Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for Microsoft SQL Server

Release 2 (2.0.2.1.0)

E10005-01

January 2007

This document provides a brief description about the Oracle System Monitoring Plug-in for the Microsoft SQL Server, details on the versions the plug-in supports, prerequisites for installing the plug-in, and step-by-step instructions on how to download, install, verify, and validate the plug-in.

Description

The System Monitoring Plug-in for the Microsoft SQL Server extends Oracle Enterprise Manager Grid Control to add support for managing Microsoft SQL Server instances. By deploying the plug-in within your Grid Control environment, you gain the following management features:

- Monitor SQL Server instances.

- Gather configuration data and tracks configuration changes for SQL Server instances.

- Raise alerts and violations based on thresholds set on monitoring and configuration data.

- Provide rich out-of-box reports for the user interface based on the gathered data.

- Support monitoring by a remote Agent. For remote monitoring, the Agent does not need to be on the same computer as the SQL Server.

Versions Supported

This plug-in supports the following versions of products:

- Enterprise Manager Grid Control 10*g* Release 2 or higher Management Service

- Enterprise Manager Grid Control 10*g* Release 2 or higher Agent for Windows

- Standard, Enterprise, and Workgroup editions of Microsoft SQL Server 2000

Prerequisites

The following prerequisites must be met before you can deploy the plug-in:

- Microsoft SQL Server 2000 is installed.

- The following components of Oracle Enterprise Manager 10*g* Grid Control release 2 or higher:

ORACLE®

- Oracle Management Service with Oracle Management Repository

- Oracle Management Agent for Windows

  You can install the Agent on the same computer as SQL Server 2000 (referred to as local Agent monitoring), or you can install the Agent on a different computer from SQL Server 2000 (referred to as remote Agent monitoring).

- Windows Management Instrumentation (WMI) provider for Windows and the SQL Server. Enable support by running the setup.exe file located in the SQL Server Installation CD:

  <CD_Drive>/x86/other/wmi

- Microsoft JDBC driver for the SQL Server is installed. See "Setting up the JDBC Driver" for the procedure.

- Windows Management Instrumentation Service is up and running.

- For remote Agent monitoring, a remote Agent must be properly configured. See "Configuring a Remote Agent" for the procedure.

- User privileges for the Job system of Enterprise Manager. For the procedure, refer to "Setting Credentials for the Job System to Work with Enterprise Manager" in one of the following installation guides:

  - Oracle Database Installation Guide 10g Release 2 (10.2) for Microsoft Windows (32-Bit) — B14316-01

  - Oracle Database Installation Guide 10g Release 2 (10.2) for Microsoft Windows (64-Bit) on Intel Itanium — B14317-02

  - Oracle Database Installation Guide 10g Release 2 (10.2) for Microsoft Windows (x64) — B15681-02

  These guides are listed in the Installation Guides section of the Oracle Database Documentation Library at the following location:

  http://www.oracle.com/pls/db102/homepage

  Note: If you do not assign the correct privileges for users, the deployment will fail.

- If you want to use version 2.0.2.1.0 of the Microsoft SQL Server plug-in, you need to do one of the following:

  - Install this version on Oracle Enterprise Manager Windows Agent version 10.2.0.2.

    or

  - Apply a one-off patch on Oracle Enterprise Manager Windows Agent version 10.2.0.1. Refer to Metalink and Oracle bug #5349647 for more information.

Deploying the Plug-in

After you ensure that the prerequisites are met, follow these steps to deploy the plug-in:

1. Download the SQL Server Plug-in archive to your desktop or computer on which the browser is launched. You can download the archive from the Oracle Technology Network (OTN).

2. Log into Enterprise Manager Grid Control as a Super Administrator.

3. Click the **Setup** link in the upper right corner of the Grid Control Home page, then click the **Management Plug-ins** link on the left side of the Setup page.

4. Click **Import**.

5. Click **Browse** and select the plug-in archive.

6. Click **List Archive**.

7. Select the plug-in and click **OK.**

8. Verify that you have set preferred credentials on all Agents where you want to deploy the plug-in.

9. In the Management Plug-ins page, click the icon in the **Deploy** column for the SQL Server plug-in. The Deploy Management Plug-in wizard appears.

10. Click **Add Agents**, then select one or more Agents to which you want to deploy the plug-in. The wizard reappears and displays the Agent you selected.

11. Click **Next**, then click **Finish.**

    If you see an error message stating that the preferred credential is not set up, go to the Preferences page and add the preferred credentials for the Agent target type.

Adding Instances for Monitoring

After successfully deploying the plug-in, follow these steps to add the plug-in target to Grid Control for central monitoring and management:

1. From the Agent home page where the plug-in was deployed, select the Microsoft SQL Server target type from the **Add** drop-down list, then click **Go**. The Add Microsoft SQL Server page appears.

