



# **HOW TO AUDIT SQL SERVER FOR FREE**

# ABOUT ME

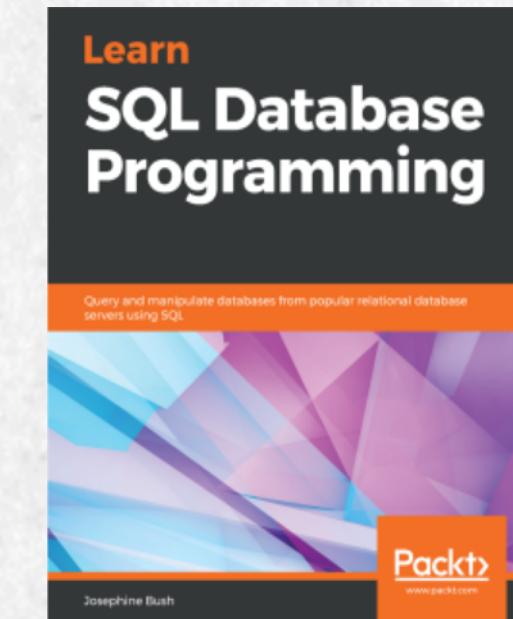
**Josephine Bush**

20+ years IT experience

Experienced DBA

MBA IT Management

MS Data Analytics



@hellosqlkitty  
sqlkitty.com

# AGENDA

---

Why use auditing?

Problems you can solve

Types and tools you can use

Centralized querying

Reporting

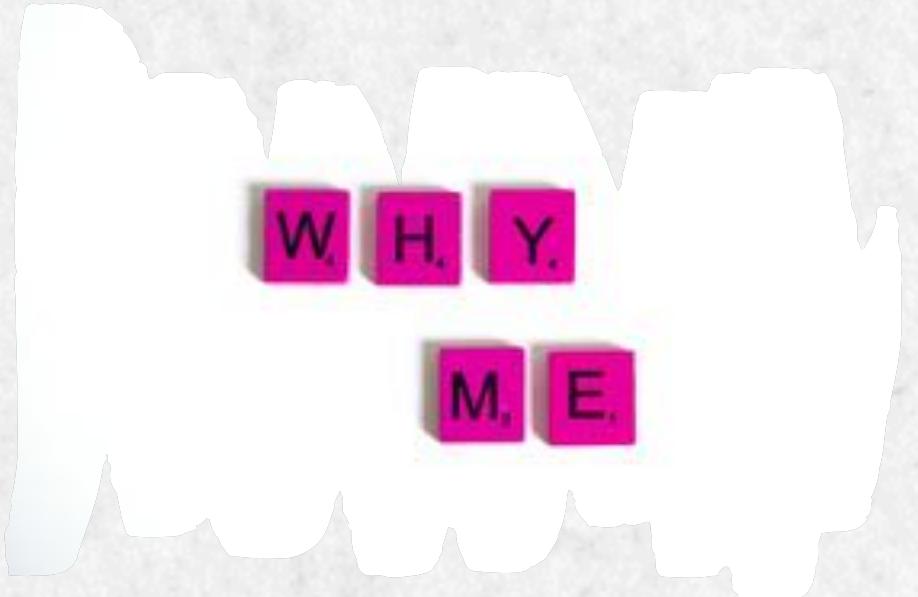
Cloud auditing



# 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!



# AUDITING REVIEW



Collecting and examining information to determine proper use or misuse

Helps you know what's happening on the database server

Helps you report who made what changes



## HOW TO AUDIT SQL SERVER

---

SQL Server audit  
is built-in auditing  
functionality  
available via SSMS

# 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

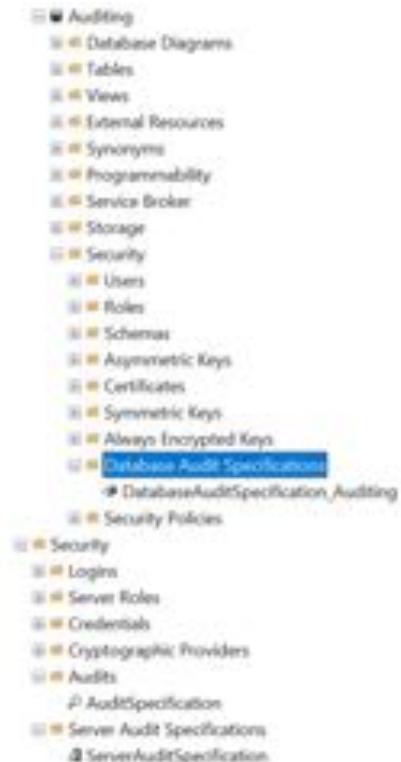
# SQL SERVER AUDIT REQUIREMENTS

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



# SQL SERVER AUDIT USE CASES

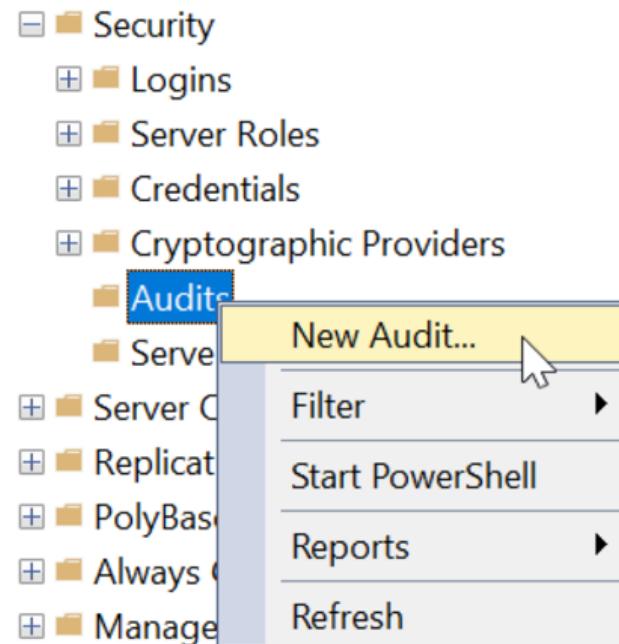
A server audit specification is good for auditing server level and/or all databases at the same time

