New features and fixed issues

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

> Idera, Inc. customers have the sole responsibility to ensure their compliance with the laws and standards affecting their business. Idera, Inc. does not represent that its products or services ensures 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.

4.5 New features

Supports SQL Server 2014

SQL Compliance Manager supports the use of SQL Server 2014. Note that SQL CM requires the repository of the SQL Server version to be greater than or equal to the highest audited version, meaning that if you want to audit SQL Server 2012 and 2014 instances, your repository must be on SQL Server 2014 to support the highest version on your instances.

Supports Windows Server 2012 cluster deployment

This version of SQL CM allows you to install in a Windows Server 2012 clustered environment. For more information about this feature, see Deploy SQL CM in a Windows Server 2012 clustered environment.

Audit the local SQL Server instance running the Collection Server on a cluster

SQL Compliance Manager allows you to audit a virtual SQL Server instance including the local instance on a cluster running the Collection Server. For more information about auditing a virtual SQL Server instance, see Audit a virtual SQL Server instance.

Schedule automatic archives

SQL Compliance Manager now allows you to schedule automatic archiving. You can select from daily, weekly, or monthly options. This feature is disabled by default. You can enable this feature and manage these settings in the Archive Preferences window.

Specify archive database drive

When setting up archiving, you can specify the drive where you want SQL CM to store the archive database. You can manage this location in the Archive Preferences window.

Receive alerts through SNMP

Users now can select to receive alerts as SNMP Trap messages to a specified destination network management console. For more information about creating a new event rule to includes SNMP Traps, see New Event Alert Rule wizard - Alert Actions tab.

Before-After data values display NULL when there is no value

After collecting data, if there is no before or after data available, SQL CM displays "NULL" in the **Before Value** and **After Value** columns of the Event Properties window. For more information about Before-After data, see Audited Database Properties window - Before-After Data tab.

Supports PCI DSS v3

SQL CM now supports Payment Card Industry Data Security Standard (PCI DSS) v3.0.

Improved table compression

The data type is changed in a number of highly-utilized tables from NTEXT to VARCHAR in an attempt to improve data compression.

Improved installation process

The SQL Compliance Manager installer now checks the permissions on the trace directory and the Idera folders to ensure that the service account is appropriately added with full control permissions for processing.

Improved database usage regarding failed inserts

SQL Compliance Manager includes new code that allows it to reuse event IDs in the event of a failed data insert.

4.5 Fixed issues

- SQL Compliance Manager includes new code regarding the threading library, making sure that all files in the trace directory are successfully processed. This fixes an issue that caused large trace file backlogs in the Collection Server.
- The Administrative Activities Audit Option no longer re-enables automatically after being disabled.
- Users no longer receive an error when processing the trace file due to a limited column size in the table associated with Before-After Data.
- Users upgrading from SQL CM 3.7 to 4.3 no longer receive numerous file parsing errors.
- This release fixes an issue causing incorrect dates to appear if you have SELECT and Sensitive Columns enabled in the Audited Database Properties window. Previously, if the **Database SELECT operations** check box on the Audited Activities tab, and the Sensitive Columns tab includes **All Columns** of the **dbo.Customers** table, the dates in the summary for the associated SQL Server instance were incorrect.
- An issue that prevented new SQL CM Agent files from processing after adding a second node to a clustered repository no longer occurs.

- All failed integrity checks now includes specific events in the **Details** area of the Integrity Check Results window.
- Users no longer experience missing registry keys after re-adding monitored SQL Server instances.
- Adding an audited database to a monitored SQL Server instance no longer returns the server settings to default.
- Providing read-only access to the SQLcompliance database no longer requires that the GUEST account be enabled.