# Best Practices for Deployment of SQL Compliance Manager

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVERVIEW/PURPOSE</td>
<td>2</td>
</tr>
<tr>
<td>REQUIRED LEVEL OF AUDITING</td>
<td>2</td>
</tr>
<tr>
<td>SQL COMPLIANCE REPOSITORY SQL SETTINGS</td>
<td>2</td>
</tr>
<tr>
<td>CONFIGURATION SETTINGS</td>
<td>3</td>
</tr>
<tr>
<td><strong>CAPTURED DATA BASELINE/SQL STATEMENT STORED</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>ARCHIVE AND DATA RETENTION</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>REPORTING</strong></td>
<td>4</td>
</tr>
<tr>
<td><strong>LOGINS</strong></td>
<td>4</td>
</tr>
<tr>
<td><strong>BACKUP AND RECOVERY</strong></td>
<td>4</td>
</tr>
<tr>
<td>PRODUCTION IMPLEMENTATION</td>
<td>4</td>
</tr>
<tr>
<td><strong>ROLL-OUT</strong></td>
<td>4</td>
</tr>
<tr>
<td><strong>ALERTING</strong></td>
<td>4</td>
</tr>
<tr>
<td><strong>FILTERING</strong></td>
<td>5</td>
</tr>
<tr>
<td>CREATING AUDIT EVENT FILTERS</td>
<td>5</td>
</tr>
</tbody>
</table>
Overview/Purpose

This document deals with the best practices of implementation and deployment of Idera’s SQL Compliance Manager.

The information in this document is to be used as a reference. Since each production environment has its own challenges, it is best to evaluate each rollout in a realistic test environment before production launch.

Required Level of Auditing

It is important to balance what is required to be audited and the hardware resources available, or you may be inundated with data and it will be difficult to follow the audit trail:

- Determine the appropriate methodology of auditing. Compliance Manager can audit based on the instance, database, and table (for DML and Select activity). You can also limit the auditing to specific users on the privileged users tab.

- What are the auditing requirements for data collection? For instance do you need to collect all failed logins, security changes, DDL, DBCC, etc? In order to get a clear concise audit trail, it is recommended to limit the audit data collected to the minimal amount required for both external auditing and internal controls.

- It is also recommended to limit Select and DML auditing to specific tables. If appropriate audit stored procedures, indexes and views. Auditing system tables usually adds higher overhead and can make it more difficult to follow the audit trail due to collecting large amounts of data on SQL system specific transactions.

SQL Compliance Repository SQL Settings

To optimize the performance of the SQL Compliance Manager repository, it is recommended to modify some of the SQL server settings.

Tempdb Setting Guidelines

Autogrow File
25% Growth
200 MB Space Allocated
The above is a guideline and makes the archive process more efficient. In larger environments, it may be necessary to increase the TempDB size to 500 MB or more. By default, tempdb auto grows as needed while SQL Server is running. Unlike other databases, however, it is reset to its initial size each time the database engine is started. If the size defined for tempdb is small, part of your system processing load may be taken up with auto-growing tempdb to the size needed to support your workload each time to restart SQL Server.

**Model Database Setting Guidelines**

- Autogrow File
- 25% Growth
- Simple Mode (optional: switch to full mode in order to ensure redundancy)
- 200 MB Space Allocated

The above is a guideline and makes the creation of new databases more realistic in larger environments. In larger environments, it may be necessary to increase the ModelDB size to 500MB or more. This is critical as well because the model database is the template used by Microsoft® SQL Server™ when creating other databases, such as tempdb or user databases. When a database is created, the entire contents of the model database, including database options, are copied to the new database; the default size is .75MB which is typically too small.

**Configuration Settings**

To optimize compliance manager, it is imperative to adjust some of the configuration settings such as SQL statement stored, Archive and Retention, Reporting, Logins, and Backup/Recovery. Below are examples of how this is completed.

**Captured Data Baseline/SQL Statement Stored**

Once the auditing settings have been completed, collect data for 7 days to get a baseline of how much data will be collected for each database. Typically each event is approximately .5KB to 1.5 KB depending on the audit settings. An estimate to calculate storage requirements: 1 million events will roughly equal 1GB of data. If the SQL statements are selected to be captured, the default length of the statement stored is 512 characters, if this is increased this will increase the size of the data.

**Archive and Data Retention**

Based on the amount of data collected, determine the most appropriate interval to archive the data. It is recommended to perform archive actions during quiet times within your environment. Based on the requirements of the compliance officer or security officer, adjust the archive event period appropriately (monthly, quarterly, or annually).
Reporting
It is recommended to have reporting services installed on a separate server. Configure the users that will have read only rights to view the captured data.

Logins
Application permissions are available within SQL Compliance Manager. To provide the best security, grant view audit data permission to those users that should not be making configuration changes.

Backup and Recovery
Implement a backup schedule for the databases containing audit information. Using Idera’s SQL Safe Backup product, you can easily backup old archive databases and take them offline. This will assist with saving disk space as well as encrypting the data. For more information on backing up the events database please refer to the SQL Compliance Manager User Guide.

Production Implementation

Roll-Out
Since the auditing of SQL server is very environment specific and depending on the load on the SQL servers, transactions audited, and hardware configuration, it is recommended to perform a phased roll-out. The phased roll-out should start with installing the Compliance Manager repository and collection server on server hardware that is sufficient for the specific audit requirements. It is recommended to dedicate this server only to be the Compliance Manager server. Once compliance has been configured, it is advisable to register new audited SQL servers in groups of five and have compliance run and collect events and evaluate the load of the Compliance Manager server. Typically CPU, Memory, and Disk I/O are aspects of the SQL Compliance Manager Collection server that experience the most performance hit. Once you have determined that the server is not being taxed too heavily you can add another five instances to audit.

Alerting
SQL Compliance Manager can generate an alert when it finds a suspicious event in your audit data. Alert rules define what a suspicious event is and how SQL Compliance Manager should respond. For example, you can create a rule to alert on DML events that occur on a sensitive database. You can configure SQL Compliance Manager to write a custom alert message to the application event log and send an alert email notification to your corporate and personal SMTP accounts when the alert is triggered.
SQL Compliance Manager only alerts on the events you select for an audited SQL Server instance or database. After the Collection Server processes the raw event data sent by the SQL Compliance Agent, the Collection Server uses the criteria defined by your alert rules to search for suspicious events. When a matching event is found, the alert is triggered. If you specified a message for this alert, SQL Compliance Manager saves the alert message in the SQL Compliance repository database. You can view alert messages and the corresponding events using the Alerts view in the Management Console. Depending on the amount of alert activity your environment generates, you may want to groom alert messages on a routine basis.

Filtering
You can audit event filters to improve scalability, remove unwanted events from the audit data stream, and increase the granularity of your audit settings. Audit event filters determine which collected SQL events should be kept for processing by the Collection Server. Like your audit settings, the audit event filters should correlate with the SQL events you need to track in order to meet your compliance objectives. After receiving the trace files from the SQL Compliance Agent, the Collection Server applies your audit event filters. Any matching events are permanently deleted and eliminated from the data stream. All remaining events are processed for alerts and stored in the appropriate Repository database.

Creating Audit Event Filters
An audit event filter allows you to exclude specific events from being captured and stored in the repository. This approach helps you collect only the audit data you need. Audit event filters can also help performance by reducing the size of the Repository databases and the processing load on the Collection Server. Event filters are very easy to set up and configure. The filter creation uses a wizard which lets you be very granular in the configuration to ensure only required events are captured.