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



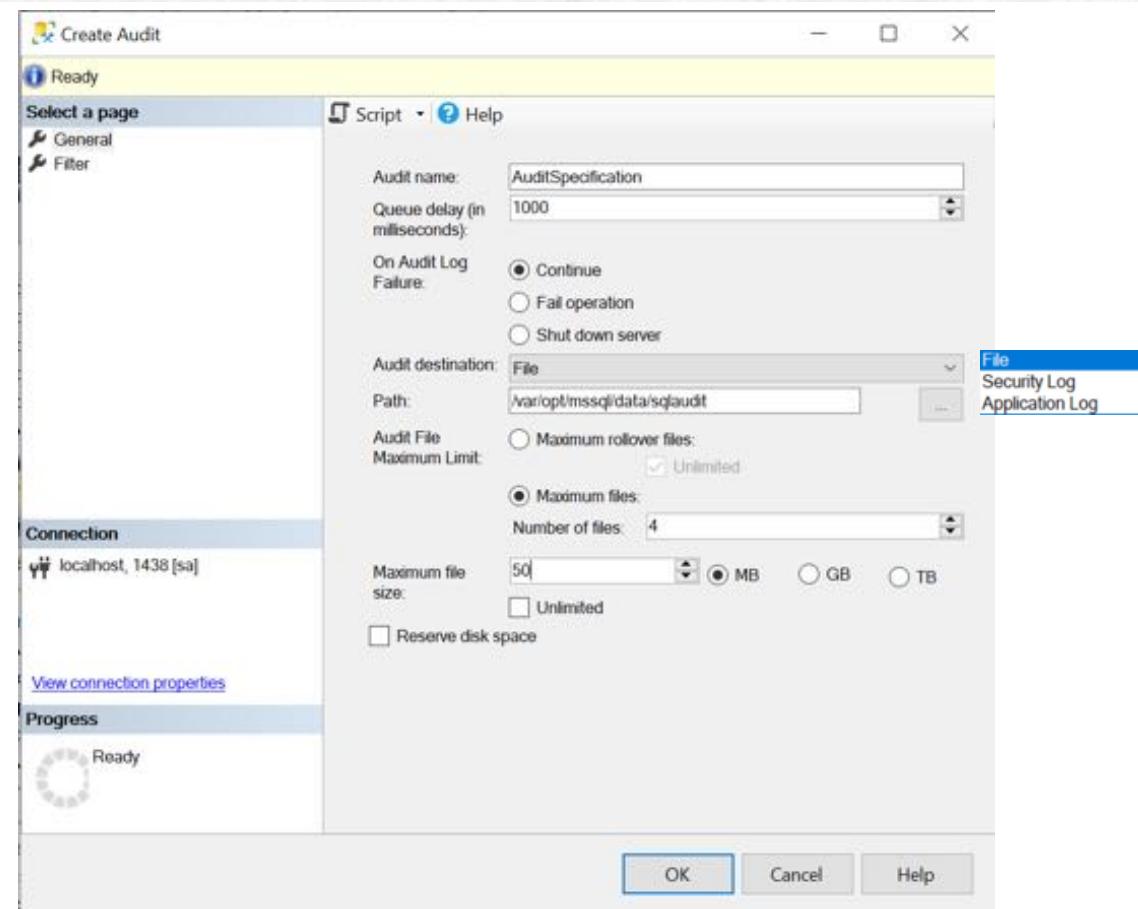
# CREATE AUDIT VIA GUI

Creating an audit specification in SSMS



# CONFIGURE AUDIT VIA GUI

Configuring an audit specification



# ENABLING AUDIT VIA GUI

Audit specifications are disabled after creation by default



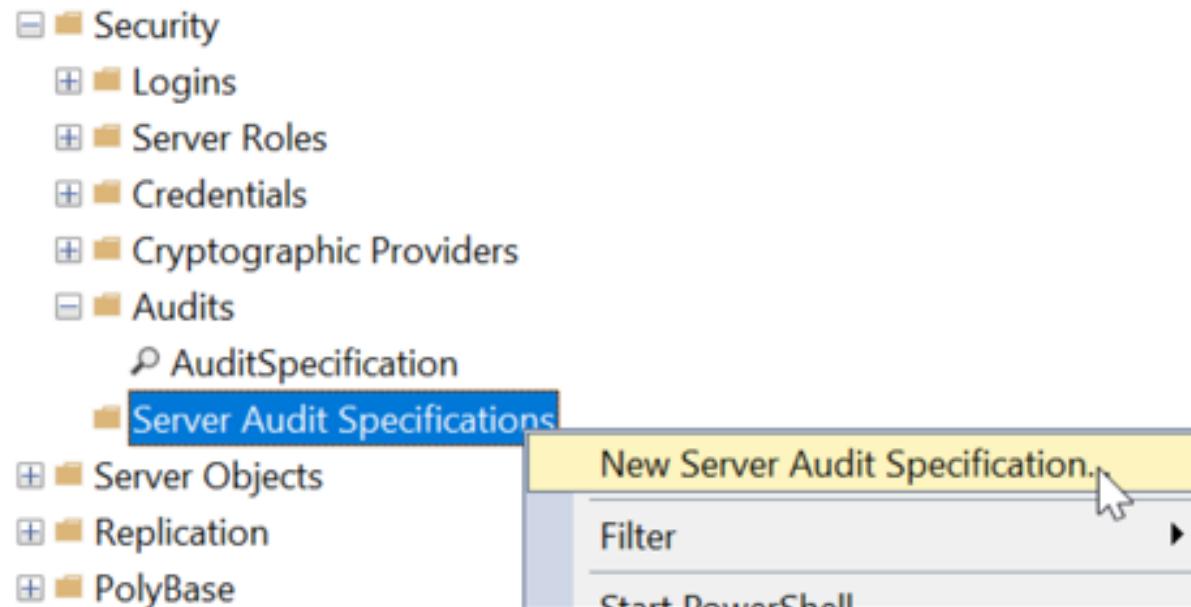
# AUDIT FILES ON DISK

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

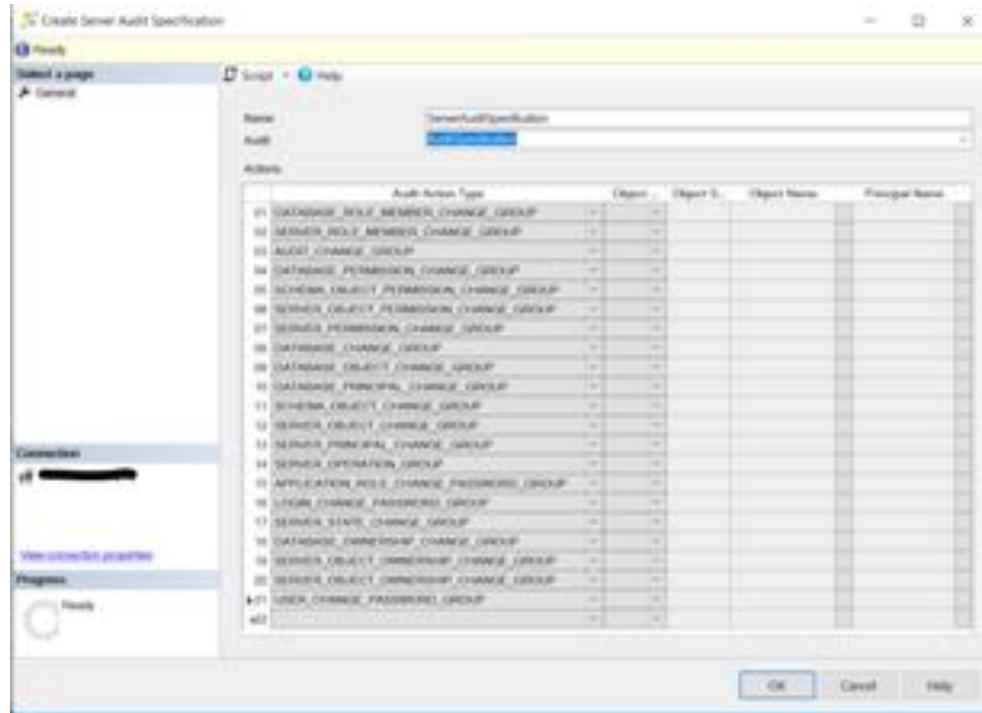
# CREATE SERVER AUDIT VIA GUI

Creating a server audit specification in SSMS



# CONFIGURE SERVER AUDIT VIA GUI

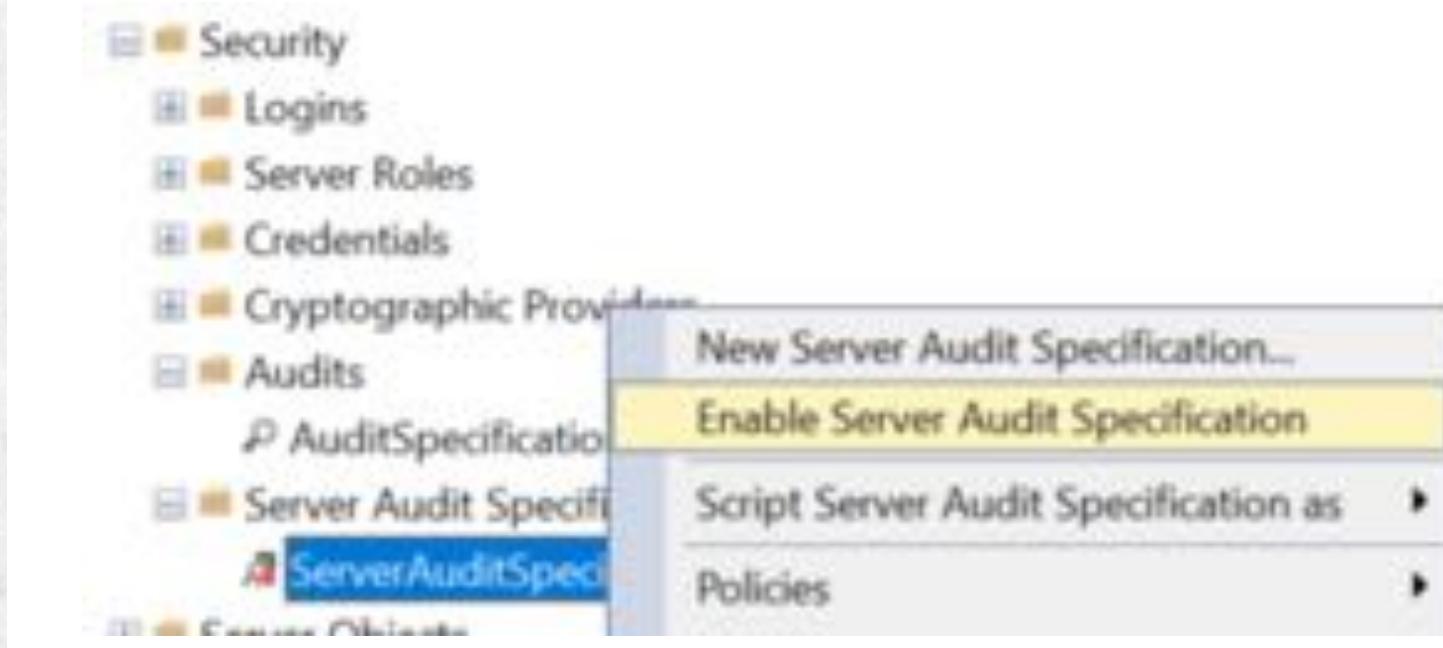
Configuring a server audit specification via SSMS



Audit Action Type	
01	DATABASE_ROLE_MEMBER_CHANGE_GROUP
02	MEMBER_ROLE_MEMBER_CHANGE_GROUP
03	AUDIT_CHANGE_GROUP
04	DATABASE_PERMISSION_CHANGE_GROUP
05	SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP
06	SERVER_OBJECT_PERMISSION_CHANGE_GROUP
07	SERVER_PERMISSION_CHANGE_GROUP
08	DATABASE_CHANGE_GROUP
09	DATABASE_OBJECT_CHANGE_GROUP
10	DATABASE_PRINCIPAL_CHANGE_GROUP
11	SCHEMA_OBJECT_CHANGE_GROUP
12	SERVER_OBJECT_CHANGE_GROUP
13	SCHEMA_PRINCIPAL_CHANGE_GROUP
14	SERVER_OPERATION_GROUP
15	APPLICATION_ROLE_CHANGE_PASSWORD_GROUP
16	LOGIN_CHANGE_PASSWORD_GROUP
17	SERVER_STATE_CHANGE_GROUP
18	DATABASE_OWNERSHIP_CHANGE_GROUP
19	SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP
20	SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP
21	USER_CHANGE_PASSWORD_GROUP
422	

