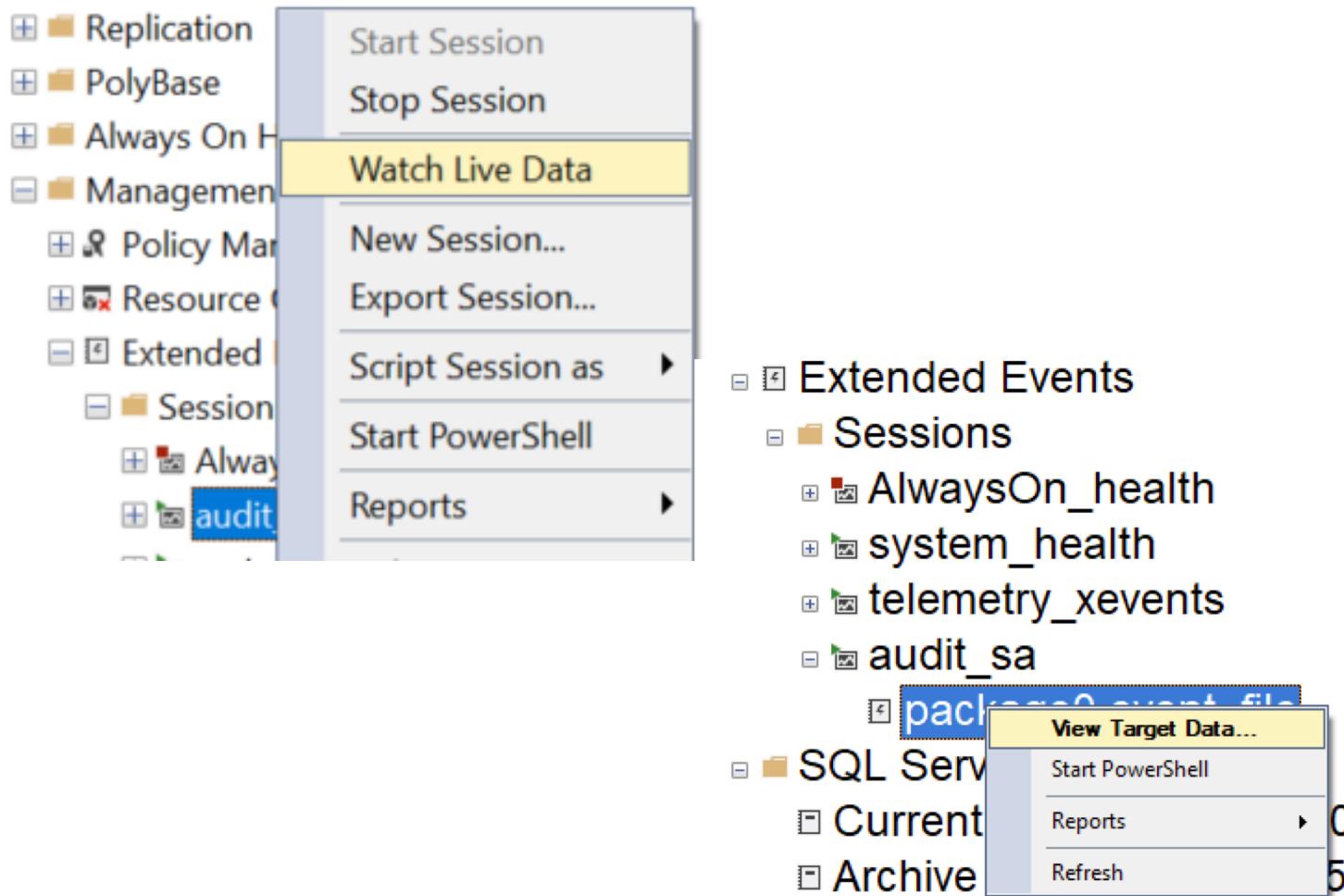
Once the xevent is enabled, it will place a file on disk

Name	Date modified	Type	Size
 audit_sa_0_132578089159200000	2/14/2021 2:08 PM	Microsoft SQL Server Extended Event Log File	100 KB



QUERY EXTENDED EVENTS VIA GUI

View extended event data via SSMS



ubuntu\$...ive Data		SQLQuer...sa (62))*
Displaying 33 Events		
name	timestamp	
rpc_completed	2021-06-05 18:04:17.1569118	
sql_batch_completed	2021-06-05 18:04:17.1808673	
sql_batch_completed	2021-06-05 18:04:17.1831300	
sql_batch_completed	2021-06-05 18:04:17.1840574	
sql_batch_completed	2021-06-05 18:04:17.1854248	
sql_batch_completed	2021-06-05 18:04:17.2051861	
rpc_completed	2021-06-05 18:04:19.6021963	
rpc_completed	2021-06-05 18:04:19.6288143	
sql_batch_completed	2021-06-05 18:04:19.6585448	
rpc_completed	2021-06-05 18:04:19.6791233	
rpc_completed	2021-06-05 18:04:19.7032714	
sql_batch_completed	2021-06-05 18:04:19.8071577	
sql_batch_completed	2021-06-05 18:04:23.7921009	
sql_batch_completed	2021-06-05 18:04:24.5169634	

Event:sql_batch_completed (2021-06-05 18:04:24.5169634)

Field	Value
database_name	master
duration	722642
logical_reads	1514
nt_username	
page_server...	0
physical_reads	1558
result	OK
row_count	0
server_prin...	sa
session_id	55
spills	0
sql_text	CREATE DATABASE testing2
username	sa
writes	41



CREATE EXTENDED EVENT VIA SCRIPT

Configure with script in SSMS

```
CREATE EVENT SESSION [audit_sa] ON SERVER
ADD EVENT sqlserver.rpc_completed(
    ACTION(sqlserver.client_app_name,
           sqlserver.client_hostname,
           sqlserver.database_name,
           sqlserver.server_instance_name,
           sqlserver.server_principal_name,
           sqlserver.sql_text)),
ADD EVENT sqlserver.sql_batch_completed(
    ACTION(sqlserver.client_app_name,sqlserver.client_hostname,sqlserver.database_name,sqlserver.server_instance_name,sqlserver.server_principal_name,sqlserver.sql_text))
ADD TARGET package0.event_file(SET
filename=N'E:\audits\audit_sa.xel',max_file_size=(10),max_rollover_files=(10))
WITH (STARTUP_STATE=ON)
GO
ALTER EVENT SESSION [audit_sa]
ON SERVER STATE = START;
GO
```



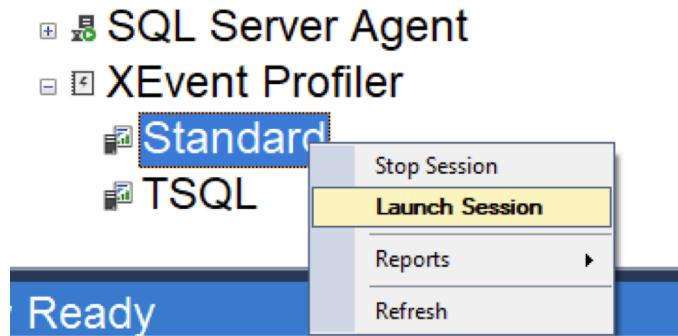
QUERY EXTENDED EVENTS VIA SCRIPT

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



QUICK VIEW XEVENTS VIA GUI



Make sure to stop it
when you are done

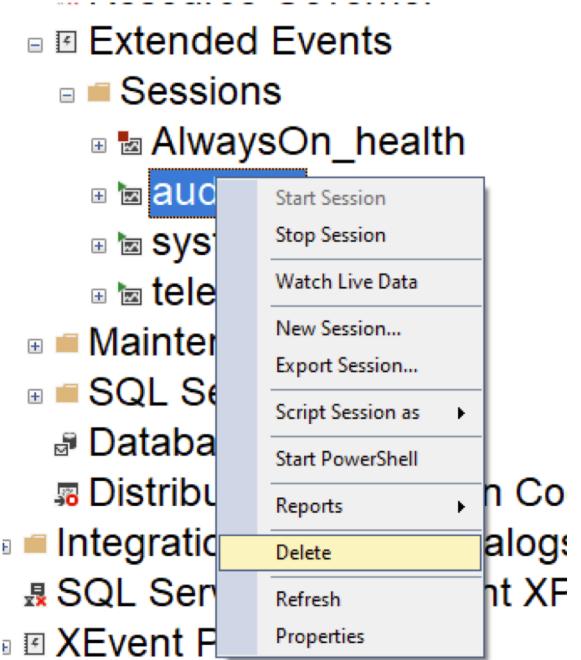
ev...	name	[TextData]	client_app_name	nt_user... AUTHO...	cpu... 0	logical... NULL	wr... 0	dura... NULL	sessi... 57	times 2021-06-05 20:42:13.9988789
48	sql_batch_starting	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	NT AUTHO... 0	NULL	NULL	NULL	NULL	57	2021-06-05 20:42:13.9988789
49	sql_batch_compl...	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	NT AUTHO... 0	0	0	0	71	57	2021-06-05 20:42:13.9988789
50	sql_batch_starting	SELECT target_data FROM...	SQLServerCEIP	NT AUTHO... 0	NULL	NULL	NULL	NULL	57	2021-06-05 20:42:13.9988789
51	sql_batch_compl...	SELECT target_data FROM...	SQLServerCEIP	NT AUTHO... 56000	0	0	0	75024	57	2021-06-05 20:42:13.9988789
52	logout	NULL	SQLServerCEIP	NT AUTHO... 56000	0	0	0	107000	57	2021-06-05 20:42:13.9988789
53	rpc_completed	exec sp_reset_connection	SQLServerCEIP	NT AUTHO... 0	0	0	0	23	57	2021-06-05 20:42:13.9988789
54	login	-- network protocol: TCP/IP set ...	SQLServerCEIP	NT AUTHO... 0	NULL	NULL	NULL	NULL	57	2021-06-05 20:42:13.9988789
55	sql_batch_starting	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	NT AUTHO... 0	NULL	NULL	NULL	NULL	57	2021-06-05 20:42:13.9988789
56	sql_batch_compl...	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	NT AUTHO... 0	0	0	0	63	57	2021-06-05 20:42:13.9988789
57	sql_batch_starting	if not exists (select * from sys....)	SQLServerCEIP	NT AUTHO... 0	NULL	NULL	NULL	NULL	57	2021-06-05 20:42:13.9988789
58	sql_batch_compl...	if not exists (select * from sys....)	SQLServerCEIP	NT AUTHO... 1000	20	0	0	1021	57	2021-06-05 20:42:13.9988789
59	sql_batch_starting	select @@trancount	Microsoft SQL Se...	0	NULL	NULL	NULL	NULL	55	2021-06-05 20:42:13.9988789
60	sql_batch_compl...	select @@trancount	Microsoft SQL Se...	0	0	0	0	438	55	2021-06-05 20:42:13.9988789
61	logout	NULL	Microsoft SQL Se...	3166000	23315	480	9856...	55	55	2021-06-05 20:42:13.9988789



