New features and fixed issues

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

3.1.200 New features

Allows reference to decommissioned server instance snapshots

IDERA SQL Secure 3.1.200 now allows you to reference snapshots of decommissioned instances. Previously, IDERA SQL Secure removed permissions data for a server when it is removed from auditing. The only way to save the permissions and snapshot information for that instance was to back up the repository before decommissioning.

Supports TLS 1.2

IDERA SQL Secure 3.1.200 includes support for Transport Layer Security (TLS) version 1.2. The TLS protocol provides encryption, authentication, and data privacy and integrity when transferring information over a network, including VPN, VOIP, and instant messaging.

Includes new product versioning (x.x.x.x)

For internal tracking reasons, this release of IDERA SQL Secure includes an updated product versioning format from three to four parts. For example, the previous version of SQL Secure was version 3.1.0 (x.x.x) and this release is 3.1.200.x (x.x.x.x).

3.1.200 Fixed issues

- This release fixes an issue causing the SQL Secure Risk Assessment Comparison Report to show changes between snapshots when no changes actually occurred.
- Users now can remove a server instance without first removing it from an assessment or draft. If any assessment data exists, the user is asked whether they want to remove the server from all active assessments as well. If **Yes**, the assessment is kept intact while the instance is deleted. If **No**, the server is removed from the assessment as well.
- The **SQL Server SYSADMIN Accounts** security check now reports an accurate status instead of always reporting **OK** and not displaying any accounts. This metric did and continues to report correctly in a snapshot.
- Resolved an issue that caused the following error while processing a security check when **Database roles and members** is enabled: "Error 515 encountered on line xxxx: Cannot insert the value NULL into column 'usertype', table '@DatabaseRoleUsers'; column does not allow nulls. INSERT fails."
- This release fixes an error regarding SQL Server 2014 and SQL Server 2016 accounts in the **Unauthorized Account** security check. Previously, the Unauthorized Account security check for SQL Server 2014 initially reported, "No issues found." Then, when a SQL Server 2016 server was added, it listed the unauthorized accounts in the result. However, when going back to the SQL Server 2014 server, it displayed the same unauthorized accounts results that the SQL Server 2016 server revealed.
- Resolved an issue causing the error message,"Cannot insert duplicate key in object 'dbo.<servername>'. The duplicate key value is (1281, 327). The statement has been terminated." when attempting to create a snapshot.
- Changed the Unauthorized Account Check wording from, "Specify the unauthorized accounts," to "Specify the authorized accounts," in the description for the **Criteria** entry on the Policy Properties page and on the edit Values for Security Check window.
- When a user registers a virtual server that is part of a failover cluster, the name now correctly resolves to the cluster name.
- Resolved an issue with the **Database roles and members** and the **Server roles and members** security checks that caused metrics to provide details from other instances/databases.
- The GUI on the final screen of the SQL Secure Setup Wizard was updated to resolve the cut-off content of the descriptive text.
- The **Launch SQL Secure Console** is now enabled after a new installation or upgrade.
- The uninstallation wizard is updated to no longer show an incorrect final window.
- The copyright year is now correct throughout the product.
- The descriptive text within the **Row-Level Security** check is changed from, "... is configured for specific *databases* ..." to, "... is configured for specific *tables* ...".
- The descriptive text within the **Dynamic Data Masking** security check is changed from, "... is configured for specific *databases* ..." to, "... is configured for specific *columns* ...".

3.1 New features

Supports auditing of Azure SQL Database and SQL Server running in Azure virtual machines

IDERA SQL Secure 3.1 offers Cloud-specific capabilities for Azure-hosted SQL Server databases, including:

- Azure SQL Database and SQL Server running on Azure Virtual Machines (VMs).
- Security audits on Azure SQL Database instances and Azure Active Directory.
- Connecting to fully-qualified domain names for Azure VMs and Azure SQL Database instances as registered servers.

Expands installation options

IDERA SQL Secure 3.1 includes expanded installation options to support hybrid cloud environments.

Expands Security Check coverage

This release expands Security Check coverage for data protection, encryption, and firewall rules for the SQL Server platform, including Always Encrypted and Transparent Data Encryption.

Moved to the Windows .NET 4.6 framework

IDERA SQL Secure 3.1 supports Microsoft Windows operating systems using .NET 4.6. For more information about requirements, see Product requirements.

3.1 Fixed issues

There are no fixed issues in this release.