Fine tune your audit settings

SQL compliance manager provides a lot of flexibility for your audit settings, allowing you to collect a wide range of SQL Server events. However, extensive auditing requires sufficient disk space, processing time, and a very stable network connection. Your environment may not provide the resources necessary to audit every event that occurs on a particular SQL Server instance.

The following auditing options can be resource-intensive and cause significant growth in the Repository databases, thereby decreasing the performance of SQL compliance manager. For more information, see Reduce audit data to optimize performance.

Auditing System Administrators or sa login as a privileged user

Many SQL Server environments are not hardened around the sysadmin fixed role. Consequently, when you audit this role as a privileged user, you will likely collect a significant number of events initiated by benign applications simply because they have been designed to operate using a login in this role. ***If you want to continue auditing System Administrator activity***, consider defining Event Filters to exclude the benign operations you do not need to monitor.

Auditing the system databases for DML or SELECT activity

Gathering events directly from the system databases is only useful under very specific circumstances in an audited environment. Internal operations of SQL Server may be accidentally collected when you audit DML or SELECT events, causing unnecessary data to be collected and stored. ***If you want to continue auditing system databases***, consider archiving or grooming your event databases on a routine basis.

Auditing login events at the server level

Some third-party applications perform a login to the SQL Server instance before any individual operation is initiated. This can cause a very large number of login events to be collected for your audit data trail. ***If you have this type of activity in your environment***, consider specifying a privileged user status to those logins whose activity you need to collect. Note that auditing the Login Failed event category does not result in the same level of data and can remain enabled.