DELETING XEVENTS

Two ways to delete xevents

GUI



Script

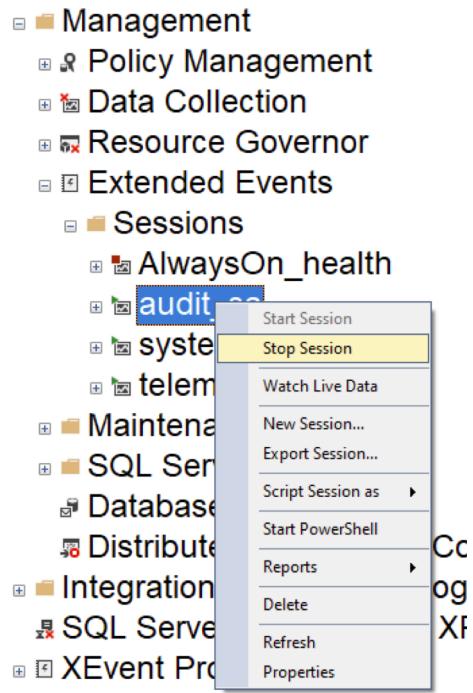
```
DROP EVENT SESSION [audit_sa]
ON SERVER
GO
```



STOPPING XEVENTS

Two ways to stop xevents

GUI



Script

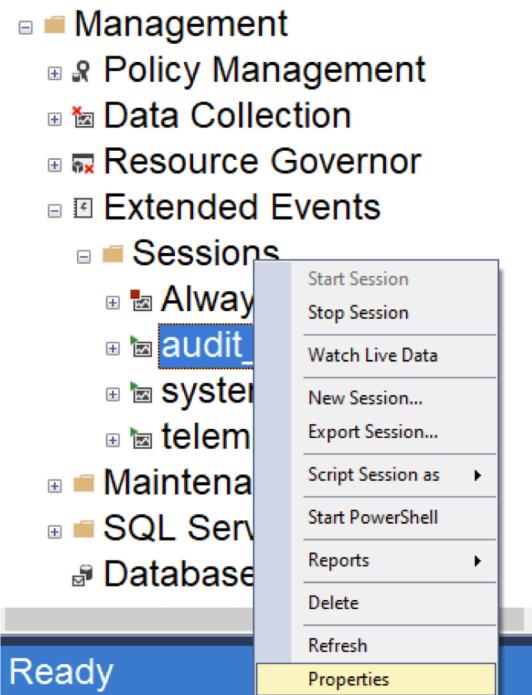
```
ALTER EVENT SESSION [audit_sa]
ON SERVER STATE = STOP;
GO
```



MODIFYING XEVENTS

Two ways to change xevents

GUI



Script

```
ALTER EVENT SESSION [audit_sa] ON SERVER
DROP EVENT sqlserver.rpc_completed
ALTER EVENT SESSION [audit_sa] ON SERVER
ADD EVENT sqlserver.rpc_completed(
    ACTION(sqlserver.client_app_name,sqlserver.client_hostname,sqlserver.database_name,sqlserver.server_instance_name,sqlserver.server_principal_name,sqlserver.sql_text,sqlserver.username))
```



EXTENDED EVENTS REVIEW

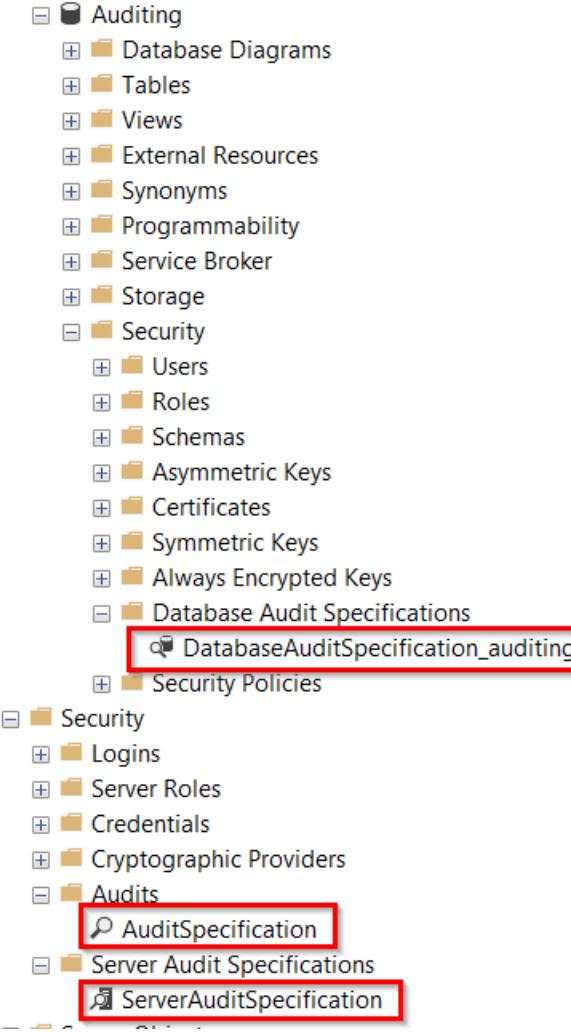


Lightweight, customizable
Best for capturing what a user is
doing and/or what's changing on
an entire database or server
Create via GUI or scripts

EXTENDED EVENTS DEMO



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 REQUIREMENTS

You need two things to make this work:

One audit specification (required)

And one of these things:

1. A server audit specification
2. A database audit specification

	■ Auditing
■ Database Diagrams	
■ Tables	
■ Views	
■ External Resources	
■ Synonyms	
■ Programmability	
■ Service Broker	
■ Storage	
■ Security	
■ Users	
■ Roles	
■ Schemas	
■ Asymmetric Keys	
■ Certificates	
■ Symmetric Keys	
■ Always Encrypted Keys	
■ Database Audit Specifications	
DatabaseAuditSpecification_Auditing	
■ Security Policies	
■ Security	
■ Logins	
■ Server Roles	
■ Credentials	
■ Cryptographic Providers	
■ Audits	
AuditSpecification	
■ Server Audit Specifications	
ServerAuditSpecification	



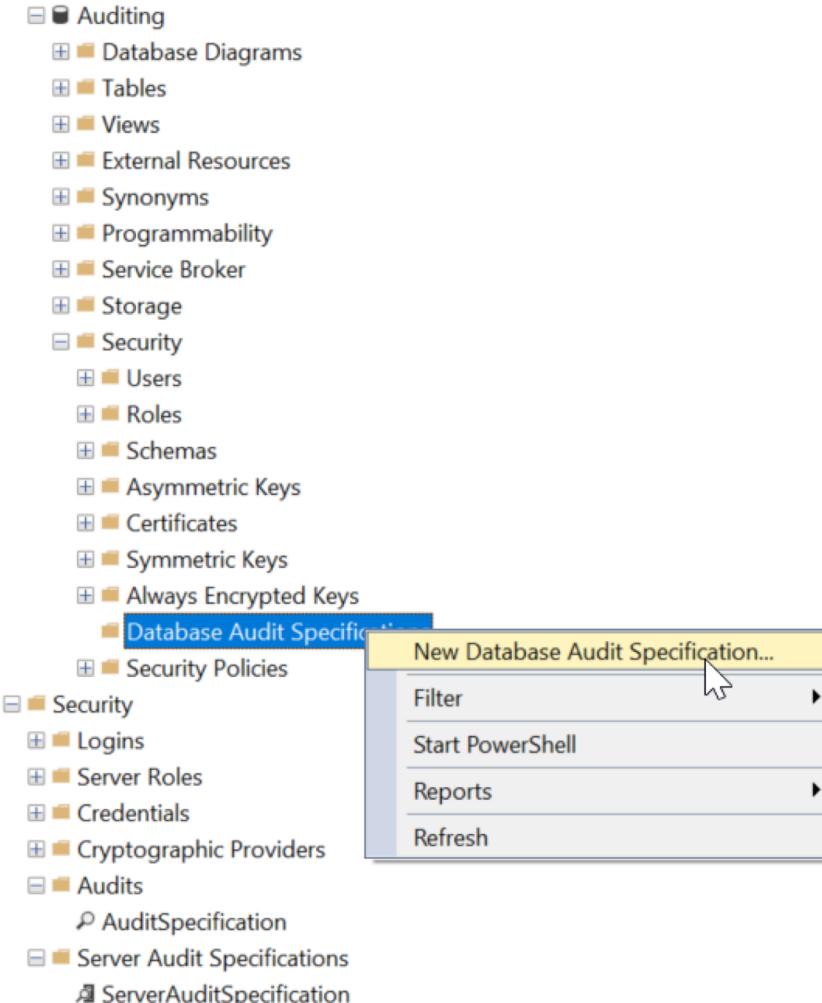
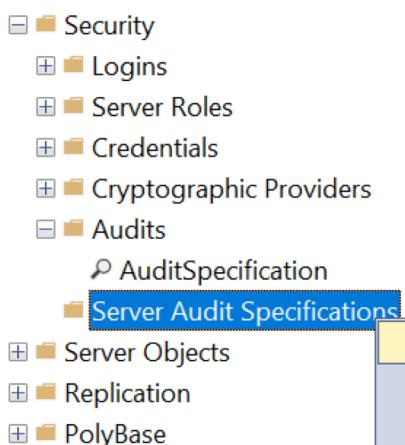
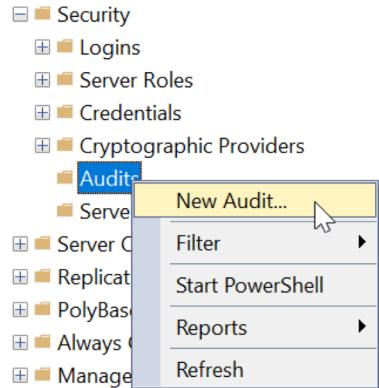
SQL SERVER AUDIT USE CASES

