MS SQL server audit

If the SQL server is to be audited via LOGmanager, SQL server auditing must be set up using either SQL Server Management Studio or SQL Transact.

SQL Server auditing feature includes three main components:

- Server Audit
- Server Audit Specification
- Database Audit Specification

Server auditing determines how and where events are logged. Server auditing must be configured in each case.

You must also configure the Server Audit Specification or the Database Audit Specification, or both of them.

The Server Audit Specification will log general server events and more general events from all databases, such as server shutdowns or user logins.

The Database Audit specification will record events associated with a specific database and there is the option to define more detailed audited actions, e.g., audit INSERT, DELETE, etc.

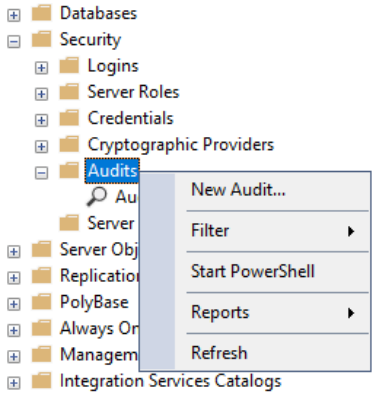
For smaller database environments, it will probably be sufficient to define a Server Audit Specification. On the other hand, for larger environments, it may be possible to define auditing only for specific actions and on important databases, thus saving system resources.

More detailed information is available at:
https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-database-engine?view=sql-server-ver15

Server Audit

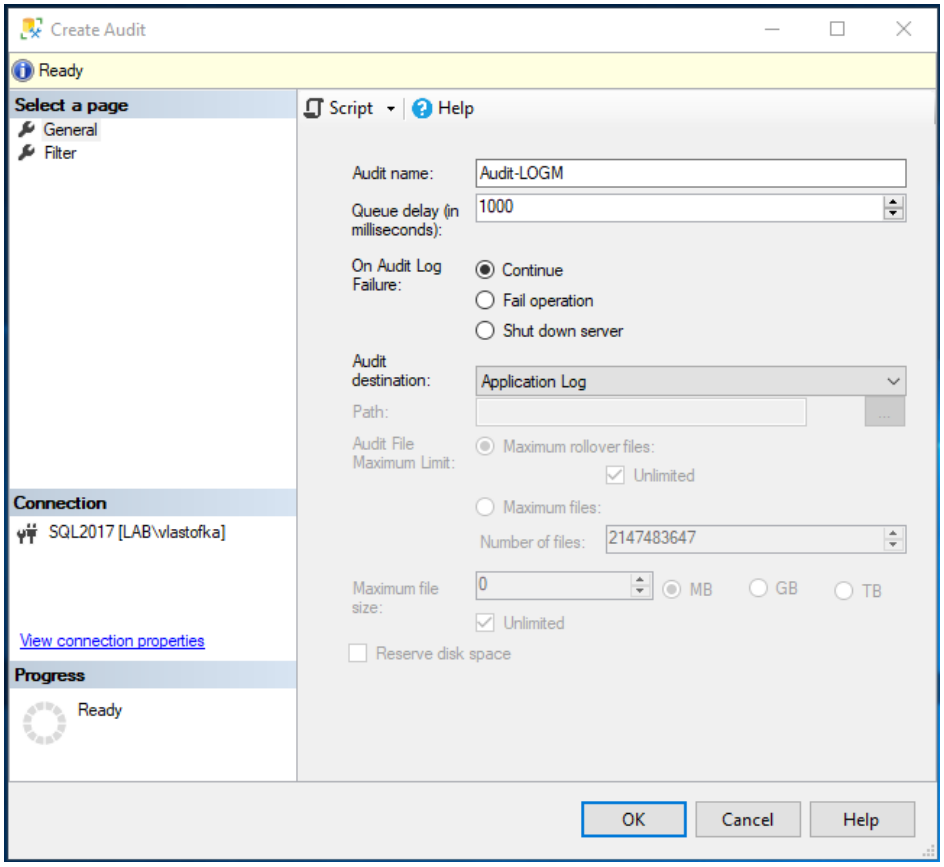
Server auditing is an overriding part of SQL Server auditing and can include server auditing specifications and/or database auditing specifications.
You can create a server audit either by using SQL Server Management Studio or by using Transact SQL.
When you configure SQL Server Management Studio, Server Audit is located in the master database. It is used to define the target where the audit information will be stored.