2. Provide the following information for the properties:

   - **Name** — Unique target name across all the Grid Control targets, such as SqlServer2k_Hostname. The name represents this SQL Server target across all user interfaces within Grid Control.

   - **SQL Server Host** — Name of the host where the SQL Server is running

   - **SQL Server Name** — Name of the SQL Server instance. Refer "Providing SQL Server Name Instance" for details.

   - **JDBC URL** — URL for JDBC. The default port is 1443. The syntax is as shown:

     jdbc:microsoft:sqlserver://<hostname>:<port>

   - **JDBC Driver** — SQLServerDriver JDBC driver class in the .jar:

     com.microsoft.jdbc.sqlserver.SQLServerDriver

   - **Database Username** — Valid user for the database

- **Password for the Database User** — Corresponding password for the database user

- **System Username** — Host user name that must be an Administrator user. Required only for remote Agent monitoring.

- **System Password** — Password for the Username. Required only for remote Agent monitoring.

- **Role** — (Optional)

3. Click Test Connection to make sure the parameters you entered are correct.

4. Reenter the encrypted parameters from step 2 if the connection test was successful, then click **OK**.

Note: After you deploy and configure the plug-in to monitor one or more targets in the environment, you can customize the monitoring settings of the plug-in. This alters the collection intervals and threshold settings of the metrics to meet the particular needs of your environment. If you decide to disable one or more metric collections, this could impact the reports that the metric is a part of.

Providing SQL Server Name Instance

The SQL Server name instance that you provide in the "SQL Server Name" field must be based on the name displayed in the server instance list. To retrieve the server instance list, follow the steps detailed in the section "Retrieving SQL Server Instance List".

The name displayed depends on the instance type (default or nondefault). Table 1 provides the details:

Table 1   Query Results

SQL Server Instance	Name Displayed	Example	SQL Server Name to be Provided
Nondefault	`<SQLServer_ MachineName>\<SQLServer _InstanceName>`	stmpi1\MYSQLAgent	MYSQLAgent
Default	- (LOCAL) - `<SQLServer_ MachineName>`	- (LOCAL) - LABSMPQA-PC15	- (LOCAL) - LABSMPQA-PC15

In the case of a default SQL Server instance, the name might be displayed in either of the ways listed in the table.

Retrieving SQL Server Instance List

1. On the SQL Server task bar, go to Start, then click **Run**.

2. Type `wbemtest` in the Open field.

3. Click **OK.**

The Windows Management Instrumentation Tester dialog box appears.

4. In the Name Space text box, type `root\MicrosoftSQLServer`.

> **Note:** You might encounter the WMI error "0x8004100e" or "Invalid Namespace" if the namespace root\MicrosoftSQLServer is not enabled. For details, refer "Prerequisites".

5. Click **Login**.

6. In the Windows Management Instrumentation Tester dialog box, click **Query**.

   The Query dialog box appears.

7. Type the following query in the Query text box:

   `select name from MSSQL_SQLServer`

8. Click **Apply.**

   All the SQL Server instances available on the system are displayed.

Naming Convention

The graphics in this section explain the naming convention followed in the query results and suggest the SQL Server name you must provide in the "SQL Server Name".

- Nondefault SQL Server Instance

Figure 1   Nondefault SQL Server Instance
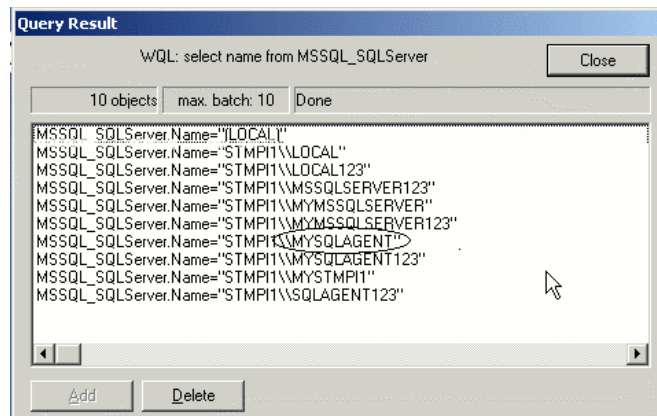
The highlighted SQL Server instance is nondefault. The name displayed is MYSQLAGENT. Therefore specify `MYSQLAGENT` as the SQL Server Name.

- Default SQL Server Instance: (LOCAL)

Figure 2   Default SQL Server Instance: Local
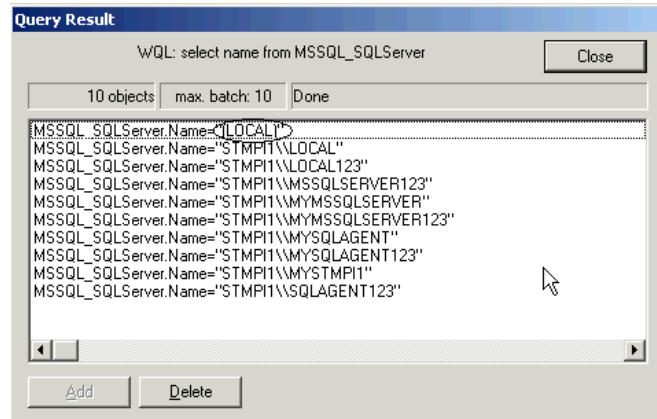
The highlighted SQL Server instance is default and the name displayed is (LOCAL). Therefore specify (LOCAL) as the SQL Server Name.

