How auditing works

IDERA SQL Compliance Manager audits each registered SQL Server instance and the associated databases according to the audit settings you configure. Your audit settings should directly correlate with the SQL events you need to track in order to meet your compliance objectives. For example, you can register a SQL Server instance for auditing but not audit the hosted databases. Likewise, you can audit a single database on a registered SQL Server instance that hosts multiple databases.

Complying with regulations

If you are subject to comply with regulations such as PCI DSS or HIPAA, you can use SQL Compliance Manager to configure your audit settings according to the specific guidelines of the regulation. SQL Compliance Manager then collects event data based on these guidelines and can provide a report that details the section of the regulation and the data collected using SQL Compliance Manager. You can apply the regulation guideline audit settings to one or more databases on a registered SQL Server instance. For more information, see Comply with specific regulations.

Understanding traces

On each registered SQL Server instance, the SQL Compliance Manager Agent starts a SQL Server trace to copy SQL event log entries, called audit events, to trace files. Trace files are temporary files that store audit events until these events can be sent to the Collection Server. Trace files are located in a trace file directory on the audited SQL Server computer. For more information, see How the SQL Compliance Manager Agent works.

SQL Compliance Manager collects all events in the SQL trace that are related to the activity you want to audit. When choosing the activities you want to audit, be aware that activities performed through the SQL Server client tools, such as Management Studio, may log multiple events. For example, when you add a login to a role, the SQL trace records one event for the add login action and another event for changing the default language. In this case, SQL Compliance Manager collects each event as separate audit data according to the SQL trace.

Using SQL Server Extended Events

IDERA SQL Compliance Manager 5.5 and later include support for event handling with SQL Server Extended Events. This optional feature is available for use in auditing instead of using SQL Trace. Running Extended Events offers a performance improvement over the default SQL Trace audit event gathering system and is available for instances running SQL Server 2012 and later. For more information about using the Extended Events option, see Using SQL Server Extended Events.

Using SQL Server Audit Logs

IDERA SQL Compliance Manager 5.5 and later include support for event handling with SQL Server Audit Logs. This optional feature is available for use in auditing as an alternative to using SQL Server Extended Events or SQL Trace. Auditing via Audit Logs offers the ability to track your alerts for Agents running SQL Server 2017 and later. For more information about using the Audit Logs option, see Using SQL Server Audit Logs.

Using the Collection Server

The Collection Server stores the compressed trace files in the CollectionServerTraceFiles folder until the files can be processed. This folder is located under the install directory (`C:\Program Files\Idera\SQLcompliance`) on the computer that hosts the Collection Server. The CollectionServerTraceFiles folder is also called a trace file directory, and is secured using ACL settings. You can specify a different location for the trace directory.

The Collection Server processes the raw audit events according to your settings and then sends the results to the appropriate event database in the Repository. The Collection Server creates an event database for each registered SQL Server instance. You can specify which audit events you want to track. You can also configure how the Collection Server and SQL Compliance Manager Agent manage the trace files.

Filtering and grooming data

For optimal data management, SQL Compliance Manager supports archiving and grooming of event data. Depending on the size of your environment, the amount of event data you audit, and your reporting cycles, you may want to archive and groom event data on a routine basis. For more information, see Manage Audit Data.

Understanding trusted and privileged users

Trusted users are SQL Server logins and members of SQL Server roles that you trust to read, update, or manage a particular audited database or an entire server. As these users are trusted, the events generated by accounts are removed by the SQL Compliance Manager Agent from the audit trail before sending the trace file to the Collection Server for processing.

By designating trusted users, you can more efficiently audit databases used by third-party applications, such as SAP, that are self-auditing. Self-auditing applications are able to audit activity and transactions initiated by their service accounts. Because service accounts can generate a significant number of login and database change events, omitting these expected events from your audit data trail lets you more easily identify unexpected activity.

When you designate trusted users, consider limiting your list to a few specific logins. This approach optimizes event processing performance and ensures you filter the intended accounts. Keep in mind that Server-level Trusted Users apply across all databases for that server, where the Database-level only applies to a particular database. For more information, see the Configuration wizard - Trusted Users window and the Registered SQL Server Properties window - Trusted User tab.

In comparison, privileged users are SQL Server logins and members of SQL Server roles that have certain privileges or authorization that you want to audit. You can audit individual SQL Server logins with privileged access as well as logins that belong to specific server roles. A sudden spike in privileged user activity could indicate a security breach. For more information about selecting privileged users for audit, see the Configuration wizard - Privileged Users window and the Registered SQL Server Properties window - Privileged User Auditing tab.

If you are auditing privileged user activity and the trusted user is also a privileged user, SQL Compliance Manager will continue to audit this user because of its elevated privileges. For example, a service account that is a member of the sysadmin fixed SQL Server role will continue to be audited even though the account is designated as trusted.

Understanding before and after data

Collect before and after data when it is critical to capture the exact data change in a table column. When this feature is enabled, you can evaluate the before value and after value for each change in the Audit Events view. Enabling this feature can impact your Collection Server and Management Console performance.

> It is important to note that the Before-After Data capture feature modifies the application schema by creating triggers on any table for which such data collection is enabled.