A new server audit can be created by right-clicking on the Security/Audits folder and selecting New Audit.

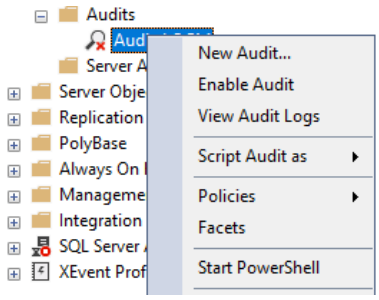


In the server audit configuration, you must set the audit name, for example, Audit-LOGM, and switch the audit destination to Application Log.

Events from the Application Log are automatically sent to LOGmanager using the Windows Event Sender agent (WES) or the Beats agent.



The new server audit is disabled by default and must be enabled by right-clicking and selecting Enable Audit.



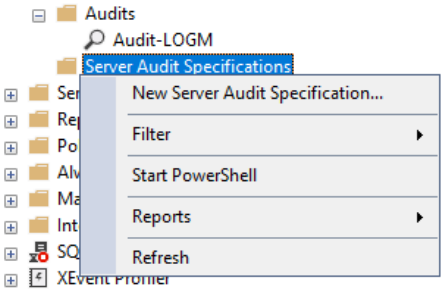
The audit can also be set and enabled using transact SQL:

```
USE [master]
GO
CREATE SERVER AUDIT [Audit-LOGM]
TO APPLICATION_LOG
WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
ALTER SERVER AUDIT [Audit-LOGM] WITH (STATE = ON)
GO
```

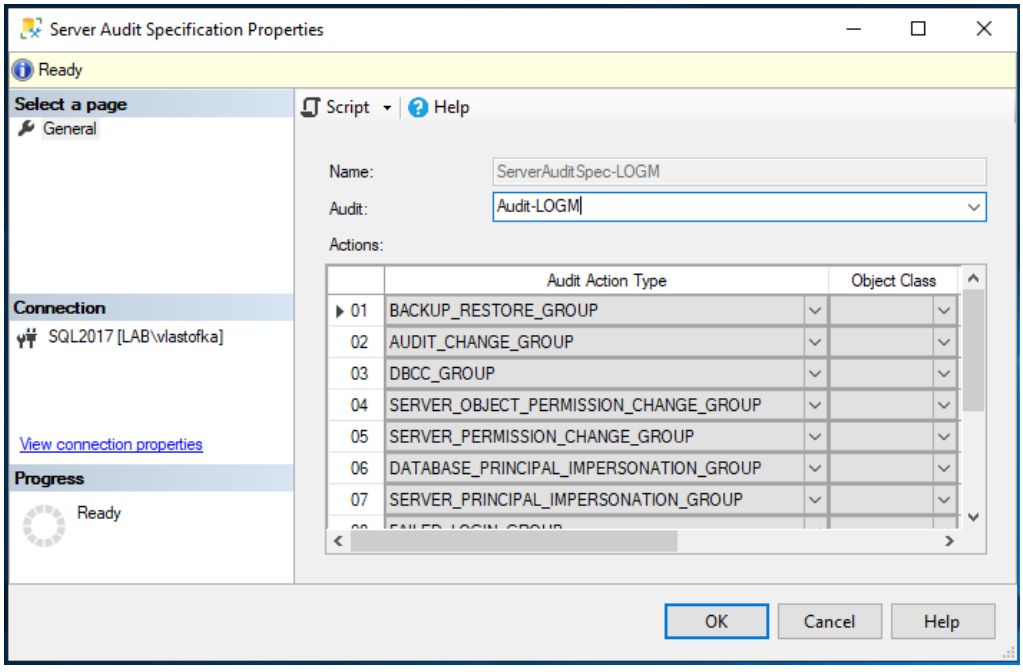
Server Audit Specification

When you configure SQL Server Management Studio, the Server Audit Specification is located in the master database.

It is used to define what needs to be audited at the server level. You can create a new server audit specification by right-clicking on the Security/Server Audit Specifications folder and selecting New Server Audit Specification...



