New features and fixed issues

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

3.0 New features

Added SQL Server file import

Users now can import a .csv file containing the SQL Servers they want to import for registration in IDERA SQL Secure. This is an important feature for environments having more than a few SQL Servers as it allows you to bulk import data into IDERA SQL Secure. For more information about this feature, see Import SQL Server instances.

Added tags for easier server management

IDERA SQL Secure now features server group tags to allow you to more easily manage your SQL Server instance snapshots. You can select tags when registering a SQL Server or simply add a tag to your existing instances. Tags allow you to select a specific group of SQL Servers rather than selecting servers one by one. For more information about server group tags, see Manage server group tags.

Added suspect SQL Server logins report

The new Suspect SQL Logins report displays all of the suspect SQL Server Accounts that do not have any assigned permissions, i.e. databases, objects, or server files. For more information about reporting, see Report on SQL Server Security.

Expanded Risk Assessment reporting

IDERA SQL Secure 3.0 includes multiple additions and modifications to the existing Security Checks in the Risk Assessment report. These new checks include:

- **Access**
  - **Files on Drive Using Not Using NTFS**. Updated to support ReFS for SQL Server 2016.
  - **Supported Operating Systems**. Removed support for Microsoft Windows 2003 and added support for Windows 2012, Windows 2012 R2, and Windows 2016.
  - **SQL Jobs and Agent**. Updated to flag any case where a proxy account is not in use.
  - **Encryption Methods**. Updated to flag any case where unsupported encryption methods are in use. Note that beginning with SQL Server 2016, all algorithms other than AES_128, AES_192, and AES_256 are deprecated.
  - **Certificate private keys were never exported**. Verifies that Certificate private keys are exported.
- **Configuration**
  - **Linked Server**. Checks to see if there are linked servers, and then checks to see if the linked server is running as a member of the sysadmin group. Linked servers can lead to performance issues and running them using sysadmin privileges can leave a database vulnerable to corruption.
  - **SQL Server Version**. Checks to make sure a supported version of SQL Server is in use. Flags any case where an unsupported SQL Server version is in use.
  - **Full Text Search Service Running**. Checks to make sure that this service is running on the selected instance.
  - **Unauthorized Accounts Check**. Updated to include checks for roles beyond sysadmin, including the Separation of Duties roles in SQL Server 2014 and the roles surrounding encryption for SQL Server 2016.
  - **Other General Domain Accounts Check**. Update to include checks for general domain accounts such as domain Users, Everyone, and Authenticated Users added to the selected instance.
- **Surface**
  - **SQL Server Available for Browsing**. Updated the name of this check to **SQL Server Browser Running**.

For more information about using reports within IDERA SQL Secure, see Report on SQL Server Security.

3.0 Fixed issues

The following issues are fixed in IDERA SQL Secure:

- Resolved an issue that occurred when trying to register a SQL Server instance, which is clustered and using AlwaysOn Availability Groups. The system tried to register the Cluster Server Name instead of the SQL Server Instance Name.
- Resolved an issue that caused SQL Server administrator accounts to show sysadmin accounts for other servers in the Server Security Report Card.
- IDERA SQL Secure no longer incorrectly pulls database role information from SQL Server 2000 databases.
- Users no longer receive false warning messages when running a snapshot.
- Resolved an issue that caused the system to display authorized accounts as unauthorized when a wildcard was included in the list of authorized accounts in Unauthorized Accounts Are Sysadmins.