Audit SQL Server Events

Auditing your SQL Server instances and databases is the first step in ensuring your SQL Server environment remains in continuous compliance with federal and corporate security and privacy policies. You can also generate reports on the audit data you collect, allowing you to demonstrate compliance on demand. For more information, see Report on Audit Data.

Auditing checklist

Use the following checklist to help you prepare your environment to successfully audit your SQL Server instances and databases. ***If you plan to audit virtual SQL Servers running in Microsoft failover clusters***, see Audit a virtual SQL Server instance for detailed installation and configuration tasks.

1. Gather the information necessary to set up your auditing.

✓	Task	Description	For more information ...
✓	Verify privileges on your Windows login account	Ensure that your Windows login account has sysadmin privileges on all SQL Server instances you want to audit.	Permissions requirements
✓	Review the list of auditable events	Review how the audit process works and which SQL events you can audit. Note that you can audit events at the server or database level.	How auditing works
✓	Identify the items you want to audit on your SQL Server instances	Identify the audit settings you want to apply to individual **instances** in your SQL Server environment. These settings should specify which server events you want to collect and report. Remember that the more data you collect, the more overhead is required. SQL Compliance Manager allows you to change your auditing settings at any time to help you make sure you collect exactly what an auditor needs.	Server-level audit settings
✓	Identify the items you want to audit on your databases	Identify the audit settings you want to apply to individual **databases** in your SQL Server environment. These settings should specify which database events you want to collect and report. Remember that the more data you collect, the more overhead is required. SQL Compliance Manager allows you to change your auditing settings at any time to help you make sure you collect exactly what an auditor needs.	Database-level audit settings
✓	Identify excluded events	Identify any events you want to exclude from your audit data.	Event Filters

2. Register your SQL Server instances.

✓	Task	Description	For more information ...
✓	Register your SQL Server instances	Register each SQL Server instance that hosts the databases you want to audit.	Register your SQL Servers

3. Enable auditing.

✓	Task	Description	For more information ...
✓	Enable server-level auditing	***If you want to audit your SQL Server instances***, enable auditing at the server level.	Enable auditing on a SQL Server
✓	Enable database-level auditing	***If you want to audit your databases***, enable auditing at the database level.	Enable auditing on a database

4. Apply regulation guidelines.

✓	Task	Description	For more information ...
✓	Apply regulation guidelines	Apply regulation guidelines to the appropriate audited databases.	Comply with specific regulations

5. Configure filters and test your settings.

	Task	Description	For more information ...
✓	Configure Event Filters	Configure the appropriate Event Filters, depending on which event category you want to exclude from your audit data.	Event Filters
✓	Test your audit settings	Test your audit settings to ensure you will collect the SQL Server events you need.	Test your audit settings

6. Monitor your settings.

	Task	Description	For more information ...
✓	Monitor event collection and adjust if necessary	Monitor how many events are collected on a daily basis. Depending on the growth rate of your audit data, consider creating Event Filters to better manage audit data in large environments.	Event Filters
✓	Monitor the Repository database growth	Monitor the growth of the SQL Compliance Manager Repository databases. ***If the databases are growing too fast***, change your auditing settings to limit growth and optimize performance.	Reduce audit data to optimize performance
✓	Determine whether you need alerts	Determine whether you need to alert on the events you are collecting. SQL Compliance Manager allows you to build rules that provide real-time alert notifications to help you quickly identify and resolve security issues.	Alert on Audit Data and Status
✓	Determine whether you need to capture before-and-after object values	***If you are auditing DML activity***, determine whether you want to capture the value of the database object before and after a specific transaction.	Audited Database Properties window - Before-After Data tab
✓	Determine who needs access rights to administer or report on audit data	Determine which SQL users should have access rights to administer or report on audit data. This security feature is important as both sensitive and audit data should be secure.	Secure Audit Data

7. Implement reports.

	Task	Description	For more information ...
✓	Review report implementation	Review how you can implement Reports in your SQL Server environment using SQL Server Reporting Services.	Report on Audit Data

8. Archive events.

	Task	Description	For more information ...
✓	Archive collected events	Configure how you want SQL Compliance Manager to archive audit data. Note that SQL Compliance Manager creates an archive database for each registered SQL Server instance.	Archive collected events