In the Server Audit Specification configuration, you must set the name of the new specification, such as ServerAuditSpec-LOGM, and select the name of the Server Audit that was configured in the previous step. Next, you need to select the types of audit actions (Actions) that should be audited. The list of set actions will vary according to the specific needs of the user and a full list of options is available here: https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions?view=sql-server-ver15



Recommended audit actions:

`SUCCESSFUL_LOGIN_GROUP` - The user has successfully logged in to SQL Server

`FAILED_LOGIN_GROUP` - Failed attempt to log in to SQL Server

`LOGOUT_GROUP` - User logged out of SQL Server

`AUDIT_CHANGE_GROUP` - Audit creation, modification or deletion of an audit specification

`BACKUP_RESTORE_GROUP` - Backup or restore from backup audit

`DBCC_GROUP` - Audit of Microsoft SQL Server Database Console Commands (DBCC)

`SERVER_OPERATION_GROUP` - Audit of security changes (e.g., external access or authorization)

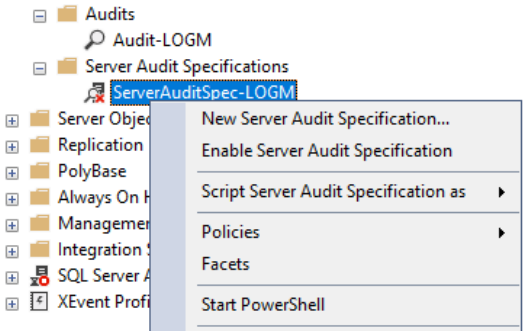
`SERVER_STATE_CHANGE_GROUP` - Auditing SQL Server state changes (starting or stopping)

`SERVER_PRINCIPAL_IMPERSONATION_GROUP` - Audit of the impersonation of credentials within the server

`DATABASE_PRINCIPAL_IMPERSONATION_GROUP` – Audit of impersonations within the database

`SERVER_PERMISSION_CHANGE_GROUP` - Audit of changes to GRANT, REVOKE, or DENY permissions within the server

The new Server Audit Specification is disabled by default and must be enabled by right-clicking and selecting Enable Server Audit Specification...



The server audit specification can also be set and enabled using transact SQL:

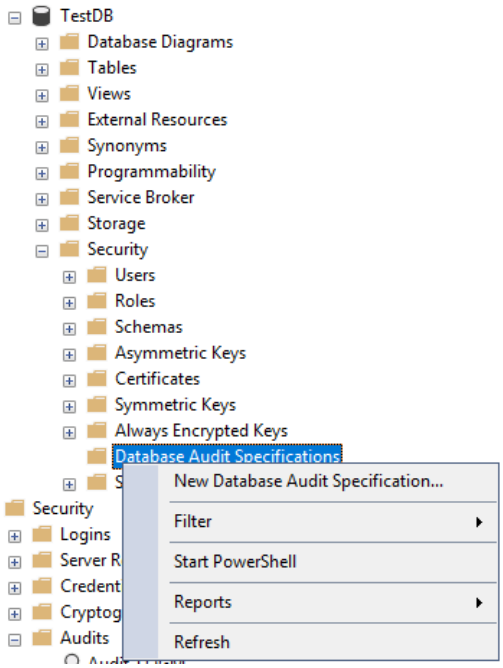
```
USE [master]
GO

CREATE SERVER AUDIT SPECIFICATION [ServerAuditSpec-LOGM]
FOR SERVER AUDIT [Audit-LOGM]
ADD (BACKUP_RESTORE_GROUP),
ADD (AUDIT_CHANGE_GROUP),
ADD (DBCC_GROUP),
ADD (SERVER_PERMISSION_CHANGE_GROUP),
ADD (DATABASE_PRINCIPAL_IMPERSONATION_GROUP),
ADD (SERVER_PRINCIPAL_IMPERSONATION_GROUP),
ADD (FAILED_LOGIN_GROUP),
ADD (SUCCESSFUL_LOGIN_GROUP),
```

```
ADD (LOGOUT_GROUP),
ADD (SERVER_OPERATION_GROUP),
ADD (SERVER_STATE_CHANGE_GROUP)
WITH (STATE = ON)
GO
```

Database Audit Specification

The Database Audit specification checks for database-level events and is configured similarly to the Server Audit specification.
The main difference is that the Database Audit Specification needs to be configured for each database separately by right-clicking on the NameDB/Security/Database Audit Specifications folder and selecting New Database Audit Specification...



