New features and fixed issues

IDERA SQL Compliance Manager provides the following new features and fixed issues.

> IDERA, Inc. customers are solely responsible for ensuring compliance with the laws and standards affecting their business. IDERA, Inc. does not represent that its products or services ensure that customer is in compliance with any law. It is the responsibility of the customer to obtain legal, accounting, or audit counsel as to the necessary business practices and actions to comply with such laws.

6.2 New Features

Quality Enhancements

Enhanced User Experience with Email and Summary Notifications

SQL Compliance Manager 6.2 improved to determine if an Alert Rule has been configured as 'Email Notification' or 'Email Summary Notification', users no longer are required to edit the alert rule. The rule description has been enhanced to make it convenient to distinguish between the two without the need for alert rule modifications.

Command Line Interface (CLI) Enhancement

SQL Compliance Manager 6.2 upgraded to provide a CLI command line for registering a server, grooming, archiving, and verifying audit data integrity - version 6.2 is now augmented with CLI for enabling and disabling auditing servers.

Reports

SQL Compliance Manager 6.2 improved and added the number of rows at the end of the reports to ease access to the information contained in each report.

Security Enhancements

Encryption

SQL Compliance Manager 6.2 enhanced security by deploying a strong Advanced Encryption Standard (AES) algorithm to meet the latest high standards of our large enterprise customers. The Advanced Encryption Standard (AES) is an algorithm that uses the same key to encrypt and decrypt protected data. Instead of a single round of encryption, data is put through several rounds of substitution, transposition, and mixing to make it harder to compromise.

6.2 Fixed Issues

- DDL, DML, and DROP events are correctly shown in the **"Audit Events"** tab after performing the DDL action on the **"Sensitive Column"** when using the **"via Audit Logs"** collection method.
- Audit events for **"insert"** are accurately being recorded for Sensitive columns with **"select and DML activity"** enabled.
- Resolved the issue where Trace events were not being correctly captured for **"delete from <table>"** audit events when sensitive columns with **"select and DML activity"** were configured.
- Fixed an issue where the number of Logout events captured was significantly more than the number of Login events.
- Resolved the issue where a warning message was displayed in the Event Viewer after execution of the trace file out to the collection Server for processing.
- Fixed an issue where the **"Delete"** DML events were shown twice after executing a single **"Delete"** query on the **"Sensitive Columns"** table when **"Trace"** or **"Audit Logs"** collection methods were used.
- Resolved the issue where the events table integrity check did not detect changes done on hash columns.
- The **“SQL Statement”** content is correctly displayed in the “Event Properties” after executing the DDL query if the “via SQL server Audit specification” is used.
- Resolved the issue where the **"+"** icon was missing for the DDL column-sensitive event in the **"Audit Events"** tab.
- Addressed an issue where the layout was broken for reports downloaded in PDF and TIF formats.
- Resolved an issue where Events were not captured as expected with Extended Events and SELECT auditing was enabled.
- Fixed the issue where the Bin file was not getting updated for the Privileged User set up through a domain group at the server level.
- Resolved an issue where **"Unknown Publisher"** was displayed in the **"User Account Control"** when installing SQLCM.

- Addressed an issue where an error message would come up when trying to import audit settings.

For more information about new features and fixed issues in version 6.1, see Previous new features and fixed issues.