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

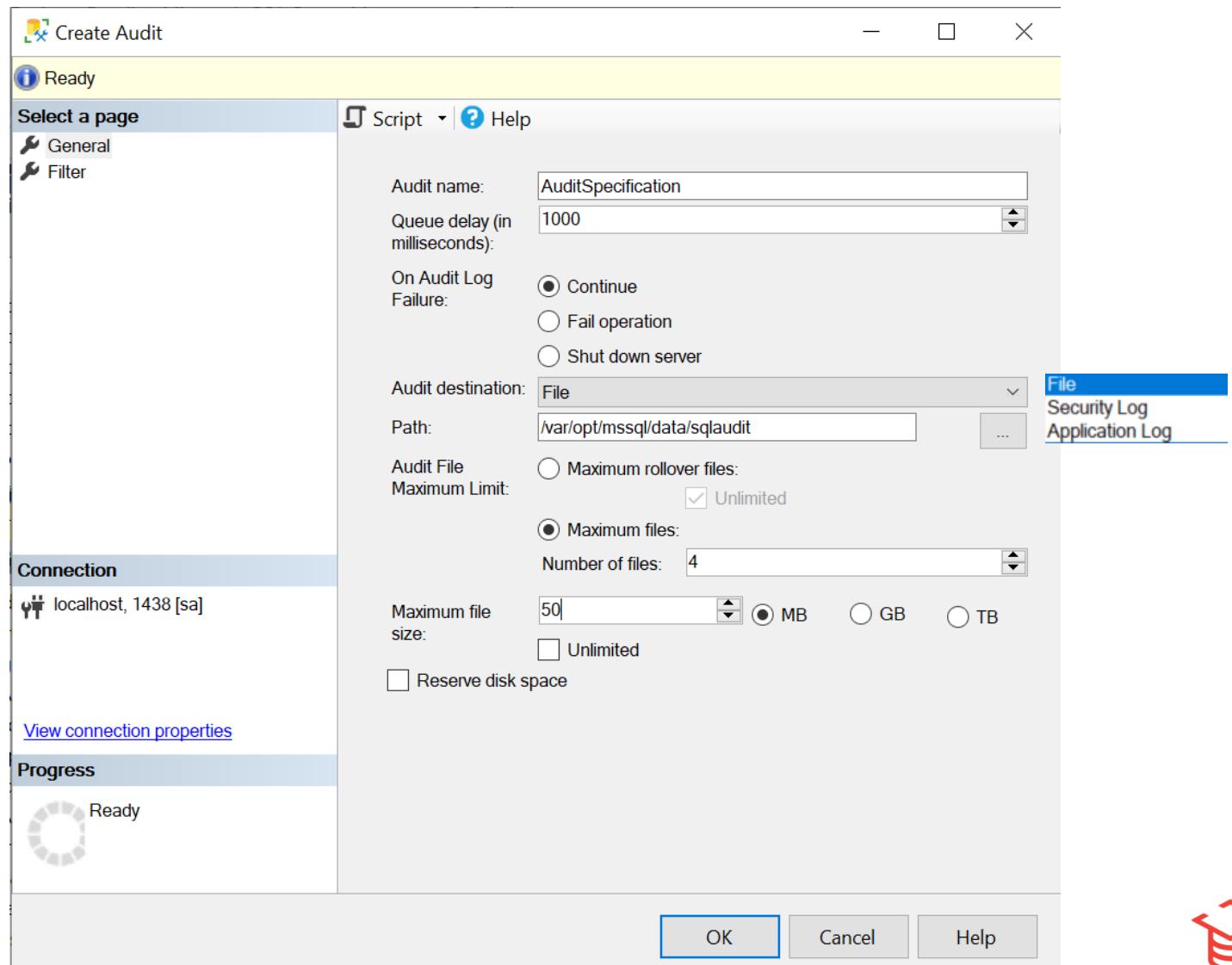


CREATE AUDIT VIA GUI



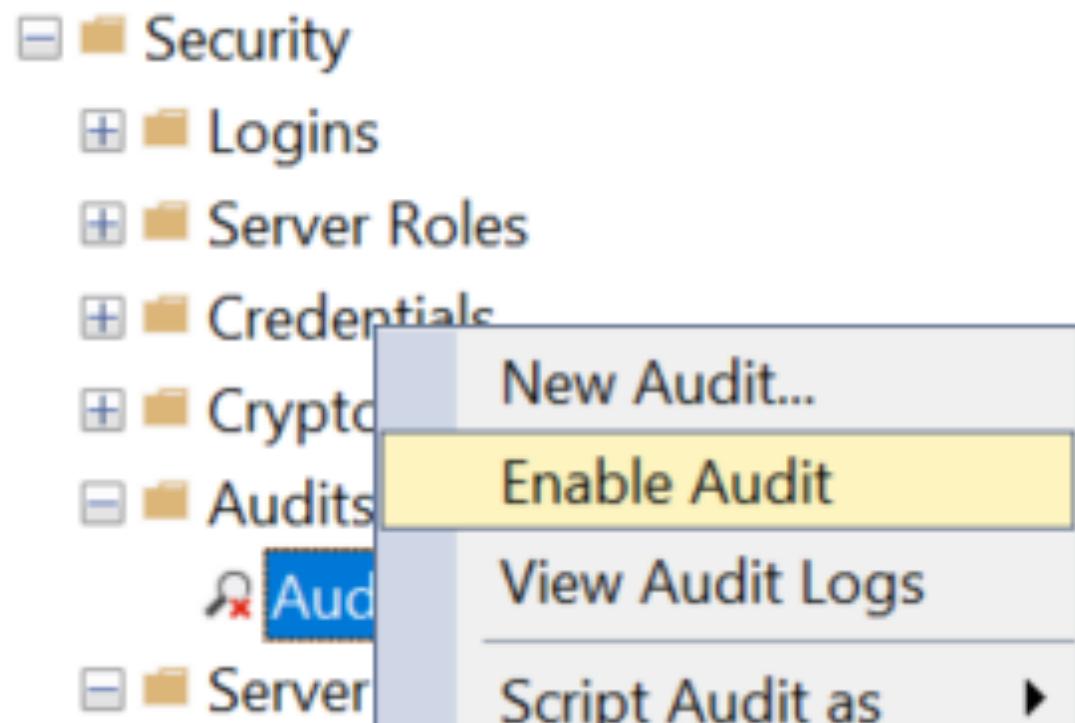
CONFIGURE AUDIT VIA GUI

Configuring an audit specification



ENABLING AUDIT VIA GUI

Audit specifications are disabled after creation by default



AUDIT FILES ON DISK

Once audit is enabled, it will place a file on disk

Name	Date modified	Type	Size
AuditSpecification_D0B8D5A4-96BE-468F-A58F-41CCC3BC9E57_0_132576453114750...	2/12/2021 4:15 PM	SQLAUDIT File	0 KB



AUDIT CATEGORIES

Server-level actions

These capture permission changes and creating databases. Includes any action that doesn't start with schema or database

Database-level actions

These include data manipulation languages (DML) and data definition language (DDL) changes. Namely things at the database level. Includes any action that starts with schema or database

Audit-level actions

These include actions in the auditing process, such as creating or dropping an audit specification. This is the AUDIT_CHANGE_GROUP option.



SERVER AUDIT ACTION GROUPS

Commonly used server-level actions

SERVER_OBJECT_CHANGE_GROUP	Captures CREATE, ALTER, or DROP actions at server level.
SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP	Captures when the owner of a server object is changed.
SERVER_OBJECT_PERMISSION_CHANGE_GROUP	Captures when GRANT, REVOKE, or DENY on a server object permission
SERVER_OPERATION_GROUP	Captures changes like altering settings, resources, external access, or authorization
SERVER_PERMISSION_CHANGE_GROUP	Captures when GRANT, REVOKE, or DENY for permissions at server level
SERVER_PRINCIPAL_CHANGE_GROUP	Captures when server principals are created, altered, or dropped.
SERVER_ROLE_MEMBER_CHANGE_GROUP	Captures when a login is added or removed from a fixed server role like db_datareader for example.
SERVER_STATE_CHANGE_GROUP	Captures when the SQL Server service state is modified like when it's restarted after patching
LOGIN_CHANGE_PASSWORD_GROUP	Captures when a login password is changed

DATABASE AUDIT ACTION GROUPS

Commonly used database-level actions

DATABASE_CHANGE_GROUP	Captures when a database is created, altered, or dropped
DATABASE_OBJECT_ACCESS_GROUP	Captures when database objects such as certificates and asymmetric keys are accessed.
DATABASE_OBJECT_CHANGE_GROUP	Captures when CREATE, ALTER, or DROP statement is executed on database objects, such as schemas
DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP	Captures when a change of owner for objects within database scope occurs.
DATABASE_OBJECT_PERMISSION_CHANGE_GROUP	Captures when a GRANT, REVOKE, or DENY has been issued for database objects, such as assemblies and schemas
DATABASE_OWNERSHIP_CHANGE_GROUP	Captures when you use the ALTER AUTHORIZATION statement to change the owner of a database
DATABASE_PERMISSION_CHANGE_GROUP	Captures when a GRANT, REVOKE, or DENY is issued for a statement permission
DATABASE_PRINCIPAL_CHANGE_GROUP	Captures when principals, such as users, are created, altered, or dropped from a database
DATABASE_ROLE_MEMBER_CHANGE_GROUP	Captures when a login is added to or removed from a database role.