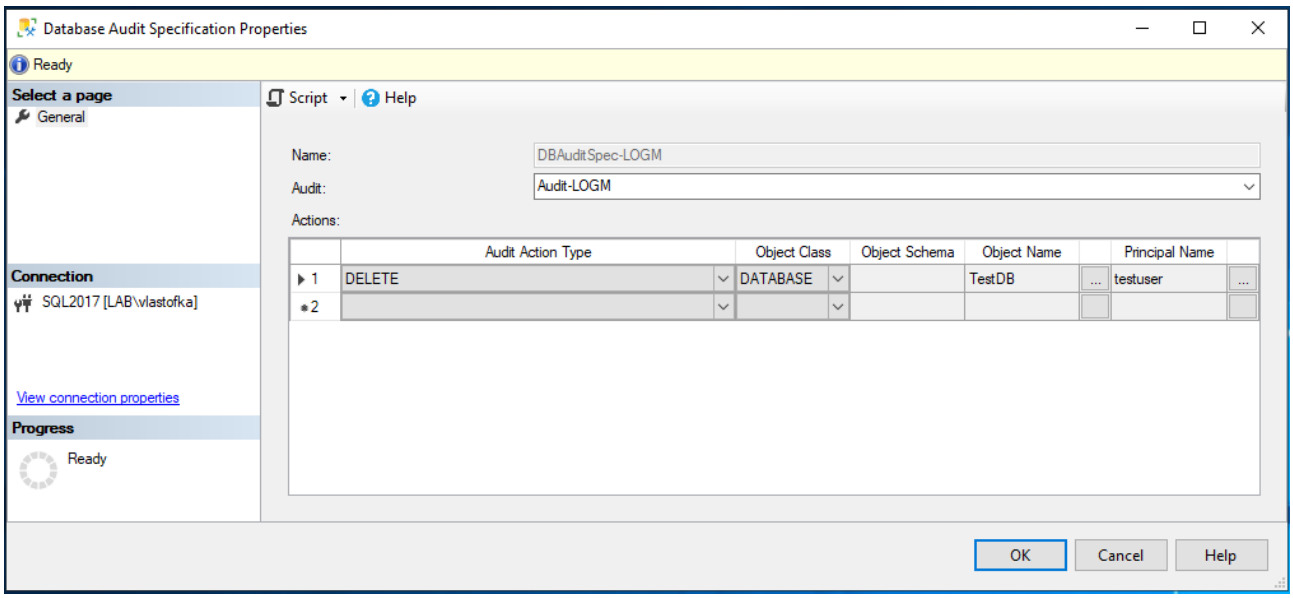
In the Database Audit Specification configuration, you must set the name of the new specification, such as DBAuditSpec-LOGM, and select the name of the Server Audit that was configured in the first step (Audit-LOGM).

Next, you need to select the types of audit actions (Actions) that should be audited.

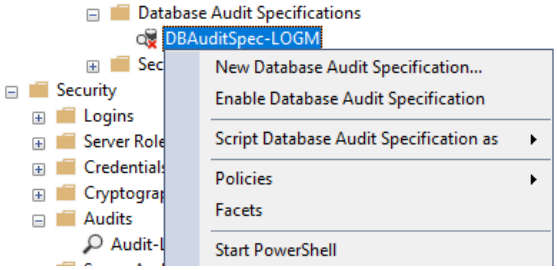
The list of set actions will vary according to the specific needs of the user and a full list of options is available here:

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

In the case of the Database Audit Specification, there is no recommended setting because each environment will require different auditing actions.



The new Database Audit Specification is disabled by default and needs to be enabled by right-clicking and selecting Enable Database Audit Specification...



Database auditing specifications can also be set and enabled using transact SQL:

```
USE [TestDB]
GO

CREATE DATABASE AUDIT SPECIFICATION [DBAuditSpec-LOGM]
FOR SERVER AUDIT [Audit-LOGM]
ADD (DELETE ON DATABASE::[TestDB] BY [testuser])
WITH (STATE = ON)
GO
```