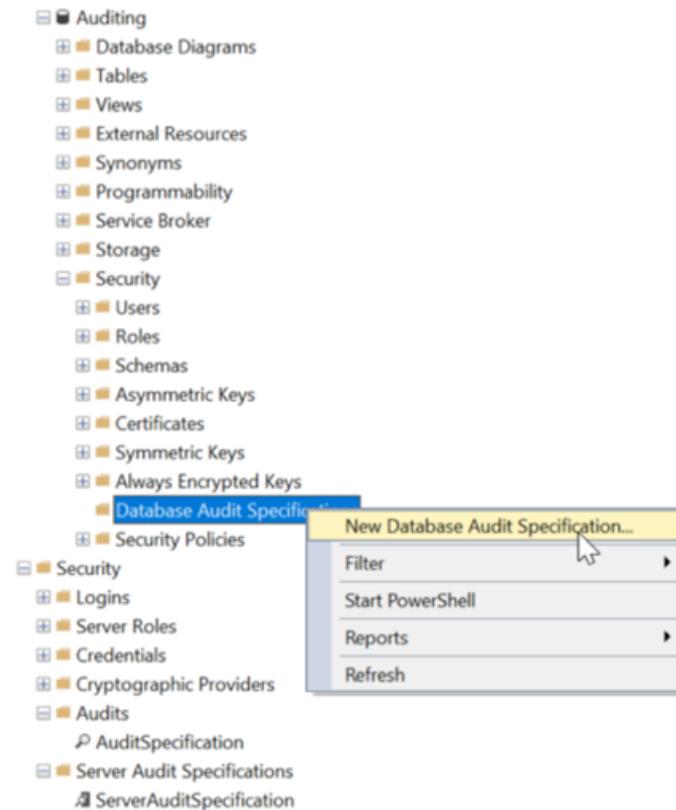
# ENABLING SERVER AUDIT VIA GUI

Server audit specifications are disabled after creation by default



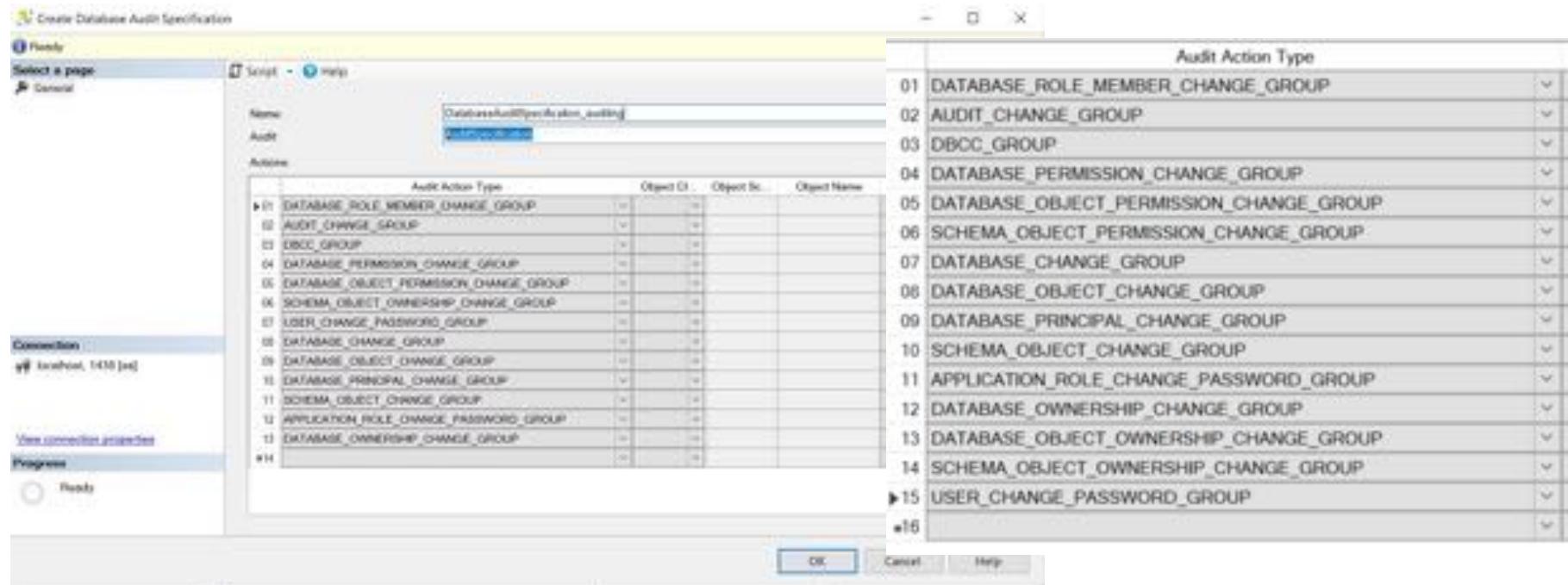
# CREATE DATABASE AUDIT VIA GUI

Creating a database audit specification via SSMS

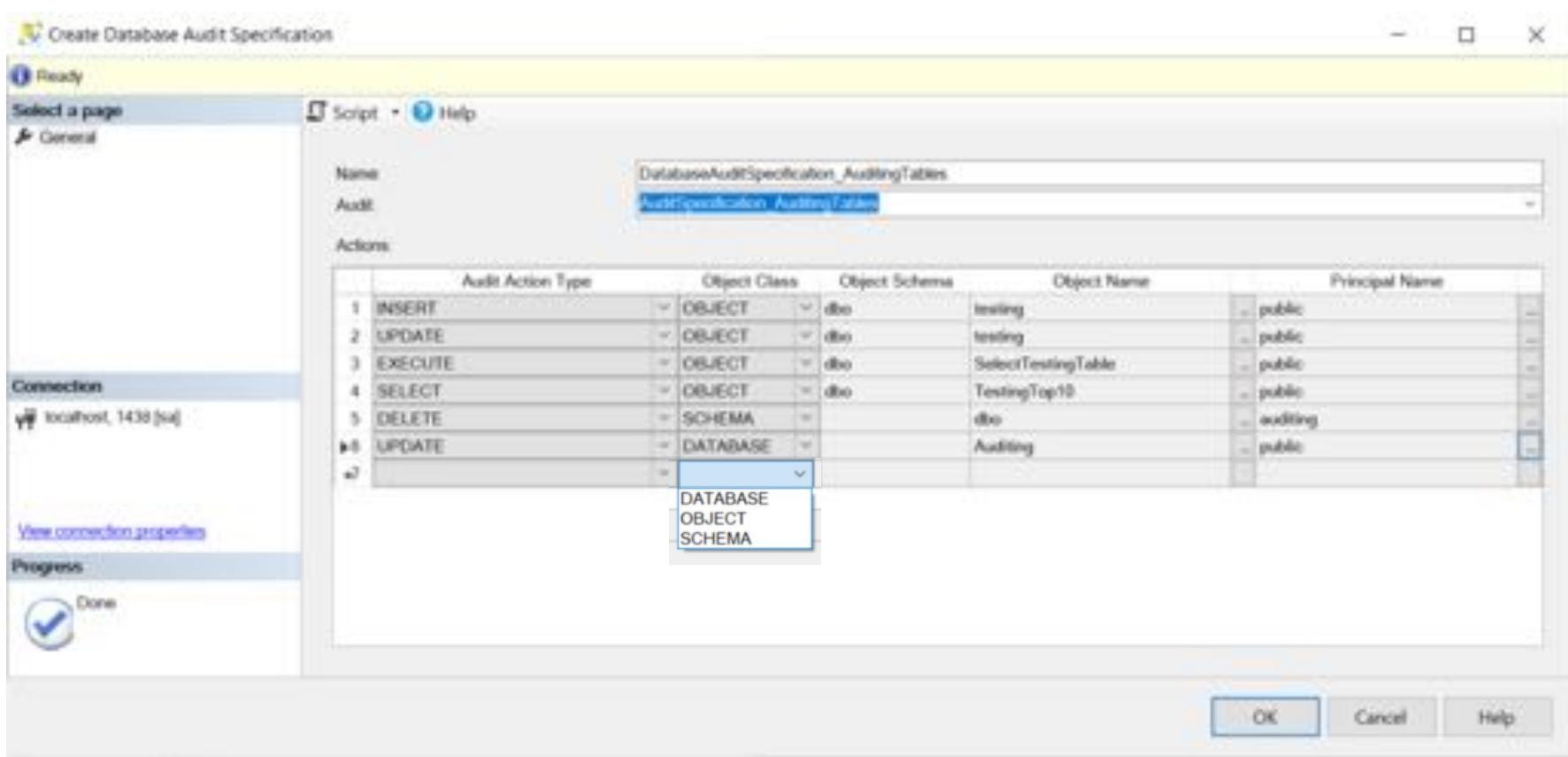


# CONFIGURE DATABASE AUDIT VIA GUI

Configuring a database audit specification via SSMS

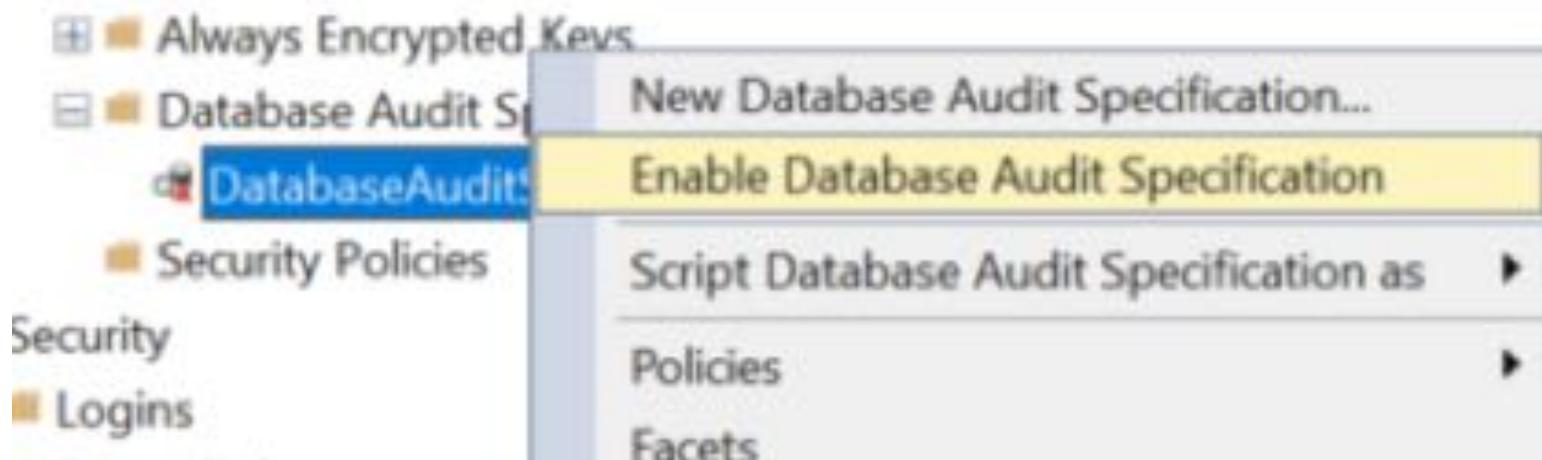


# SQL SERVER AUDIT OBJECTS VIA GUI



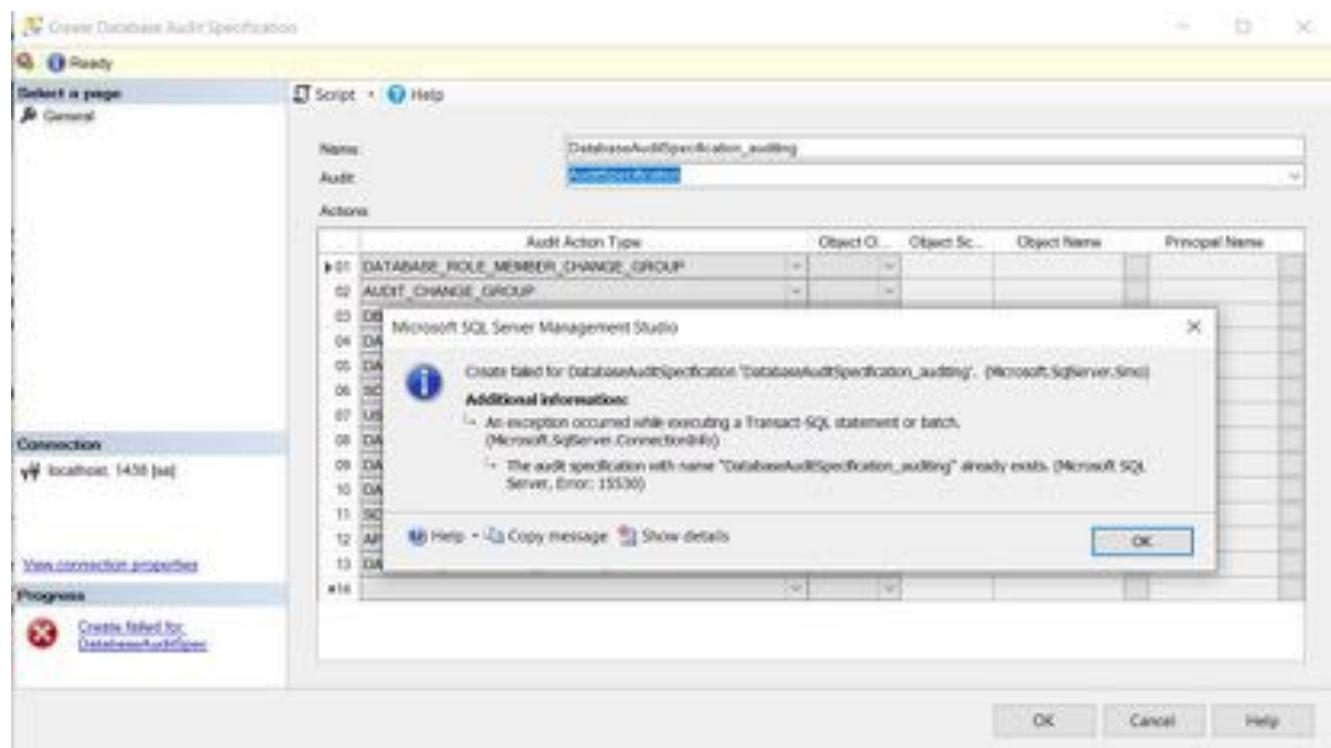
# ENABLING DATABASE AUDIT VIA GUI

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	
Audit everyone changing a table	Audit_tblChanges		DatabaseAudit_tblChanges with insert, update, delete on the table

# AUDITS IN GUI

Audits seen in relation to each other



# QUERYING AUDIT VIA GUI

The screenshot shows the Log File Viewer interface on a Windows system. On the left, a navigation pane lists various audit-related options under 'Audits'. The 'AuditSpec' item is selected, and a context menu is open, with 'View Audit Logs' highlighted in yellow. The main pane displays a table of audit logs. The table has columns