Fine tune your audit settings

IDERA SQL Compliance Manager provides 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 possibly are resource-intensive and can cause significant growth in the Repository databases, thereby decreasing SQL Compliance Manager performance. For more information about avoiding performance issues, 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 can collect a significant number of events initiated by benign applications simply because they are 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 useful only under very specific circumstances in an audited environment. Accidental collection of SQL Server internal operations can occur when you audit DML or SELECT events, resulting in the storage of unnecessary data. ***If you want to continue auditing system databases***, consider routinely archiving or grooming your event databases.

Auditing login events at the server level

Some third-party applications perform a login to the SQL Server instance before initiating any individual operation. This action can cause the collection of a large number of login events 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.

⚠ Auditing the Login Failed event category does not result in the collection of the same level of data. You can leave this action enabled.