SQLdm components and architecture

SQLdm consists of a light, unobtrusive architecture that easily runs in your SQL Server environment with minimal configuration. All SQLdm components run outside and separate from SQL Server processes.

SQLdm Console

Use the SQLdm Console to:

- View real-time status
- Configure alert notifications on specific metric thresholds at the server and database levels
- View historical reports
- Perform administrative functions

The SQLdm Console retrieves historical information directly from the SQLdm Repository. All real-time requests use the SQLdm services to poll the monitored SQL Server.

SQLdm Services

SQLdm has three centralized services, the Management Service, the Collection Service, and the Predictive Service. These three services reside on the same computer.

The Management Service: The Management Service performs the following primary functions:

- Provides real-time data to the SQLdm Console
- Receives historical data from the Collection Service for storage in the Repository
- Raises alerts and sends alert notifications

The Collection Service: The Collection Service performs on-demand and scheduled collection from the monitored SQL Servers.

The Predictive Service: The Predictive Service is used for Alert Forecasting and performs the following primary functions:

- Calculates the Alert Forecast every hour
- Builds a forecasting model once a day

SQLdm Plug-in

When SQLdm is registered with the Idera Dashboard, the product plug-in module is deployed. The SQLdm plug-in consists of web views and widgets and a .NET based add-in module (SQLdm add-in). The web views and widgets are deployed in the Web Application Service of the Idera Dashboard, and the SQLdm add-in in the Core Service of the same.

The Web Application Service dynamically loads in SQLdm's views and widgets and makes them available to web console users. The views and widgets use the SQLdm add-in REST APIs to retrieve data. Likewise, the SQLdm add-in retries data from the product services and Repository.

SQLdm Web Console integrated to the Idera Dashboard

The Idera Dashboard and SQLdm web console are automatically installed upon upgrade or during installation of the 9.0 or higher versions.

To access the web console:

1. Open your selected Browser, make sure it is compatible with the SQLdm web console requirements.
2. Type the SQLdm product URL: **http://<machinename>:<port>** where **<machinename>** is the name of your host or machine, and **<port>** is the port specified during installation. The default URL is **http://<localhost>:9290**.
3. When the SQLdm web console launches on your browser, use your Windows user account **<domain\user>** with the respective password to log into the product.

To learn about the new components and architecture, hardware and software requirements, and the required accounts and permissions you need to run the Idera Dashboard and SQLdm web console in your environment, see Deploy the Idera Dashboard and SQLdm.

The Idera Dashboard Web Application service comes with SSL already set up. For more information on running the Idera Dashboard over SSL, see Run the Idera Dashboard over SSL (HTTPS)

SQLdm Repository

The SQLdm Repository is a centralized SQL Server database that stores collected metrics on a scheduled basis, historical data, and alerts information. The SQLdm Repository also stores configuration information, such as the credentials used to monitor a registered SQL Server instance.

SQLdm 9.0 and later requires Microsoft SQL Server 2005 or above running on the computer that hosts the SQLdm Repository database for all installations.

Authentication in SQLdm

SQLdm uses the same types of authentication available in the SQL Server security model. When specifying account credentials for the SQLdm services, you can use Windows Authentication or SQL Server Authentication.

When considering which authentication to use, keep in mind that SQL Server Authentication is required when no domain trust exists between the SQLdm Services computer and the computers hosting the monitored SQL Server instances. For example, if the monitored SQL Server instances are located in an untrusted domain or behind a firewall, you must use SQL Server Authentication to successfully deploy SQLdm. In this case, you must use the **sa** account or a SQL Server login that has System Administrator permissions.

For more information about these authentication types and the SQL Server security model, see the Microsoft document, Authentication in SQL Server.