for Date, Event Time, Server Instance Name, and Action ID. The logs show several events from 2021-05-21, mostly related to 'Audit Collection' changes and SELECT operations. A detailed view of one log entry is shown on the right, including fields like Date, Log, Event Time, Server Instance Name, Action ID, Class Type, Sequence Number, Succeeded, and Permission Bit Mask.

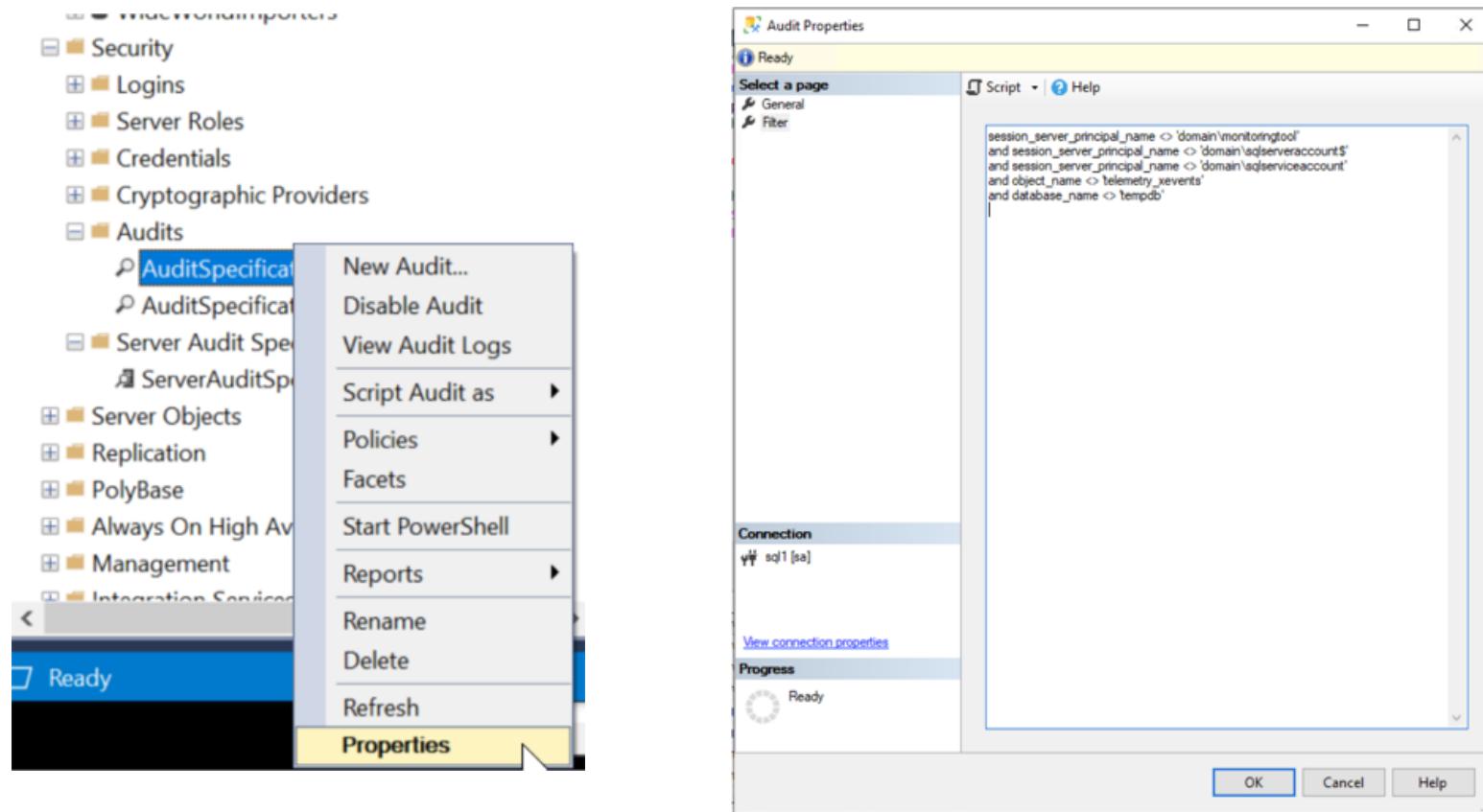
Date	Event Time	Server Instance Name	Action ID
21/5/2021	10:05:39 PM	Tts384code30	AUDIT SESSION CHANGED
21/5/2021	10:05:39 PM	Tts384code30	AUDIT SESSION CHANGED
21/5/2021	10:05:39 PM	Tts384code30	ALTER
21/5/2021	10:05:39 PM	Tts384code30	SELECT
21/5/2021	10:05:39 PM	Tts384code30	SELECT
21/5/2021	10:05:39 PM	Tts384code30	SELECT
21/5/2021	10:05:39 PM	Tts384code30	SELECT
21/5/2021	10:05:39 PM	Tts384code30	ALTER
21/5/2021	10:04:51 PM	Tts384code30	ALTER
21/5/2021	10:04:49 PM	Tts384code30	SELECT
21/5/2021	10:04:49 PM	Tts384code30	SELECT
21/5/2021	10:04:49 PM	Tts384code30	SELECT
21/5/2021	10:04:49 PM	Tts384code30	SELECT
21/5/2021	10:04:49 PM	Tts384code30	VIEW SERVER STATE
21/5/2021	10:04:49 PM	Tts384code30	VIEW SERVER STATE

