Use snapshots to collect audit data

A snapshot is a set of audit data that IDERA SQL Secure has collected from a specific SQL Server instance. You can configure snapshot filters to select which SQL Server objects you want to audit. You can take snapshots manually, as you need fresh data, or schedule snapshots to be taken at regular intervals.

SQL Secure uses audit snapshots to capture SQL Server user and object permission settings. These snapshots are listed in the **Explore Permissions** view by expanding the respective servers of the Audited SQL Servers tree. When you click a Snapshot, information about the snapshot is displayed on the right section of the console where the following tabs are displayed: Snapshot Summary, User Permissions, Role Permissions, and Object Permissions.

The **Snapshot Summary** tab provides all the information collected about your snapshot, some options change according the type of server.

Data located on the Snapshot Summary

The Snapshot Summary contains the following types of information:

Snapshot Properties

Provides the basic status of the selected snapshot, the time it was collected, how long the collection took to complete, whether or not it has been selected as a baseline, and any comments associated with it.

Audit Summary

Lists the statistics of the snapshot. These statistics include the number of objects, permissions, databases, logins, Windows accounts, Windows well-known groups associated with the snapshot, and whether Weak Password Detection is enabled or not.

> To collect and review data about the password health of your SQL logins, you need to enable the Weak password detection.

For On-premise, SQL Server on Azure VM, and SQL Server on Amazon EC2 accounts

Windows Accounts

Provides a partial list of the Windows users and groups that have access to the selected SQL Server instance either by a direct SQL Login or inherited via group membership.

OS Windows Accounts

Provides a partial list of the Windows users and groups that have access to OS objects but do not interact with SQL Server objects.

Suspect Windows Accounts

Lists the Accounts that SQL Secure was unable to collect data on. This can occur when SQL Secure does not have the proper rights to collect information on these users, or if the account was deleted. For more information, see Identify Suspect Windows Accounts.

Suspect OS Windows Accounts

Lists the Accounts that SQL Secure was unable to collect data on. This can occur when SQL Secure does not have the proper rights to collect information on these users, or if the account was deleted. For more information, see Identify Suspect Windows Accounts.

Unavailable Databases

Lists the databases that SQL Secure was unable to collect SQL Server security data on. This can happen when a database is unavailable during SQL Secure data collection; for example, a database being backed up is unavailable for data collection. For more information, see Identify unavailable databases.

Filters

Provides the filter information associated with the selected snapshot. For more information, see Add new filter.

For Azure SQL Database Amazon RDS for SQL Server accounts

Azure AD accounts and Amazon AD accounts

Provides a list of the Azure or Amazon users and groups that have access to the selected instance either by a direct SQL Login or inherited via group membership.

Unavailable databases

Lists the databases that SQL Secure was unable to collect SQL Server security data on. For more information, see Identify unavailable databases.

> ⚠ SQL Secure cannot collect data from the **model database** on RDS servers because of Amazon restrictions.

Filters

Provides the filter information associated with the selected snapshot. For more information, see Add new filter.