DATABASE AUDIT ACTION GROUPS

Other commonly used database-level actions

APPLICATION_ROLE_CHANGE_PASSWORD_GROUP	Captures whenever a password is changed for an application role
DBCC_GROUP	Captures when a principal issues any DBCC command
SCHEMA_OBJECT_CHANGE_GROUP	Captures when a CREATE, ALTER, or DROP operation is performed on a schema
SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP	Captures when the permissions changes to the owner of schema object
SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP	Captures whenever a grant, deny, or revoke is issued for a schema object



DATABASE AUDIT ACTIONS

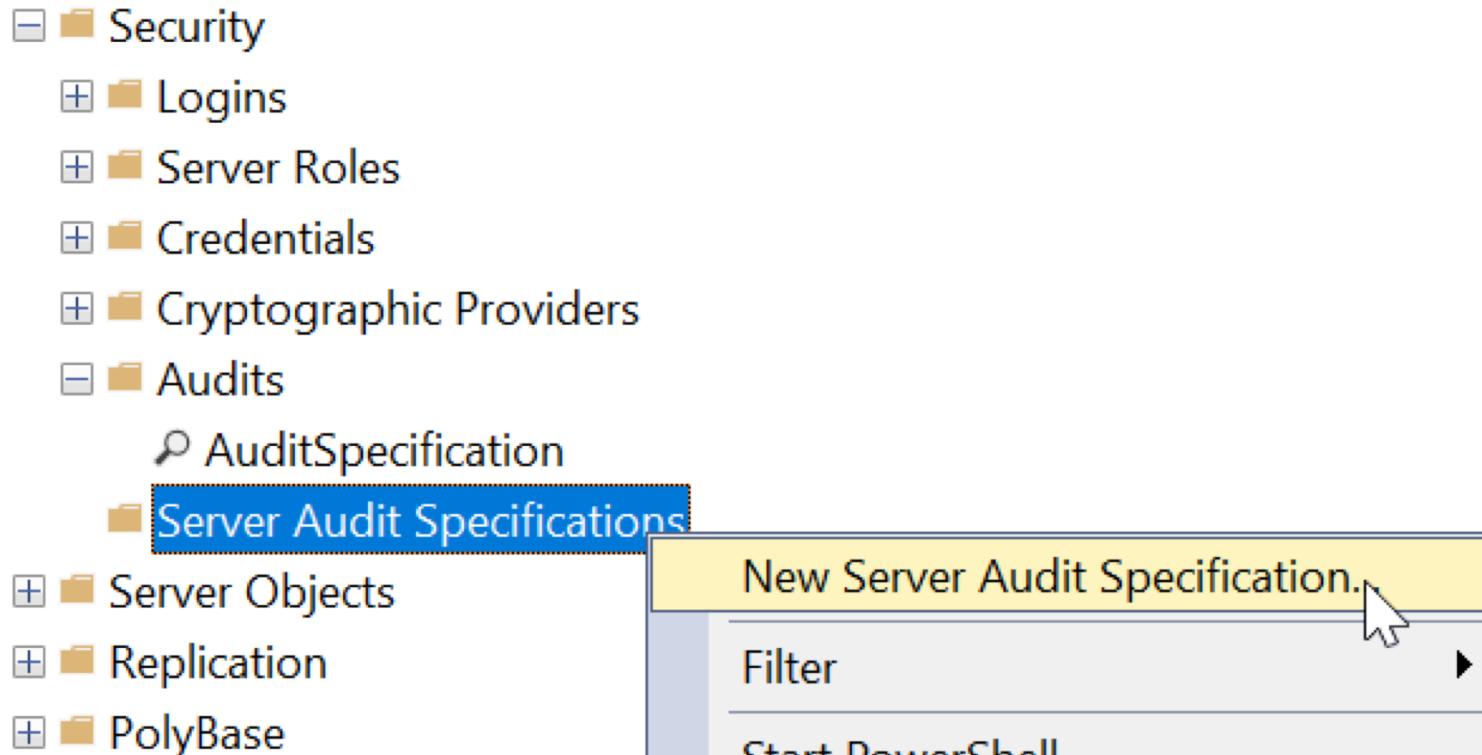
Capturing DML

SELECT	Captures SELECT statements
INSERT	Captures INSERT statements
UPDATE	Captures UPDATE statements
DELETE	Captures DELETE statements
EXECUTE	Captures EXECUTE statements



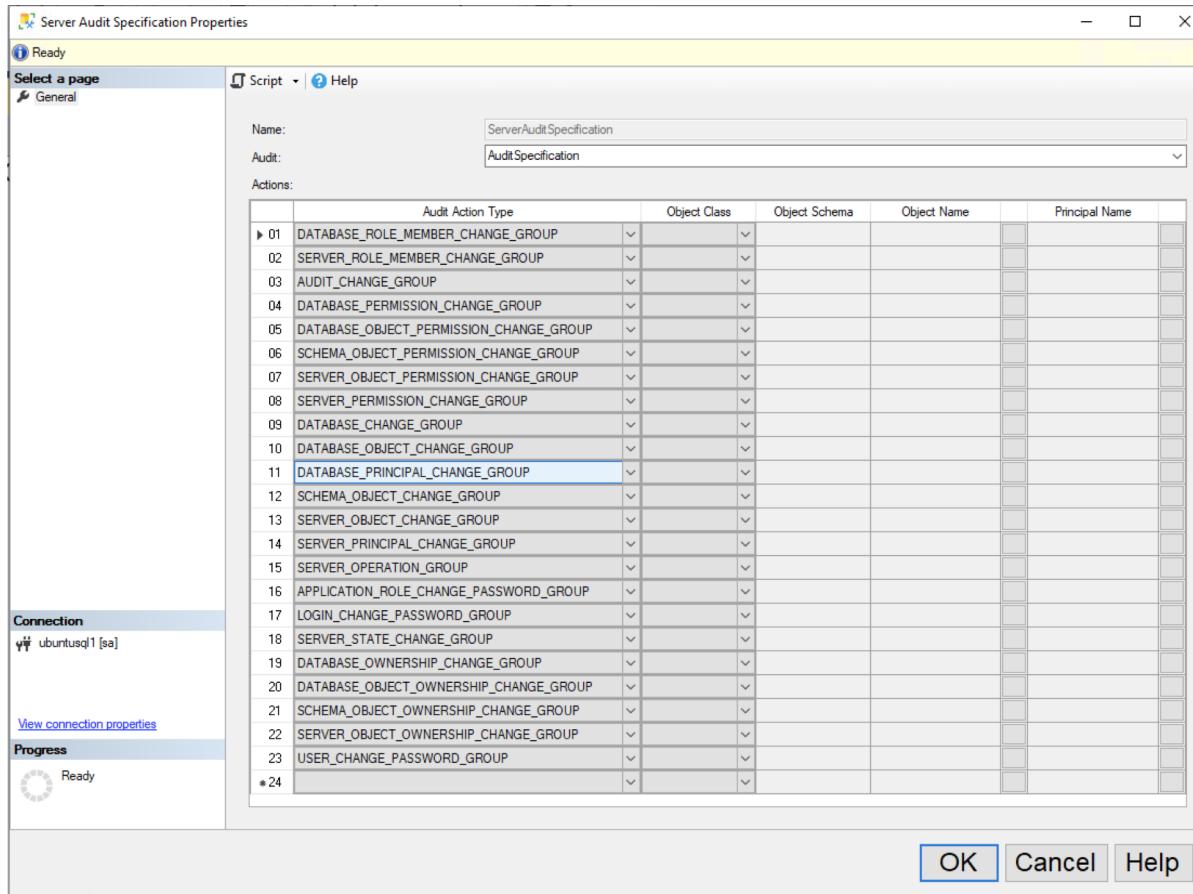
CREATE SERVER AUDIT VIA GUI

Creating a server audit specification in SSMS



CONFIGURE SERVER AUDIT VIA GUI

Configuring a server audit specification via SSMS

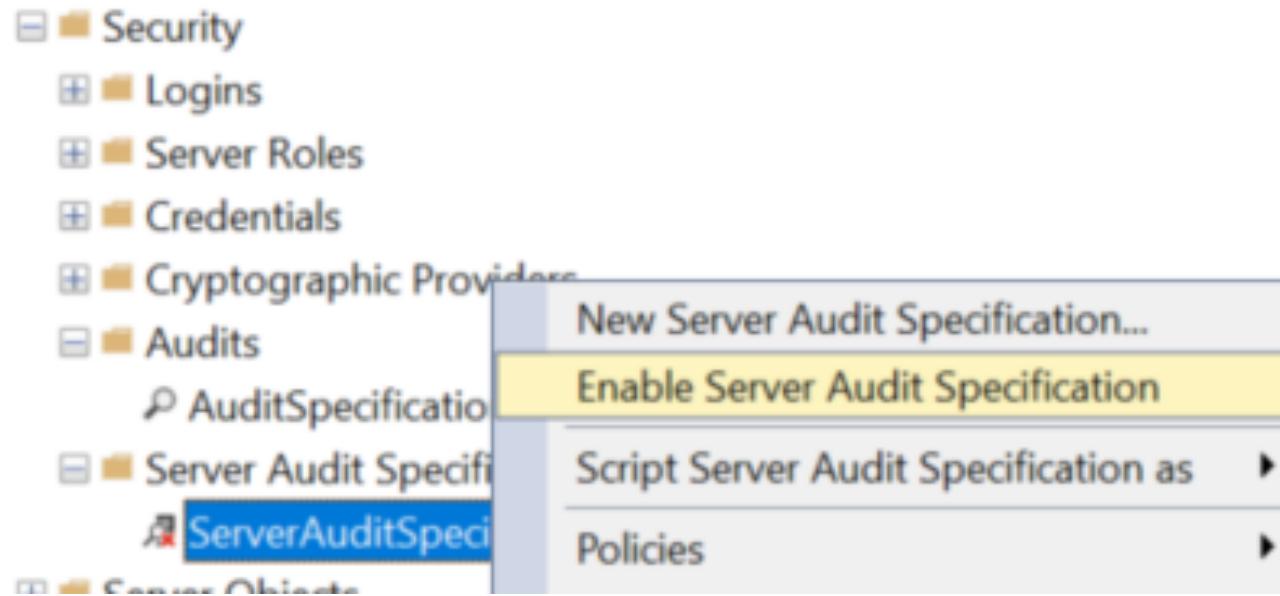


Audit Action Type		
► 01	DATABASE_ROLE_MEMBER_CHANGE_GROUP	v
02	SERVER_ROLE_MEMBER_CHANGE_GROUP	v
03	AUDIT_CHANGE_GROUP	v
04	DATABASE_PERMISSION_CHANGE_GROUP	v
05	DATABASE_OBJECT_PERMISSION_CHANGE_GROUP	v
06	SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP	v
07	SERVER_OBJECT_PERMISSION_CHANGE_GROUP	v
08	SERVER_PERMISSION_CHANGE_GROUP	v
09	DATABASE_CHANGE_GROUP	v
10	DATABASE_OBJECT_CHANGE_GROUP	v
11	► DATABASE_PRINCIPAL_CHANGE_GROUP	v
12	SCHEMA_OBJECT_CHANGE_GROUP	v
13	SERVER_OBJECT_CHANGE_GROUP	v
14	SERVER_PRINCIPAL_CHANGE_GROUP	v
15	SERVER_OPERATION_GROUP	v
16	APPLICATION_ROLE_CHANGE_PASSWORD_GROUP	v
17	LOGIN_CHANGE_PASSWORD_GROUP	v
18	SERVER_STATE_CHANGE_GROUP	v
19	DATABASE_OWNERSHIP_CHANGE_GROUP	v
20	DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP	v
21	SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP	v
22	SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP	v
23	USER_CHANGE_PASSWORD_GROUP	v
* 24		v



