SQL Sentry Pass-through Authentication

Last Modified on 04 August 2021

⚠**Important:** SQL Server authentication can be used for any **Watched** SQL Server instance using an instance's **Monitoring Service Connection Properties** context menu item. This eliminates the need for **Pass-through Authentication** if SQL Sentry's performance monitoring isn't being utilized to collect Windows performance counters from the targets, and if you aren't monitoring the target with **Performance Analysis** or **Events** Windows Task Scheduler.

Pass-through Authentication enables Windows computers in different domains or in non-Windows network environments to communicate with one another by using identical user accounts and passwords on each computer.

If performance monitoring is required either through SQL Sentry **Performance Analysis** or you need to watch a Windows Task Scheduler, **Pass-through Authentication** may still be required.

Additional Information: See the SQL Sentry Tips and Tricks: Monitoring Targets Across Multiple Domains blog post.

Example

For example, if user JDoeDBA with password SQLrocks! is created on SERVER1 and SERVER2, JDoeDBA can connect and authenticate directly from SERVER1 to SERVER2, and vice versa, without using domain-level authentication.

It's the SQL Sentry monitoring service's job to collect data from monitored targets, then store the data in the SQL Sentry database for analysis with the SQL Sentry client. In the example above, SERVER1 may be the computer where the SQL Sentry monitoring service is running, and SERVER2 is either the monitored computer, or the computer where the SQL Sentry database resides.

User Access Control

Additional configuration may be required on machines running Windows Vista and higher with the introduction of User Access Control (UAC). When a remote connection is made using **Pass-through Authentication,** the machine is unable to resolve elevated permissions under UAC, and for WMI and registry purposes the account is treated as a regular (non-admin) user, even if the account exists in the local administrators group.

Additional Information: For more information and configuration details about using **Pass-through Authentication** on Windows Vista and higher, see the WMI Registry Access article from Microsoft.