# 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

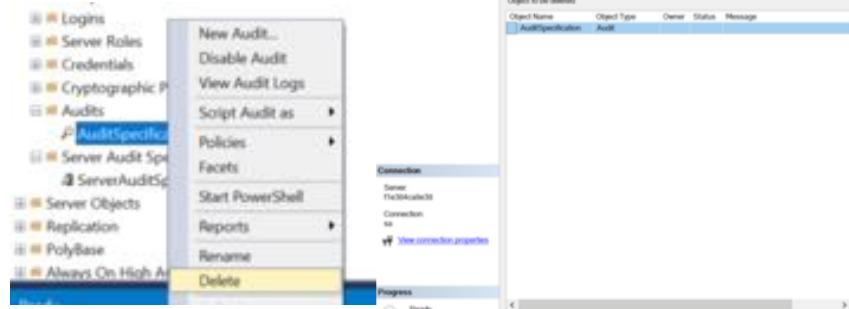
# FILTERING AUDITS WITH GUI



# DELETING AUDITS

Two ways to delete audits

GUI



Script

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

The screenshot shows the SSMS Object Explorer Details pane. It displays a T-SQL script named 'SQLQuery12.sql' with the following content:

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

In the 'Messages' pane, there is an error message: 'Msg 32071, Level 16, State 1, Line 5 This command requires audit to be disabled. Disable the audit and rerun this command.'

# STOPPING AUDITS

Two ways to stop audits

GUI



Script

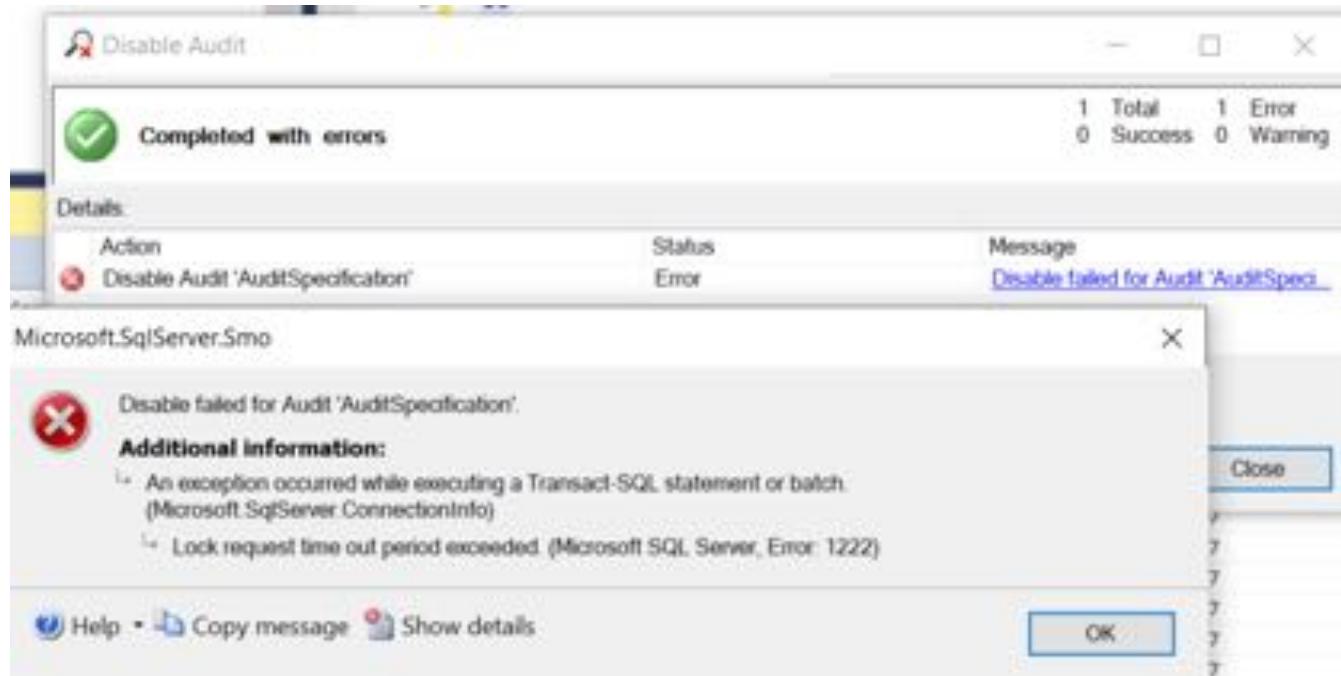
```
USE master;
ALTER SERVER AUDIT AuditSpecification
WITH (STATE = OFF);
```

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

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

# STOPPING AUDIT FAILURE

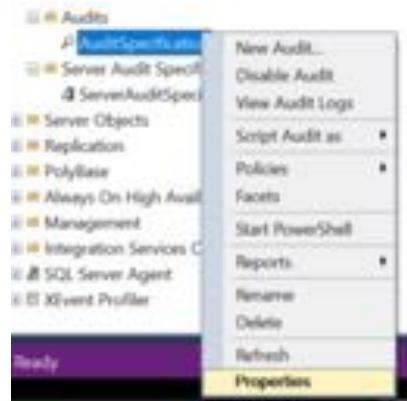
If you have long running queries preventing stopping audit



# 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 14, 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:

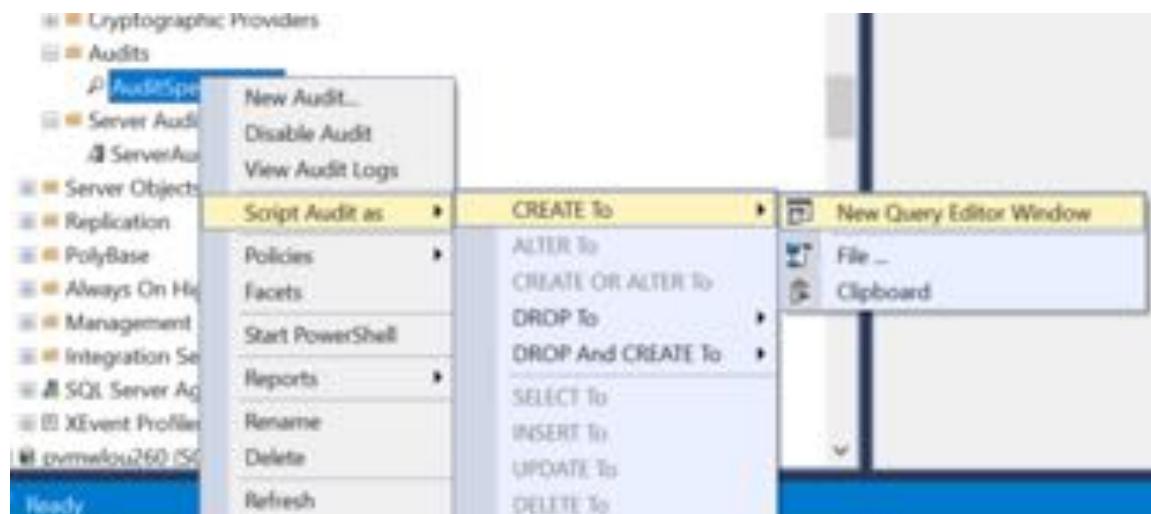
One audit specification (required)