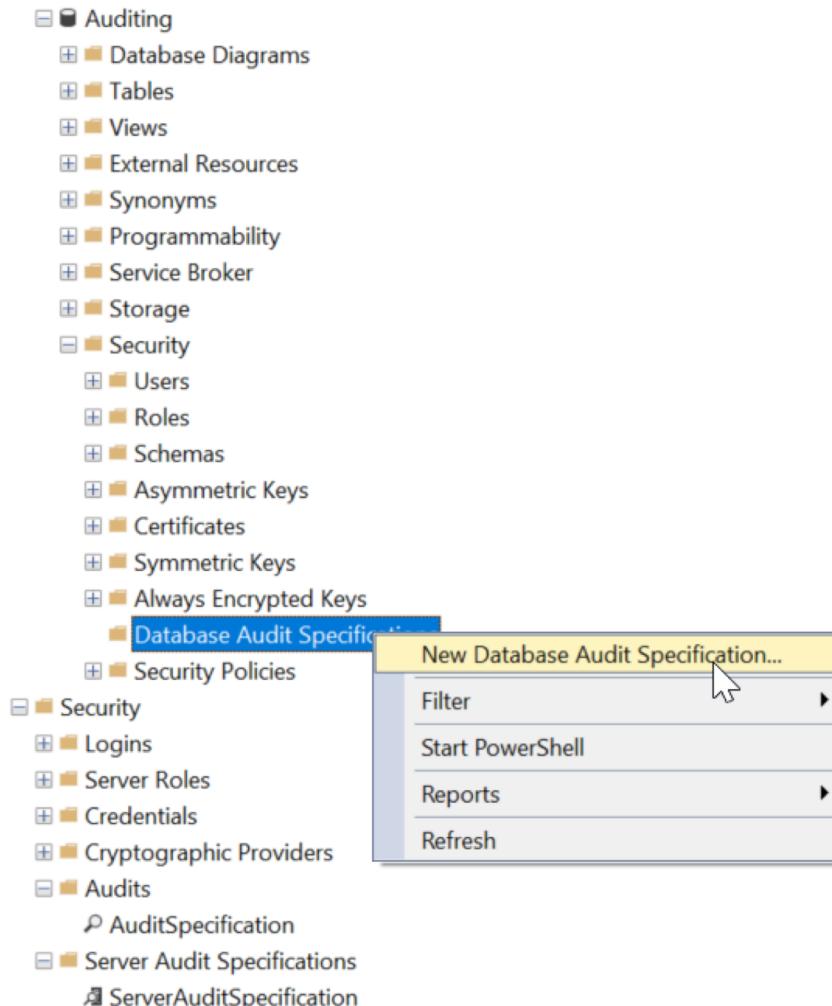
ENABLING SERVER AUDIT VIA GUI

Server audit specifications are disabled after creation by default



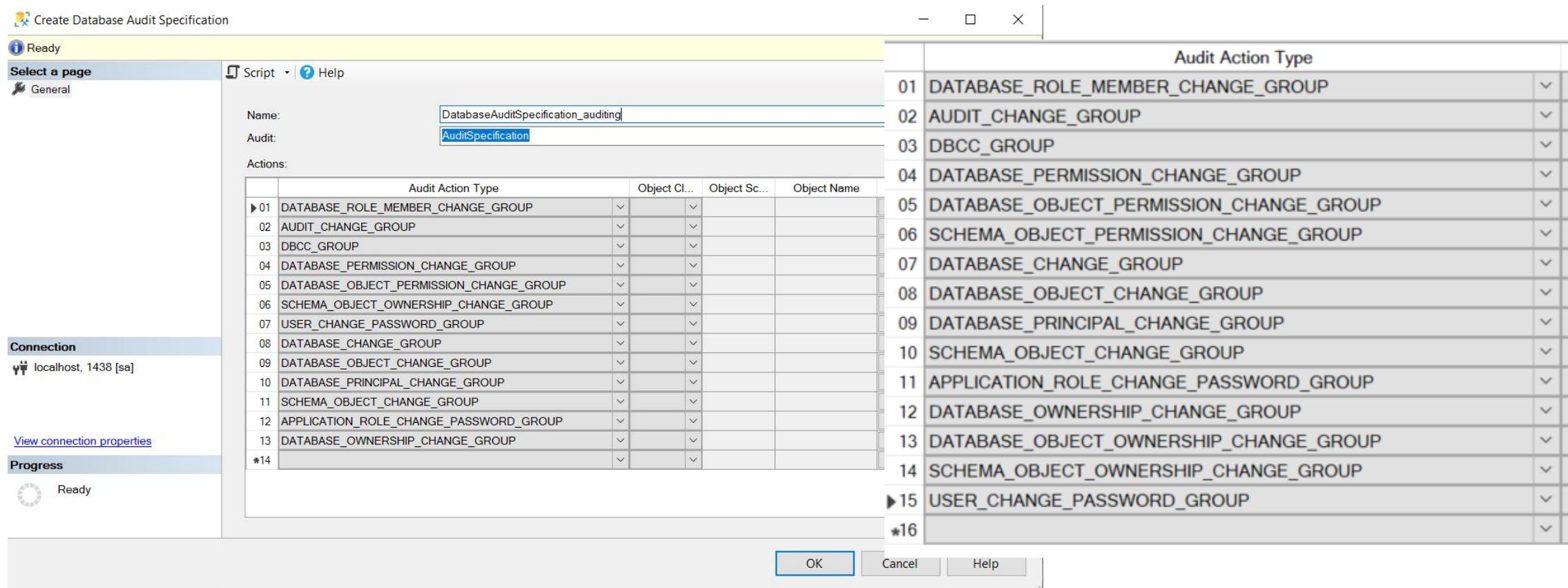
CREATE DATABASE AUDIT VIA GUI

Creating a database audit specification via SSMS



CONFIGURE DATABASE AUDIT VIA GUI

Configuring a database audit specification via SSMS



SQL SERVER AUDIT OBJECTS VIA GUI

Create Database Audit Specification

Ready

Select a page: General | Script | Help

Name: DatabaseAuditSpecification_AuditingTables

Audit: AuditSpecification_AuditingTables

Actions:

	Audit Action Type	Object Class	Object Schema	Object Name	Principal Name	
1	INSERT	OBJECT	dbo	testing	public	...
2	UPDATE	OBJECT	dbo	testing	public	...
3	EXECUTE	OBJECT	dbo	SelectTestingTable	public	...
4	SELECT	OBJECT	dbo	TestingTop10	public	...
5	DELETE	SCHEMA		dbo	auditing	...
▶6	UPDATE	DATABASE		Auditing	public	...
*7						

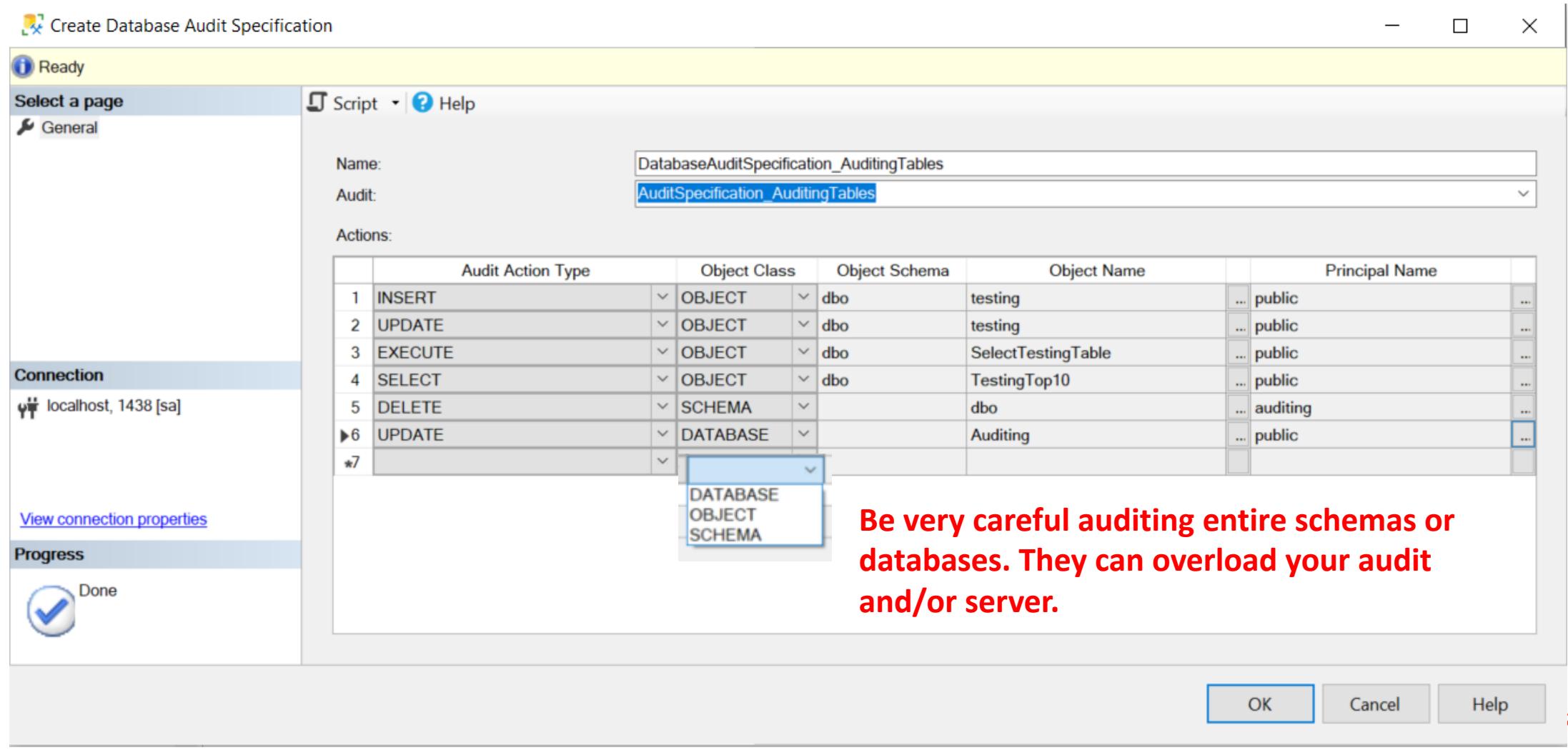
Be very careful auditing entire schemas or databases. They can overload your audit and/or server.

