View snapshot summary

The IDERA SQL Secure **Snapshot Summary** tab lists statistics and other information about the selected snapshot. To access this information, expand the SQL Server for which you want to see its snapshots and then select a specific Snapshot.

Each snapshot is a listing of permission settings on a SQL Server instance at a particular point in time. Snapshots help you assess and manage your security settings. This provides a powerful tool you can use to diagnose security problems and quickly see where changes occur.

The **Snapshot Summary** displays the following sections:

- **Snapshot properties**. Gives general information about the snapshot, the status, the collection time, the duration, whether is its marked as a baseline snapshot or not, and any additional comments.
- **Audit Summary**. Displays the main summary information retrieved by the snapshot such as number of objects, permissions, databases, logins, windows accounts, OS controlled windows groups, and whether Weak Password Detection is enabled or not (Click here to enable /disable Weak Health Detection)
- **Accounts**. Windows accounts, OS Windows accounts, Suspect Windows accounts, Suspect OS Windows accounts, Unavailable databases, and Filters.

Login counts may differ from what is displayed in SQL Server 2005 or later. This count displays the number of Server Principles collected. In SQL Server 2005 or later, Server Principles include Logins, Server Roles, and Certificates, while in SQL Server 2000, principles include only Logins.

Configuration before collecting snapshots

Before snapshots are taken, you must tell SQL Secure what permission data you would like to collect and when you want SQL Secure to collect it.

You can specify these settings in **Audited SQL Server Properties** window that you can access by clicking the **Configure Audit Settings** in the upper section of the **Snapshot Summary**.

Permission Data

Configure the permission data that it is most important to you to be taken by the snapshot.

To configure these settings, in the **Audited SQL Server Properties** window, select the **Filters** tab, then specify those filters that will help you collect the data you need.

For more information about defining filters, go to Add Filter.

Snapshot schedule configuration

Snapshots capture security permission settings on SQL Server instances at configured intervals. At the scheduled time, a SQL Secure job is executed and data is collected from the SQL Server instance to the Repository database. This data set represents a single snapshot and is accessed directly by the SQL Secure Console. SQL Secure allows you to define when snapshots are taken.

You can specify these settings in the **Schedule** tab of the **Audited SQL Server Properties** window.

For more information of how to change the schedule collection time, go to Schedule snapshots.

Scheduling snapshots

Consider taking snapshots on a routine, scheduled basis. Because snapshots are taken over time, they can be viewed to see when changes are made to user or object permissions.

Grooming Snapshots

Snapshots are managed through the grooming process. Grooming allows you to determine which snapshots should be deleted from the SQL Secure Repository. You can schedule grooming to occur on a routine basis, ensuring you keep only the snapshots you need. For more information, see Set Snapshot Grooming.

Keep in mind

- Snapshots associated with saved assessments cannot be groomed.
- Snapshots that have been marked as baselines are not groomed

Mark a snapshot as a baseline

Baseline snapshots are snapshots that will not be deleted in the grooming process. To mark snapshots as baseline, you can right-click the snapshot and choose **Mark as Baseline**.

When a snapshot should be marked as baseline	Importance
When you take your first snapshot	To have a starting point to use to identify changes to permissions over time
At the end of the month, quarter, or year	To track compliance to your database security policies
When you implement a new security model	To identify unwanted changes or issues with the new model
When you notice problems or irregularities in permission settings in a snapshot	To analyze the issue to correct problems and change permissions settings

Viewing which snapshot is marked as baseline

To view which snapshot is marked as baseline, click the respective SQL Server. The **Audit History** section of the **Server Summary** pr operties displays a list of all snapshots in this server where you can find a **Baseline** column that informs you which snapshot is marked as a baseline and which ones are not.

Managing your snapshots

In addition to the setting above, you can perform the following actions with Snapshots.

- **Delete snapshots**. Right-click the respective snapshot (from the Audited SQL Servers tree or the **Audit History** of the **Server Summary**) and select **Delete Snapshot**.
- **Collect audit data manually**. Select **Take Snapshot Now** from the upper section of the **Snapshot Summary** or click the respective SQL Server, go to the **Snapshots** menu, and click the same option.

Resolve group names and group memberships across multiple domains

Using a single account to resolve group names and enumerate group memberships can be problematic when SQL Server grants permissions to accounts across multiple externally trusted domains.

In this situation, the server account specified on the Audited SQL Server Properties window should be an account that has been granted access to these external domains. This can be accomplished by either setting up two-way trusts between the account's domain and the external domains, or by creating pass-through accounts on all the external domains.