Set general server options

The General tab allows you to edit the most common property settings. These settings include the data collection interval or the amount of time between data collections, the server availability verification interval, and the credentials used to collect data.

Access the General tab

You can access the General tab of the Monitor SQL Server Properties window by right-clicking the appropriate monitored SQL Server instance, and then selecting **Properties**.

Associate tags with an instance

The tag field allows you to select a tag to add your server to or add a new tag. Tags help you organize server instances into meaningful groups.

Select a diagnostic data collection interval

The data collection interval is the amount of time SQLdm waits between each collection of data on the selected SQL Server instance. You can set a different interval for each of the following functions:

Collect diagnostic data and raise alerts (max 30 minutes)

The interval between times that the SQLdm Collection Service collects diagnostic data and raises the associated alerts. Lower values cause SQLdm to raise alerts more quickly, but also cause more frequent refreshes, which increases your monitoring overhead.

Collect and alert on database metrics (max 24 hours)

The interval between times that the SQLdm Collection Service collects database space-related data and raises the associated alerts. Lower values cause SQLdm to raise alerts more quickly, but also cause more frequent refreshes, which increases your monitoring overhead. In environments with a large number of databases whose sizes do not change rapidly, setting the database data collection to a long interval can greatly reduce the monitoring footprint.

By default, SQLdm collects diagnostic data every six minutes and database data every 60 minutes. Consider the following factors before selecting your data collection interval:

Data collection purpose

If your goal with this data collection is to identify broad trends and alert on critical downtime, then a longer refresh interval is appropriate. If you are closely monitoring your SQL Server instance for minute-by-minute changes, use a shorter duration.

Data collection frequency

When diagnosing specific problems or when working with a problematic SQL Server instance, a short interval lets you capture enough data to diagnose the issue. In most situations, the default interval provides sufficient data for your diagnostic needs. Note that SQL Server instances used only occasionally may require less monitoring attention.

Notification of existing or potential problems

Remember that a lower collection interval results in SQLdm raising alerts more quickly, but also increases your monitoring overhead. This is true when any setting causes more frequent refreshes.

System resource impact

Although SQLdm limits the amount of system resource impact when collecting data, short collection times on SQL Server instances with large amounts of data could potentially cause system performance degradation. Using the default interval should meet your data collection needs while limiting any system resource impacts.

Space needed for the SQLdm Repository

A lower collection interval results in more frequent refreshes which are all stored in the SQLdm Repository. Make sure you have enough available space to accommodate these lower settings.

Data spikes

SQLdm averages most metrics over the timeframe between collections. More-frequent data collection causes increased movement in averages because of short-duration events. For example, a 15-second CPU spike has a greater effect on a one-minute refresh than on a six-minute refresh. You can use alert smoothing to reduce the impact of data spikes on a per-alert basis.

Select a server availability verification interval

The server availability verification interval is the amount of time SQLdm waits between verifying availability on the selected SQL Server instance. If the connection test collector does not complete within the time specified in the **Alert if the server is inaccessible (max 10 minutes)** field, the SQL Server instance is considered unresponsive. Setting this field to a very low value can result in false positive alerts.

Collect extended session data

The extended session collection data includes important session information, such as details, locks and blocks. If this information is important to you, make sure the **Collect extended session data, including session details, locks, and blocks** check box is selected.

Limit the number of DBCC Inputbuffer executions

You can limit the number of executions performed by the DBCC Inputbuffer, which retrieves the actual input command for the Session Details view, among others. Note that on busy servers, decreasing the **Limit executions of DBCC Inputbuffer to** value can reduce monitoring impact.

Data collection credentials

SQLdm uses the specified credentials to collect data from the monitored SQL Server instance. You can choose to use either Windows authentication or SQL Server authentication.

Windows authentication

Windows Authentication uses the security of the operating system to create a trusted connection only if the account matches a security account defined in SQL Server. This security account must have sufficient permissions on the monitored instance to collect data and OS metrics.

SQL Server authentication

Select this option to use the credentials of a specific SQL Server account.

Select encryption options

SQLdm allows you to designate encryption methods used to encrypt data between the Collection Service and the monitored SQL Server instance. You can choose to use SSL or SSL with Trust Service Certificate.

Encrypt Connection (SSL)

This option sets a flag in the connection properties that is used when the collection service connects to a monitored server that specifies that SSL (Secure Sockets Layer) is used to encrypt the data between the collection service and the monitored SQL Server instance. For this option to work correctly, configure the monitored SQL Server instance to support encryption.

Trust Server Certificate (Bypass Certificate Validation)

This option is available only when the Encrypt Connection (SSL) is selected. This option allows you to skip the certificate validation when a SQL Server instance establishes a connection. If SSL on the monitored SQL Server instance is not configured to use a certificate that the collection service trusts, the connection is rejected unless the Trust Server Certificate option is selected.