OK Cancel Help

Connection: localhost, 1438 [sa]

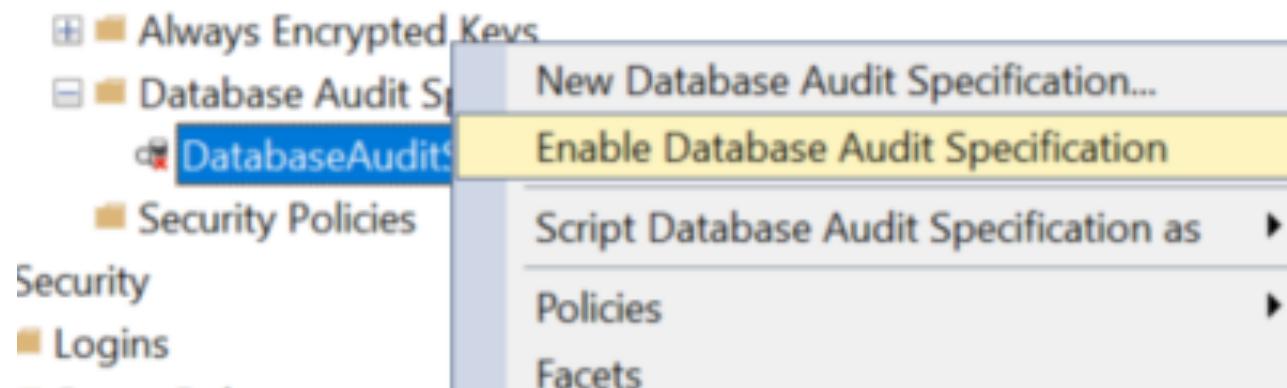
View connection properties

Progress: Done



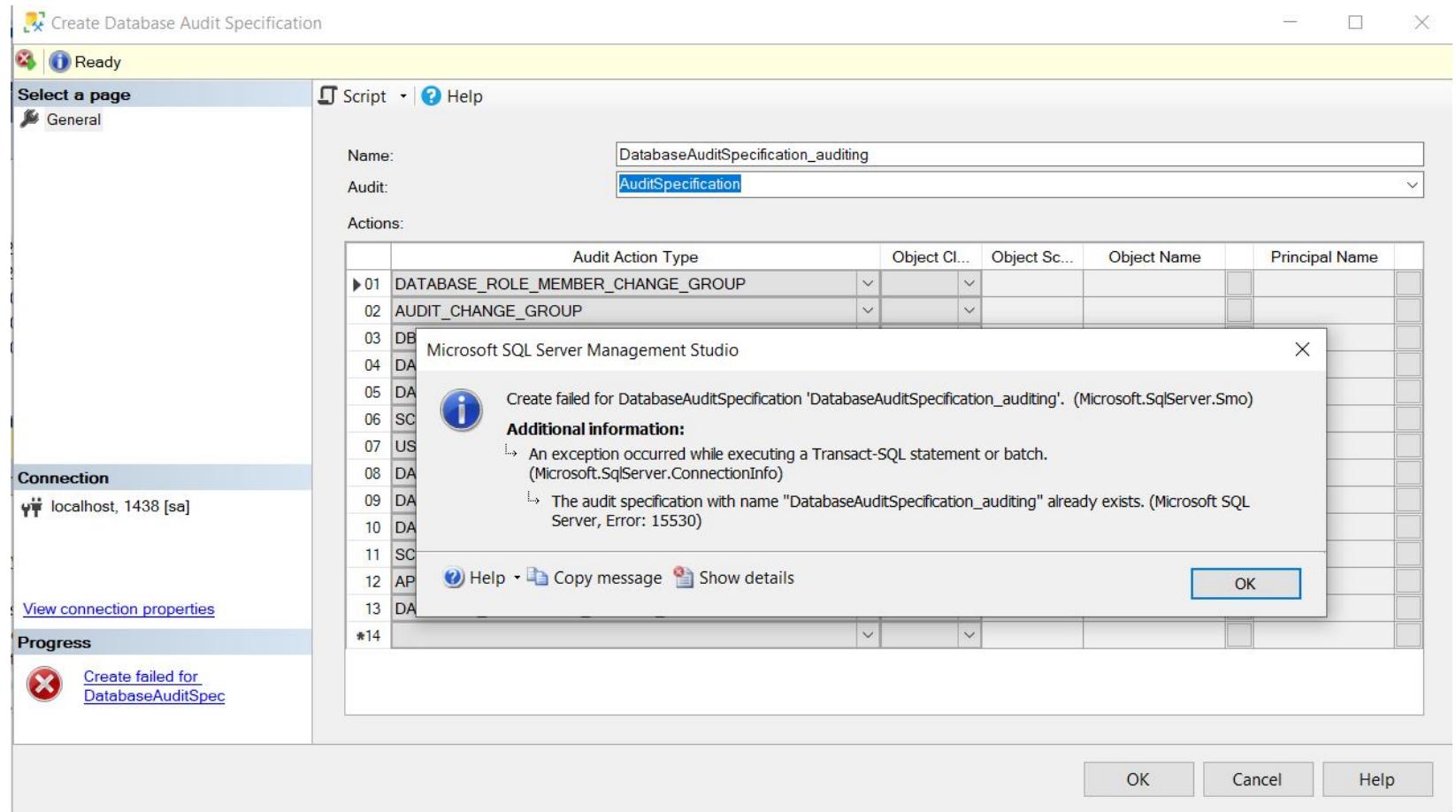
ENABLING DATABASE AUDIT VIA GUI

Database audit specifications are disabled after creation by default



ADDING MULTIPLE AUDITS ERROR

You must add additional audit specifications to add additional server or database specifications



ADDING MULTIPLE AUDITS

Audit scenario	Audit specification	Server audit specification	Database audit specification
Auditing schema and perms changes at server and db level	Audit_SchemaPerms	ServerAudit_SchemaPerms	
Audit everything sa does	Audit_sa with filter to just get sa user	ServerAudit_sa which includes auditing schema & perms, but also anything else happening at the db level	



ADDING MULTIPLE AUDITS

Audit scenario	Audit specification	Server audit specification	Database audit specification
Audit everyone changing a table	Audit_tblChanges		DatabaseAudit_tblChanges with insert, update, delete on the table
Auditing schema and perms changes at server level and specific database	Audit_Changes	ServerAudit_Changes Don't audit databases at server level	DatabaseAudit_Changes Just on the database you need to audit



QUERYING AUDIT VIA GUI

The screenshot shows the SQL Server Management Studio (SSMS) interface. On the left, the Object Explorer tree is visible with nodes like Audits, AuditSpec, Server Audit, Server Audit Policies, Server Objects, Replication, PolyBase, and Always On. A context menu is open over the AuditSpec node, with the 'View Audit Logs' option highlighted in yellow. To the right of the tree, the 'Log File Viewer - localhost, 1438' window is open. The window title bar says 'Log File Viewer - localhost, 1438'. The main area displays a table of audit logs with columns: Date, Event Time, Server Instance Name, and Action ID. The table shows numerous entries for 'Audit SESSION CHANGED', 'ALTER', and 'SELECT' actions. At the bottom of the viewer, a 'Selected row details:' section provides specific information for the last log entry:

Date	2/17/2021 10:05:39 PM
Log	Audit Collection (AuditSpecification)
Event Time	22:05:39.1609474
Server Instance Name	f1e384ca8e38
Action ID	AUDIT SESSION CHANGED
Class Type	SERVER AUDIT
Sequence Number	1
Succeeded	True
Permission Bit Mask	0x00000000000000000000000000000000
Column Permission	False
Session ID	56
Server Principal ID	1



