Previous features and fixed issues

This build of IDERA SQL Compliance Manager includes many fixed issues, including the following updates.

5.0 New features

Fully supports the SQL Server AlwaysOn Availability Groups feature

SQL Compliance Manager 5.0 now allows DBAs to monitor their availability groups, availability replicas, and availability databases through AlwaysOn Availability in SQL Server 2012 and newer. AlwaysOn automatically switches auditing from the primary to the secondary replica in the event of failure as well as failback to primary when it comes back online. This advantage prevents a loss of audit data trail in the event of failure.

Support for this feature also comes with:

- An Availability Group Statistics report that allows you view the historical health of your availability groups, availability replicas, and availability databases.
- An Availability Group Topology report that allows you to view the current topology of your availability groups configuration.
- Monitoring of key metrics specific to the AlwaysOn Availability Groups feature.
- Queue Size and Transfer Rates charts.

For additional information on SQL Compliance Manager and the AlwaysOn Availability Groups feature, see Enable automatic failover using AlwaysOn Availability Groups.

Offers a technology preview of a new web-based SQL Compliance Manager Dashboard

Along with the integration of the IDERA Dashboard, SQL Compliance Manager 5.0 includes a preview of a newly-designed web console that offers quick views of key audit trail activities on your SQL Servers from any web browser. Identify key compliance issues quickly and provide an easy access point to non-DBAs without giving them access to the entire Management Console.

Added integration with the IDERA Dashboard

SQL Compliance Manager 5.0 now integrates with the IDERA Dashboard, a common technology framework designed to support the IDERA product suite. Users are able to obtain an overview of the status of their SQL Servers and hosted databases all in a consolidated view and navigate to individual product dashboards for details. The IDERA Dashboard provides a central set of services for managing users, product registry, instance registry, aggregated alerts across IDERA applications, a central web server, and tags for grouping instances. For more information about the IDERA Dashboard, see Navigate the IDERA Dashboard web console.

Moved to the Windows .NET 4.0 framework

SQL Compliance Manager 5.0 supports Microsoft Windows operating systems using .NET 4.0. Note that .NET 4.0 or later must be installed on the audited server. For more information about requirements, see Software requirements.

5.0 Fixed issues

- Active Trace is now properly cleared when necessary.
- A change to the SQL Compliance Manager login filter settings from minutes to seconds fixes an issue that allowed new user events such as failed login attempts to be missed in reports.
- Reports now are viewable in .CSV format.
- SQL Compliance Manager 5.0 includes an update that clarifies alert email triggers when users to have two alert rules for Sensitive Columns.
- SQL Compliance Manager no longer displays conflicting data by including a fix that forces the collection of object names while processing trace file records.
- Normal user accounts are no longer able to capture SQL text used in admin activities without enabling additional options.
- When you have multiple columns selected for a particular table in Before-After Data (BAD), SQL Compliance Manager no longer labels events that update other columns as BAD events.
- SQL Compliance Manager now includes descriptions for ALTER ANY SCHEMA and ALTER ANY USER in the tracejob.cs file.
- The permissions check process is updated in SQL Compliance Manager 5.0 to avoid any issues when performing a check.
- Event types 158 and 258 now include expanded details that display when these types of events occur.
- SQL Compliance Manager Integrity Check now properly tracks and reports on deleted rows.

4.5 New features

Supports SQL Server 2014

SQL Compliance Manager supports the use of SQL Server 2014. Note that SQL Compliance Manager 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 Compliance Manager allows you to install in a Windows Server 2012 clustered environment. For more information about this feature, see Deploy SQL Compliance Manager 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 Compliance Manager 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 Compliance Manager 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 Compliance Manager 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 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 Compliance Manager 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 Compliance Manager 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.

4.3 New features

SQL Compliance Manager 4.3 now offers a Collection Server-only install

SQL Compliance Manager 4.3 now allows you to install the Collection Server and Repository only to support installing SQL Compliance Manager on a cluster.

4.3 Fixed issues

There are no fixed issues in this release.

4.2 New features

New Family Educational Rights and Privacy Act (FERPA) guideline

Apply the new FERPA regulatory guideline to ensure your audited databases meet the requirements of this legislation. You can apply this guideline through the CLI or through the Import Audit Settings feature in the Console.

FERPA was introduced in 1974. This federal law mandates the confidentiality and protection of student information in any educational institution that receives funding from the Federal Government from kindergarten through the university level. FERPA generally prevents an education agency or institution from sharing student records or personally identifiable information in those records with individuals who are not authorized to view that information. In some cases authorized individuals need to be monitored to deter insider theft and unauthorized dissemination of information.

New Sarbanes Oxley (SOX) guideline

Apply the new SOX regulatory guideline to immediately enforce the right auditing settings for sensitive financial data. Collect a detailed audit trail of all access to that data and then deliver reports that prove your compliance to auditors. You can apply this guideline through the CLI or through the Import Audit Settings feature in the Console.

SOX, also known as the Corporate and Auditing Accountability and Responsibility Act, was first introduced in 2002. This legislation was put in place as a response to the corporate and accounting scandals which cost investors billions of dollars. From an information technology standpoint, security professionals and database administrators must collectively implement policies and processes that audit permissions on, and access to, financial data as well data changes such as before and after values.

New CLI actions register instances and apply audit settings

Use the new command line interface (CLI) actions to quickly and easily register large numbers of SQL Server instances and immediately apply audit settings to the hosted databases. You can choose to apply the default audit settings, custom audit settings you have exported from another audited instance, or a regulation guideline.

4.2 Fixed issues

- When the T-SQL query associated with an event cannot be parsed, SQL Compliance Manager now captures the SQL statement and indicates that it could not be parsed. This issue was mostly likely to occur when auditing sensitive column access.
- The Details tab of the Event Properties window now displays the SQL statement that is issued to SQL Server before SQL Server performs its query parameterization. This code represents the initial T-SQL query executed by the user.

4.0 New features

Offers HIPAA compliance guideline support

Collect data that helps you align with nine Health Insurance Portability Accountability Act (HIPAA) citations and one HITECH requirement via an out-of-the-box, customizable template.

Includes PCI compliance templates

Use the new, customizable auditing templates to help you comply with eight Payment Card Industry Data Security Standards (PCI DSS) requirement guidelines.

Provides Regulation Guideline reporting

The Regulation Guidelines report includes details for all of the guidelines applied to the databases on the selected SQL Server instance.

Features a new SQL Compliance Manager Configuration Wizard for ease of use

The new SQL Compliance Manager Configuration Wizard allows you to use a single wizard to register SQL Server instances, deploy the SQLcompliance Agent, add databases for audit, configure your audit settings for selected regulatory guidelines, and more.

4.0 Fixed issues

- SQL Compliance Manager now properly processes Grant statements.
- An issue causing SQL Compliance Manager to record Create and Drop Index events as Alter User Table events no longer occurs.
- SQL Compliance Manager now loads custom reports on the Archived Events page without requiring the user to select a filter.
- SQL Compliance Manager now honors the DML/SELECT filters if you enable both Select auditing and Sensitive Column Auditing.

- SQL Compliance Manager now properly applies event filters for instances using non-standard ports.