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)
```

# SQL SERVER AUDIT OBJECTS VIA SCRIPT

```
USE [master]
CREATE SERVER AUDIT [AuditSpecification_AuditingTables]
TO FILE
(FILEPATH = N'E:\sqlaudit\'  

,MAXSIZE = 10 MB  

,MAX_FILES = 10  

,RESERVE_DISK_SPACE = OFF
) WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
ALTER SERVER AUDIT [AuditSpecification_AuditingTables] WITH (STATE = ON)
```

```
USE [Auditing]
CREATE DATABASE AUDIT SPECIFICATION [DatabaseAuditSpecification_AuditingTables]
FOR SERVER AUDIT [AuditSpecification_AuditingTables]
ADD (INSERT ON OBJECT::[dbo].[testing] BY [public]),
ADD (EXECUTE ON OBJECT::[dbo].[SelectTestingTable] BY [public]),
ADD (SELECT ON OBJECT::[dbo].[TestingTop10] BY [public]),
ADD (DELETE ON SCHEMA::[dbo] BY [auditing]),
ADD (UPDATE ON DATABASE::[Auditing] BY [public])
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 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/data/audit/*.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 [ServerAuditSpec]	1	ubuntusql1	master		sa
2021-03-10 00:14:43.2910458	ALTER	ALTER SERVER AUDIT SPECIFICATION [ServerAuditSpec]	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 [ServerAuditSpec]	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_databreader] ADD MEMBER [testing]	1	ubuntusql1	testing		sa
2021-03-10 00:12:47.7993722	CREATE	CREATE USER [testing] FOR LOGIN [testing] WITH DEF...	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

# DISCLAIMER ON AUDITING

Be very careful how and what you audit

**You can overload or freeze up a production server**

Less is more



# 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



# AUDIT DATA REPORTING

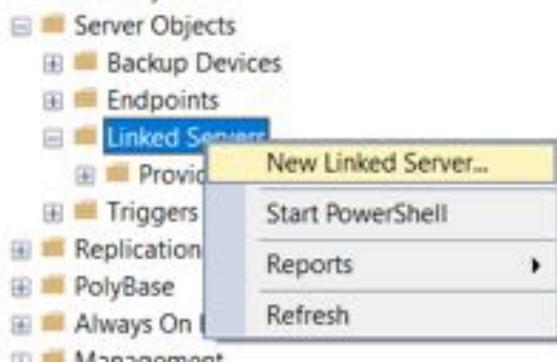


Centralized audit database for easy querying and reporting on multiple servers' audit data

# CENTRALIZING AUDITING DATA

## Using linked servers

Each audited server will link to a centralized database server



## Using SQL Server Agent

Each audited server will send data to a central database server via SQL Agent job

Agent job scheduled hourly or on an interval of your choosing

# REPORTING VIA AGENT JOB

Agent jobs on centralized server:

- Send an email with the daily auditing results in HTML format
- Auditing cleanup to keep only 30 days

You also need database mail configured on your centralized server



# SAMPLE AUDIT FINDINGS REPORT

## SQL Server Auditing Findings

Event Time	Partial Statement	Server	Database	Schema	Username	Successful
03/05/21 4:27:01 PM	ALTER SERVER ROLE [sysadmin] ADD MEMBER [domain\group]	Sql1	master		josephine	1
03/05/21 4:08:58 PM	CREATE LOGIN [domain\group] FROM	Sql1	master		josephine	1
03/05/21 2:06:43 PM	TRUNCATE TABLE [dbo].[tablename]	Sql2	userdb	dbo	appuser	0
03/05/21 1:27:00 PM	DROP DATABASE db	Sql3	master		sa	1
03/05/21 12:27:00 PM	ALTER VIEW [dbo].[tablename_view] AS SELECT	Sql4	userdb	dbo	anotherappuser	1

# CENTRALIZED AUDIT DATA SUMMARY



Centralized audit database for easy querying and reporting on multiple servers' audit data

Audited servers send data via agent jobs and linked servers to centralized server

Centralized server sends audit data via email daily or weekly depending on your reporting needs

# CLOUD SQL AUDITING OPTIONS

Cloud solution	SQL Server Audit Available	Auditing differences
Azure SQL	No	Server and database audits via Azure portal
Azure SQL Managed Instance	Yes	Need to use cloud storage
Amazon Web Services RDS	Yes	Need to use cloud storage
Google Cloud	No	Cloud audit logs via Google portal
VMs	Yes	Same with the ability to save to disk

# AZURE SQL AUDITING



Audit at server and database level via the portal

Use these to see queries run by users on Azure SQL

# SETUP AZURE SQL AUDITING

Enable auditing at the server level

Home > SQL databases > auditingtest (josephinebtest/auditingtest) > josephinebtest

josephinebtest | Auditing

SQL server

Search (Ctrl +/)

Save Discard Feedback

DTU quota

Properties

Locks

Security

Auditing

Firewalls and virtual networks

Private endpoint connections

Security Center

Transparent data encryption

Intelligent Performance

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  ON  OFF

Audit log destination (choose at least one):

Storage

Log Analytics (Preview)

Log Analytics details >

JBSQLAuditing

Event Hub (Preview)

# VIEW AZURE SQL AUDITING

View audit data at the database level

The screenshot shows the Azure portal interface for managing a database named 'auditingtest'. The left sidebar has sections for Settings, Integrations, Security, and Auditing (which is selected). The main area displays audit logs for the database.

**1** In the top navigation bar, there is a 'View audit logs' button highlighted with a red box.

**2** In the top right corner of the audit records page, there is a 'Log Analytics' button highlighted with a red box.

**3** In the bottom left of the audit records page, there is a 'New Query' button highlighted with a red box.

The audit records table shows the following data:

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

The 'Logs' blade on the left shows a query result:

```
1 AzureDiagnostics
2 | where Category == "SqlSecurityAuditEvents"
3 | where ResourceId == "/SUBSCRIPTIONS//RESOURCEGROUPS/SQLAUDITING/PROVIDERS/MICROSOFT.SQL/SERVERS/JOSEPHINETEST/DATABASES/MASTER" and database_name_s == "auditingtest"
4 | project event_time_t, statement_s, succeeded_s, affected_rows_d, server_principal_name_s, client_ip_s, application_name_s
5 | order by event_time_t desc
```

The 'Audit records' table at the bottom shows the following results:

event_time_t (UTC)	statement_s	succeeded_s	affected_rows_d	server_principal_name_s	client_ip_s	application_name_s
2/21/2021, 11:21:36.019 PM	ALTER TABLE dbo.testing SET (LOCK_ESCALATION = TABLE)	true	0	josephine		
2/21/2021, 11:21:35.892 PM	CREATE TABLE dbo.testing ( testing_idchar(10) NULL ) ON [PRIMARY]	true	0	josephine		
2/21/2021, 11:21:35.941 PM		true	0	josephine		
2/21/2021, 11:21:35.894 PM	DECLARE @edition sysname; SET @edition = cast(SERVERPROPERTY...	true	4	josephine		

# CLOUD AUDITING SUMMARY



Each cloud provider has options for auditing database changes:  
AWS, Azure Managed Instance, and VMs in the cloud are most like SQL Server auditing  
Azure SQL has similar functionality in the portal  
Google cloud has auditing capabilities in their portal

# SQL SERVER AUDIT REVIEW

One audit specification (required)

And a server audit specification and/or  
a database audit specification

Setup and query via GUI or scripts

**Remember to not audit so much that  
you can't stop the audit or easily  
query the data. You can overload or  
freeze up a production server**



# 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>

## Linked servers

<https://docs.microsoft.com/en-us/sql/relational-databases/linked-servers/create-linked-servers-sql-server-database-engine?view=sql-server-ver15>

## SQL Agent jobs

<https://docs.microsoft.com/en-us/sql/ssms/agent/create-a-job?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>

## Azure SQL Auditing

<https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview>

## Database mail

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



Thank  
you!