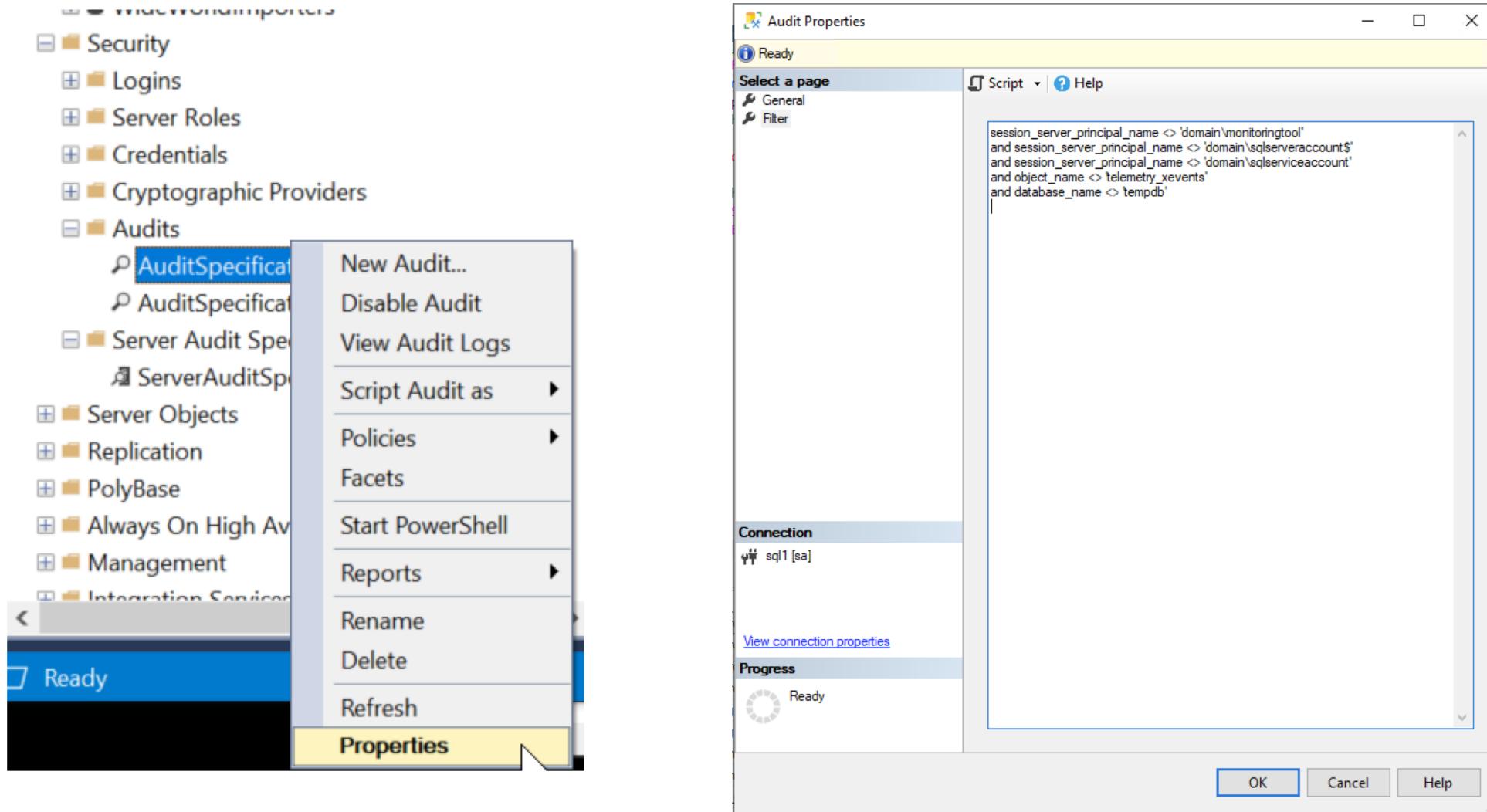
COLUMNS AVAILABLE IN SQL AUDIT

Different versions of SQL Server have different columns available

SQL Server 2012/2014/2016	SQL Server 2017	SQL Server 2019
event_time	event_time	event_time
action_id	action_id	action_id
succeeded	succeeded	succeeded
server_principal_name	server_principal_name	server_principal_name
server_instance_name	server_instance_name	server_instance_name
database_name	database_name	database_name
schema_name	schema_name	schema_name
object_name	object_name	object_name
statement	statement	statement
file_name	file_name	file_name
	client_ip	client_ip
	application_name	application_name
		host_name



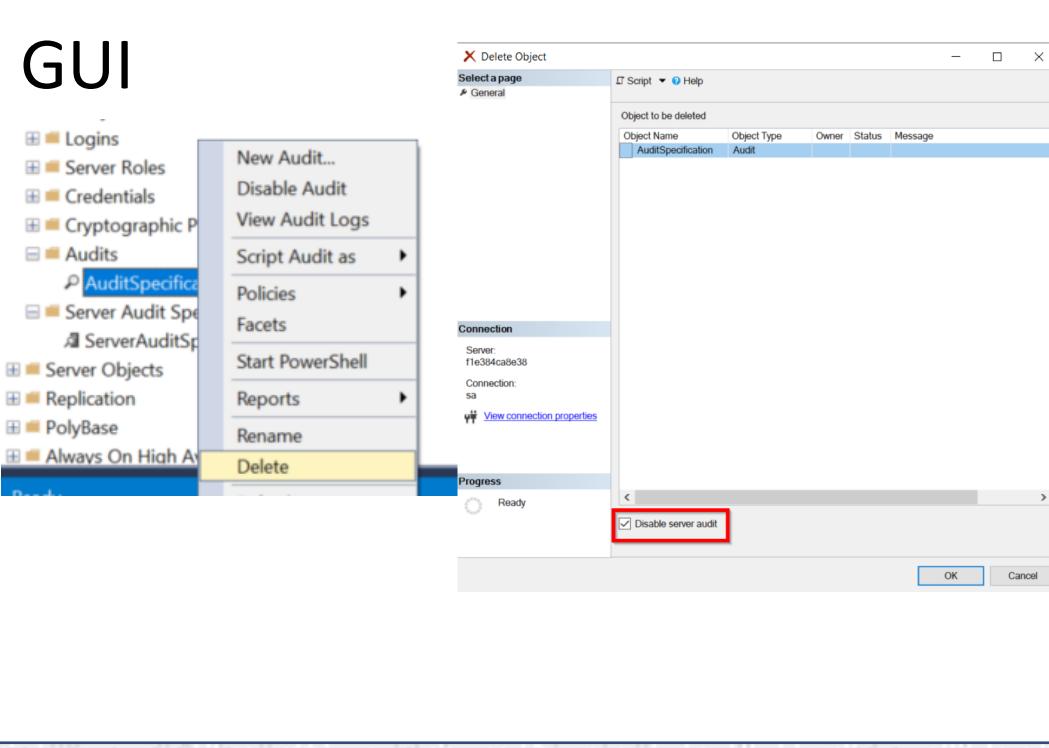
FILTERING AUDITS WITH GUI



DELETING AUDITS

Two ways to delete audits

GUI



Script

The screenshot shows the SSMS Object Explorer Details pane. A T-SQL script is being run in a query window titled 'SQLQuery12.sql*'. The script consists of five numbered lines: 1. USE [master], 2. GO, 3. , 4. DROP SERVER AUDIT [AuditSpecification], and 5. GO. In the 'Messages' pane below, an error message is displayed: 'Msg 33071, Level 16, State 1, Line 5 This command requires audit to be disabled. Disable the audit and rerun this command.' The status bar at the bottom indicates '110 %' completion.

```
1 USE [master]
2 GO
3
4 DROP SERVER AUDIT [AuditSpecification]
5 GO
```



STOPPING AUDITS

Two ways to stop audits

GUI



Script

```
USE master;
ALTER SERVER AUDIT AuditSpecification
WITH (STATE = OFF);

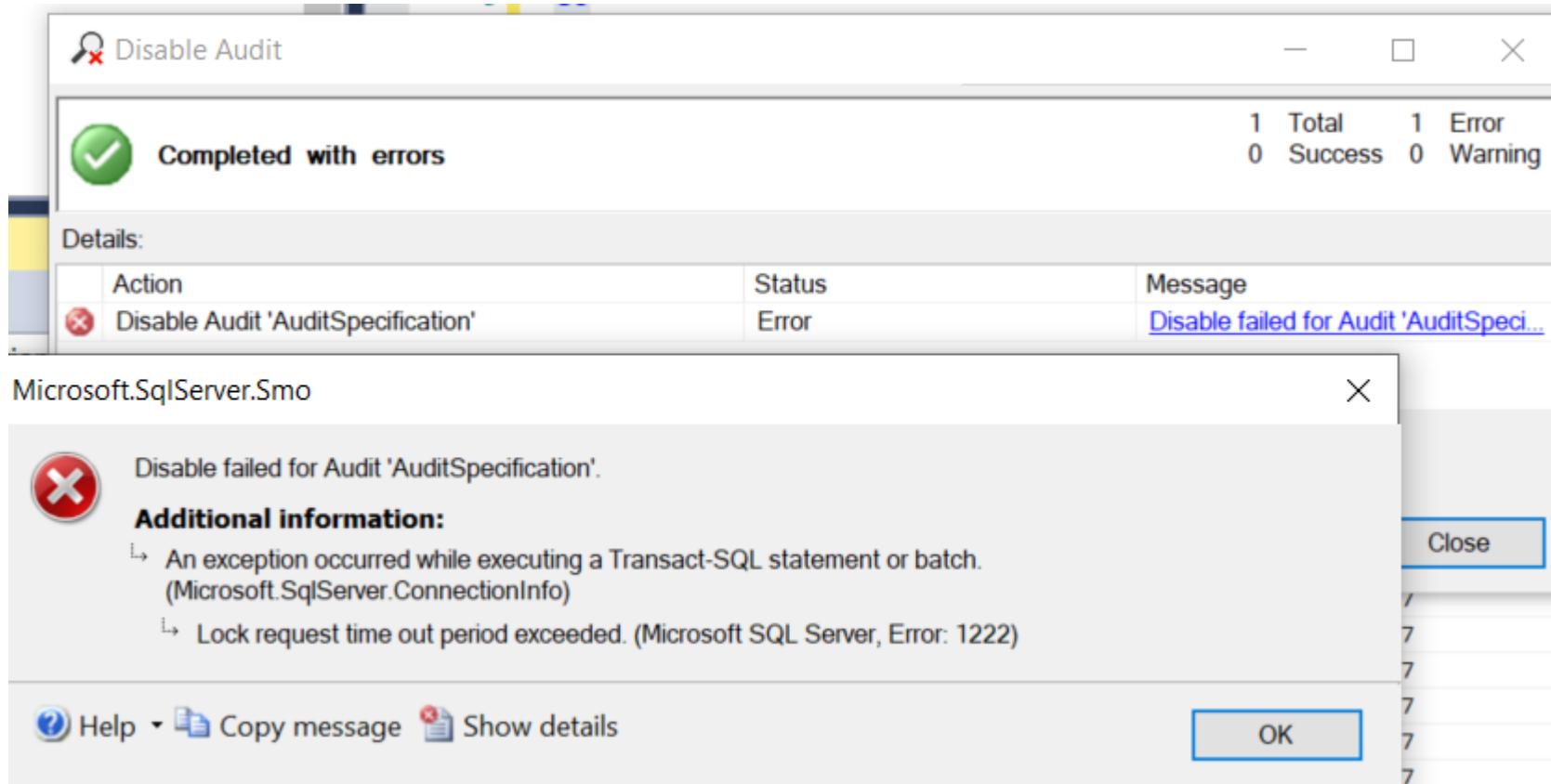
USE master;
ALTER SERVER AUDIT SPECIFICATION
[ServerAuditSpecification]
WITH (STATE = OFF);

USE Auditing;
ALTER DATABASE AUDIT SPECIFICATION
[DatabaseAuditSpecification-auditing]
WITH (STATE = OFF);
```



