New features and fixed issues

IDERA SQL Secure provides the following new features and fixed issues.

2.8 New features

- SQL Secure now supports SQL Server 2014
- SQL Secure now supports Always On Availability Groups
- SQL Secure now allows you to install the SQL Secure Repository on a failover cluster. The installer provides an option to select Cluster installation and specify a cluster node.
- Policy Templates have been updated to use the latest versions of SQL Server and OS:
    - Updated to policy templates:
        - CIS v 2.0 for SQL Server 2005 (from version 1.2)
        - PCI-DSS v 3.0 Guidelines for SQL Server (from version 2.0)
        - HIPAA Guidelines for SQL Server - update security checks as needed e.g. Operating System Version
    - Added templates for:
        - CIS v1.1.0 for SQL Server 2008
        - CIS v1.0.0 for SQL Server 2012
        - MS Best Practices Analyzer for 2008
        - MS Best Practices Analyzer for 2012
- This version had updated to a granular process for Exporting and Importing policies, so that authorized SQL Logins can be excluded from exporting, and when imported the active settings for those checks remain unmodified.
- The process for registering new SQL Server instances with SQL Secure now allows to define folders for file system permissions checks.
- SQL Secure now supports Sequence Objects for SQL Server 2012.
- SQL Secure supports users in contained databases for SQL Server 2012 and 2014.
- SQL Secure now provides the following new Security Checks:
    - Security Check for SQL Server Integration Services (SSIS) to verify if any public or other unauthorized principals have been granted permissions to use SSIS stored procedures.
    - Security Check added to level 1 and level 2 policy templates that shows risk on systems where permissions have been granted to the public role on objects outside the sys schema in user databases.
    - Security Check: *Unacceptable Database Ownership* detects if a database is found with an unacceptable owner
    - The Risk Assessment Report has been updated with new nine security checks.

2.8 Fixed issues

The following issues have been fixed in IDERA SQL Secure 2.8:

Phase out SQL Secure Itanium support

IDERA is beginning to phase out all Itanium support in SQL Secure 2.6 and all subsequent 2.x versions. While 2.8 will continue to operate with Itanium and support is available, SQL Secure 3.0 will not support the Itanium processor architecture. For more information, see the product requirements.

SQL Secure Repository requires SQL Server 2005 or later

When upgrading, migrating, or deploying the SQL Secure Repository for the first time, ensure you select an instance running SQL Server 2005 or later for your target location. SQL Secure no longer supports SQL Server 2000 platform for the SQL Secure Repository.

If you are upgrading from SQL Secure version 2.0 or earlier , you will need to migrate the Repository to a SQL Server 2005 or later instance. For more information, see IDERA Solution 00002617 ("How do I migrate SQL Secure from one server to another?").

Microsoft Reporting Services 2000 is no longer supported

If you are upgrading reports from Microsoft Reporting Services 2000 , then upgrade to Microsoft Reporting Services 2005 before installing the new reports in SQL Secure 2.8 to ensure the upgrade is successful.

New credentials may be necessary when upgrading

SQL Secure no longer uses the default credentials of your SQL Server Agent to collect Operating System and SQL Server security information. If, in a previously installed version, SQL Secure was configured to use the default SQL Agent credentials to collect security information, a window will open when you first open SQL Secure 2.8, prompting you for new credentials.

Blank password not accepted when registering a SQL Server instance

When registering a new SQL Server instance, blank passwords are not accepted for SQL logins due to the extreme security risk this poses.

SQL Secure can now audit the same cluster node on which it is installed

The SQL Secure now allows you to audit security data from SQL Server instances hosted on the same cluster node that hosts the SQL Secure Collector.

Fixed issues in this version

Support for contained database authentication security

SQL Secure now displays information and report on the security settings of database principals used for contained database authentication and connections. Contained databases are a new security feature available in SQL Server 2012.

SQL Secure now collects security data for AlwaysOn Availability Groups

When you take snapshots of the SQL Server 2012 instances you audit, SQL Secure now collects properties or security data for the AlwaysOn Availability Groups feature. AlwaysOn can be enabled only on instances running SQL Server 2012 & 2014 Enterprise Edition.