# THANK YOU FOR ATTENDING

---

Contact me @hellosqlkitty  
or visit me at [sqlkitty.com](http://sqlkitty.com)

# **EXTRAS**

---

The following slides are extras to this presentation because time didn't allow the covering of these topics.

# SQL SERVER AUDITING A USER

```
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]='auditing' AND [schema_name]<>'sys')
ALTER SERVER AUDIT [Audit-AuditingUser] WITH (STATE = ON)
```

```
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)
```

# SQL SERVER AUDITING AGENT JOBS

Added to the database audit specification for MSDB

```
USE [msdb]
CREATE DATABASE AUDIT SPECIFICATION [DatabaseAuditSpecification_MSDB]
FOR SERVER AUDIT [AuditSpecification]
ADD (EXECUTE ON OBJECT::[dbo].[sp_add_jobstep] BY [public]),
ADD (EXECUTE ON OBJECT::[dbo].[sp_delete_jobstep] BY [public]),
ADD (DELETE ON OBJECT::[dbo].[sysjobs] BY [public]),
ADD (INSERT ON OBJECT::[dbo].[sysjobs] BY [public]),
ADD (UPDATE ON OBJECT::[dbo].[sysjobs] BY [public]),
ADD (EXECUTE ON OBJECT::[dbo].[sp_add_jobschedule] BY [public]),
ADD (EXECUTE ON OBJECT::[dbo].[sp_delete_jobschedule] BY [public]),
ADD (EXECUTE ON OBJECT::[dbo].[sp_add_job] BY [public]),
ADD (EXECUTE ON OBJECT::[dbo].[sp_update_job] BY [public]),
ADD (EXECUTE ON OBJECT::[dbo].[sp_delete_job] BY [public])
WITH (STATE = ON)
```

# SQL SERVER AUDITING SSIS

Added to the database audit specification for SSISDB

```
USE [SSISDB]
ALTER DATABASE AUDIT SPECIFICATION [DatabaseAuditSpecification_SSISDB]
FOR SERVER AUDIT [AuditSpecification]
ADD (DELETE ON OBJECT::[internal].[projects] BY [public]),
ADD (INSERT ON OBJECT::[internal].[projects] BY [public]),
ADD (UPDATE ON OBJECT::[internal].[projects] BY [public]),
ADD (DELETE ON OBJECT::[internal].[packages] BY [public]),
ADD (INSERT ON OBJECT::[internal].[packages] BY [public]),
ADD (UPDATE ON OBJECT::[internal].[packages] BY [public]),
ADD (DELETE ON OBJECT::[internal].[folders] BY [public]),
ADD (INSERT ON OBJECT::[internal].[folders] BY [public]),
ADD (UPDATE ON OBJECT::[internal].[folders] BY [public])
WITH (STATE = ON)
```

# SQL SERVER AUDIT LIST QUERY

```
/*this query gives you a listing of audit specifications*/
select sfa.audit_id, sfa.name, sfa.is_state_enabled, sfa.create_date, sfa.modify_date,
sfa.type_desc, sfa.queue_delay, sfa.max_file_size, sfa.max_rollover_files,
sfa.max_files, sfa.log_file_path, sfa.log_file_name
from sys.server_file_audits sfa

/*this query gives you a listing of server audit specifications with their corresponding audit specifications*/
select sfa.name, sas.name, sas.create_date, sas.modify_date, sas.is_state_enabled,
sasd.audit_action_name
from sys.server_file_audits sfa
left join sys.dm_server_audit_status dsas
on sfa.audit_id = dsas.audit_id
left join sys.server_audit_specifications sas
on sfa.audit_id = sas.server_specification_id
left join sys.server_audit_specification_details sasd
on sas.server_specification_id = sasd.server_specification_id

/*this query gives you a listing of database audit specifications with their corresponding audit specifications*/
select sfa.name, das.name, das.create_date, das.modify_date, das.is_state_enabled,
dasd.audit_action_name, dasd.class_desc
from sys.server_file_audits sfa
left join sys.database_audit_specifications das
on sfa.audit_guid = das.audit_guid
left join sys.database_audit_specification_details dasd
on das.database_specification_id = dasd.database_specification_id
```

# SQL SERVER AUDIT LIST QUERY RESULT

	audit_id	name	is_state_enabled	create_date	modify_date	type_desc	queue_delay	max_file_size	max_rollover_files	max_size	class_desc
1	65540	AuditSpecification	0	2021-02-12 23:14:58.880	2021-02-12 23:14:58.880	FILE	1000	500	2147483647	4	
2	65541	AuditSpecification_AuditingTables	1	2021-02-18 00:18:43.743	2021-02-18 00:18:43.743	FILE	1000	10	2147483647	10	
	name	name	create_date	modify_date	is_state_enabled	audit_action_name					
1	AuditSpecification	ServerAuditSpecification	2021-02-12 23:19:27.403	2021-02-12 23:19:27.403	0	DATABASE_ROLE_MEMBER_CHANGE_GROUP					
2	AuditSpecification	ServerAuditSpecification	2021-02-12 23:19:27.403	2021-02-12 23:19:27.403	0	SERVER_ROLE_MEMBER_CHANGE_GROUP					
3	AuditSpecification	ServerAuditSpecification	2021-02-12 23:19:27.403	2021-02-12 23:19:27.403	0	AUDIT_CHANGE_GROUP					
4	AuditSpecification	ServerAuditSpecification	2021-02-12 23:19:27.403	2021-02-12 23:19:27.403	0	DATABASE_PERMISSION_CHANGE_GROUP					
5	AuditSpecification	ServerAuditSpecification	2021-02-12 23:19:27.403	2021-02-12 23:19:27.403	0	SCHEMA_OBJECT_PERMISSION_CHANGE_G					
6	AuditSpecification	ServerAuditSpecification	2021-02-12 23:19:27.403	2021-02-12 23:19:27.403	0	SERVER_OBJECT_PERMISSION_CHANGE_G					
7	AuditSpecification	ServerAuditSpecification	2021-02-12 23:19:27.403	2021-02-12 23:19:27.403	0	SERVER_PERMISSION_CHANGE_GROUP					
8	AuditSpecification	ServerAuditSpecification	2021-02-12 23:19:27.403	2021-02-12 23:19:27.403	0	DATABASE_CHANGE_GROUP					
	name	name	create_date	modify_date	is_state_enabled	audit_action_name					
10	AuditSpecification	DatabaseAuditSpecification-auditing	2021-02-13 00:04:50.897	2021-02-13 00:04:50.897	1	SCHEMA_OBJECT_CHANGE_GROUP					
11	AuditSpecification	DatabaseAuditSpecification-auditing	2021-02-13 00:04:50.897	2021-02-13 00:04:50.897	1	APPLICATION_ROLE_CHANGE_PASSWORD_G					
12	AuditSpecification	DatabaseAuditSpecification-auditing	2021-02-13 00:04:50.897	2021-02-13 00:04:50.897	1	DATABASE_OWNERSHIP_CHANGE_GROUP					
13	AuditSpecification	DatabaseAuditSpecification-auditing	2021-02-13 00:04:50.897	2021-02-13 00:04:50.897	1	DATABASE_OBJECT_OWNERSHIP_CHANGE_G					
14	AuditSpecification	DatabaseAuditSpecification-auditing	2021-02-13 00:04:50.897	2021-02-13 00:04:50.897	1	SCHEMA_OBJECT_OWNERSHIP_CHANGE_G					
15	AuditSpecification	DatabaseAuditSpecification-auditing	2021-02-13 00:04:50.897	2021-02-13 00:04:50.897	1	USER_CHANGE_PASSWORD_GROUP					