STOPPING AUDIT FAILURE

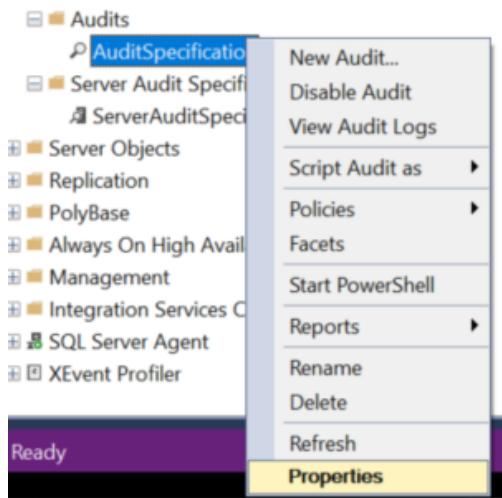
If you have long running queries preventing stopping audit



MODIFYING AUDITS

Two ways to change audits

GUI



Script

```
1 USE [master]
2 GO
3 ALTER SERVER AUDIT [AuditSpecification]
4 TO FILE
5   (MAXSIZE = 100 MB)
6 GO
```

) %

Messages

Msg 33071, Level 16, State 1, Line 3
This command requires audit to be disabled. Disable the audit and rerun this command.



SQL SERVER AUDITING VIA GUI SUMMARY



You need two things to make this work:

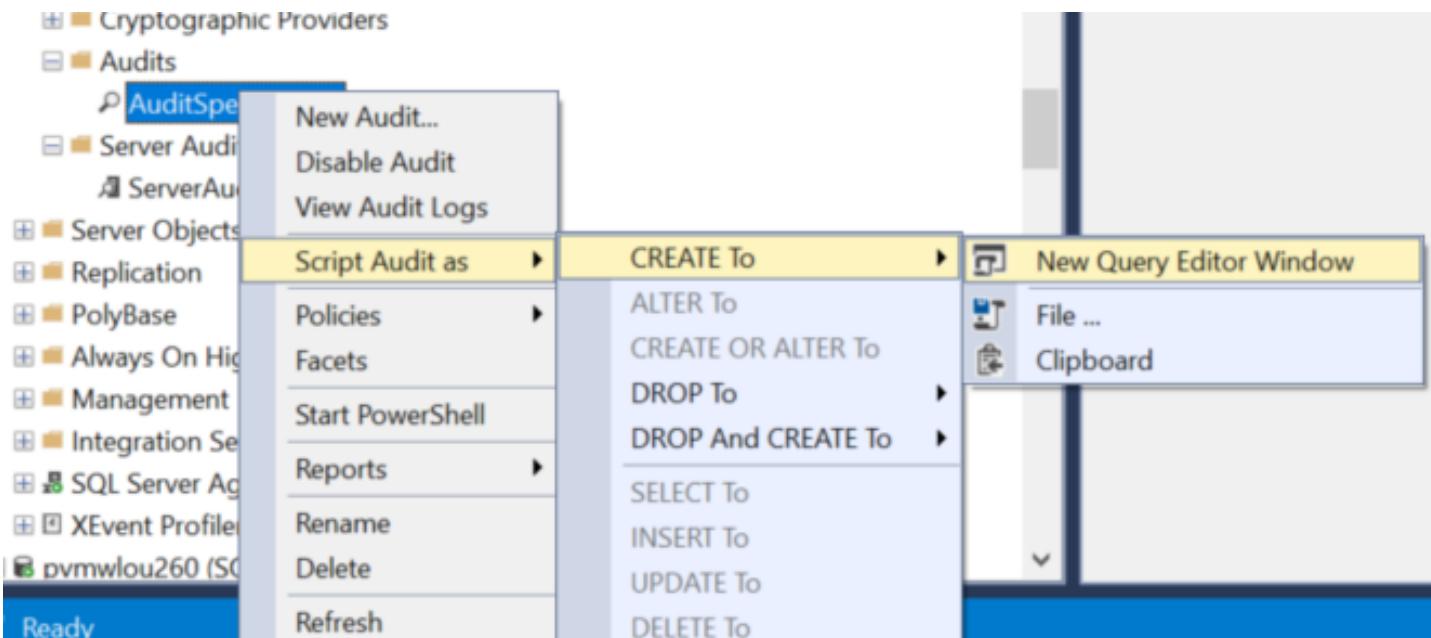
One audit specification (required)

And one of these things:

1. A server audit specification
2. A database audit specification

SCRIPT OUT AUDITS

Scripting out audits



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)
```



FILTERING SQL SERVER AUDIT

Filtering so you don't wind up with SQL Server built-in accounts or the account you use for monitoring filling up the audit data using WHERE clause

```
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)
WHERE (server_principal_name <> 'monitoringserviceaccount'  

AND server_principal_name <> 'builtinsqlserveraccount'  

AND schema_name <> 'sys')
ALTER SERVER AUDIT [AuditSpecification] WITH (STATE = ON)
GO
```



QUERYING AUDIT VIA GUI

The screenshot illustrates the process of querying audit logs via the SQL Server Management Studio (SSMS) graphical user interface.

Left Panel (Audit Context Menu):

- Audits
- AuditSp
- Server Audit
- Server Audit Policies
- Server Objects
- Replication
- PolyBase
- Always On History

The "AuditSp" item is currently selected, opening a context menu:

- New Audit...
- Disable Audit
- View Audit Logs** (highlighted in yellow)
- Script Audit as
- Policies
- Facets

Right Panel (Log File Viewer):

Title Bar: Log File Viewer - localhost, 1438

Selectlogs:

- Audit Collection
- AuditSpecification

Status:

- Last Refresh: 2/17/2021 3:52:11 PM
- Filter: None
- [View filter settings](#)

Progress:

- Done (1000 records).

Log file summary: No filter applied

Date	Event Time	Server Instance Name	Action ID
2/17/2021 10:05:39 PM	22:05:39.1609474	f1e384ca8e38	AUDIT SESSION CHANGED
2/17/2021 10:05:39 PM	22:05:39.1568155	f1e384ca8e38	AUDIT SESSION CHANGED
2/17/2021 10:05:39 PM	22:05:39.1068008	f1e384ca8e38	ALTER
2/17/2021 10:05:28 PM	22:05:28.3435811	f1e384ca8e38	SELECT
2/17/2021 10:05:28 PM	22:05:28.3435811	f1e384ca8e38	SELECT
2/17/2021 10:05:28 PM	22:05:28.3435811	f1e384ca8e38	SELECT
2/17/2021 10:05:28 PM	22:05:28.3435811	f1e384ca8e38	SELECT
2/17/2021 10:04:56 PM	22:04:56.1744390	f1e384ca8e38	ALTER
2/17/2021 10:04:51 PM	22:04:51.8110921	f1e384ca8e38	ALTER
2/17/2021 10:04:48 PM	22:04:48.8949143	f1e384ca8e38	SELECT
2/17/2021 10:04:48 PM	22:04:48.8949143	f1e384ca8e38	SELECT
2/17/2021 10:04:48 PM	22:04:48.8949143	f1e384ca8e38	SELECT
2/17/2021 10:04:48 PM	22:04:48.8949143	f1e384ca8e38	SELECT
2/17/2021 10:04:26 PM	22:04:26.5922084	f1e384ca8e38	VIEW SERVER STATE
2/17/2021 10:04:26 PM	22:04:26.5839081	f1e384ca8e38	VIEW SERVER STATE
2/17/2021 10:04:26 PM	22:04:26.5839081	f1e384ca8e38	VIEW SERIVED STATE

Selected row details:

Date	2/17/2021 10:05:39 PM
Log	Audit Collection (AuditSpecification)
Event Time	22:05:39.1609474
Server Instance Name	f1e384ca8e38
Action ID	AUDIT SESSION CHANGED
Class Type	SERVER AUDIT
Sequence Number	1
Succeeded	True
Permission Bit Mask	0x00000000000000000000000000000000
Column Permission	False
Session ID	56
Server Principal ID	1

Buttons: Load Log, Export, Refresh, Filter ..., Search ..., Stop, Help, Close

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_principal_name
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



SQL AUDITING SCRIPTS SUMMARY



Everything you can do in the GUI
you can do via scripts

Easier to create on multiple
servers

Easier to filter audit results with a
query

SQL SERVER AUDITING DEMO



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



SPECIFIC USE CASES

What I want to capture	Extended events	SQL Server audit
Audit everything a user does	X	
Audit all the perms and schema changes		X
Audit who's changing a table		X
Audit everything happening in a specific database (be careful with this on busy databases)	X	



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>

Querying SQL Server Audit file

<https://docs.microsoft.com/en-us/sql/relational-databases/system-functions/sys-fn-get-audit-file-transact-sql?view=sql-server-ver15>

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>

SQL Server Audit Server Actions

<https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions?view=sql-server-ver15#database-level-audit-action-groups>

SQL Server Audit Database Actions

<https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions?view=sql-server-ver15>

Extended events overview

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



GROUPBY 2021 | OCT 26-27

Thank you for attending!

Twitter: @hellosqlkitty

Blog: sqlkitty.com

Email: hellosqlkitty@gmail.com