- Default SQL Server Instance: SQL Server Machine Name

Figure 3   Default SQL Server Instance: SQL Server Machine Name
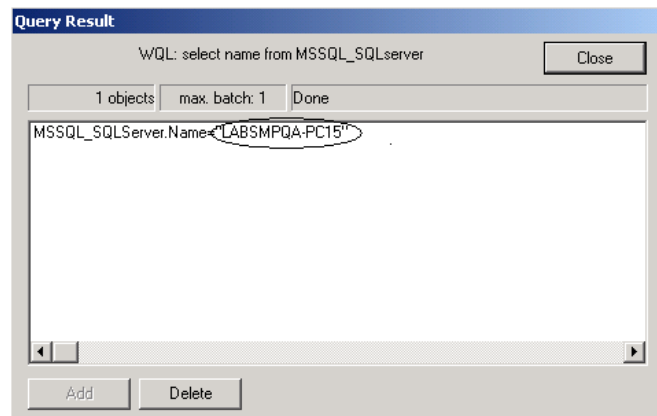
The highlighted SQL Server instance is default. The name displayed is the SQL Server Machine name. Therefore, specify the SQL Server Machine name as the SQL Server Name.

Verifying and Validating the Plug-in

After waiting a few minutes for the plug-in to start collecting data, use the following steps to verify and validate that Enterprise Manager is properly monitoring the plug-in target:

1. Click the SQL Server target link from the Agent home page Monitored Targets table. The Microsoft SQL Server home page appears.

2. Verify that no metric collection errors are reported in the Metrics table.

3. Ensure that reports can be seen and no errors are reported by clicking the **Reports** property page.

4. Ensure that configuration data can be seen by clicking the **View Configuration** link in the Configuration section. If configuration data does not immediately appear, click **Refresh** in the View Configuration page.

Setting up the JDBC Driver

The Microsoft SQL Server 2000 Driver for JDBC consists of three .jar files that the Agent should be able to access: msbase.jar, mssqlserver.jar and msutil.jar. The driver is available from the Microsoft Download Center.

Follow the steps below if the Microsoft JDBC driver is not installed.

1. Place the files in an appropriate directory. It is recommended that you create a jdbcdriver directory under agent/sysman/.

2. Add the location of each individual driver .jar file to the classpath.lst file under the $ORACLE_HOME/sysman/config directory if the Agent is installed on a standalone system.

3. If the Agent is installed on a system that is part of an OS cluster, you need to edit the classpath.lst file under the $ORACLE_HOME/<node_name>/sysman/config directory, where node_name is the name of the system where the Agent is installed.

   If the classpath.lst file does not exist, create the file. For example, the classpath.lst file in a Windows environment might appear as shown in the following example:

   C:\ms\jdbcdriver\msbase.jar

   C:\ms\jdbcdriver\mssqlserver.jar

   C:\ms\jdbcdriver\msutil.jar

4. Restart the Agent by executing the following commands at prompt:

   ```
   $$ORACLE_HOME/bin/emctl stop agent
   $$ORACLE_HOME/bin/emctl start agent
   ```

   The modification of classpath.lst takes effect.

Configuring a Remote Agent

The steps for deploying the plug-in are the same for remote Agent monitoring and local Agent monitoring. However, if the Agent is on a remote computer from the plug-in target, certain configuration changes are required to access the Windows Management Instrumentation (WMI) data on the computer where the plug-in target resides.

In a scenario where Computer A runs the Agent, and the target is installed on computer B, do the following to set up Computer A:

1. Go to the Windows Control Panel and select Administrative Tools, then Services.

2. Select the Oracle Enterprise Manager Agent service from the listed computer where the Agent is running.

3. Right-click the service, then select **Properties**.

4. Click the **Log On** tab. By default, this service is started with the Local System account.

5. Change the default account by selecting the **This account** radio button, and provide an account and password that exists on both computer A as well as computer B.

   Note that the account should be a member of the Administrators group, and the account should have administrative privileges on computer B. The password should not be left blank.

6. Click **OK**, then restart the Agent service.

7. Ensure that the Windows Management Instrumentation Service is up and running on both computers.

The Agent should now be able to collect data from the remote plug-in target computer. If the configuration above is not initiated, metric collection errors can appear for the plug-in target's metrics.

To ensure that metric collection errors do not occur within Enterprise Manager, Oracle recommends reviewing the Microsoft documentation on the WMI setup. Refer to the Microsoft documentation from the Microsoft website for additional configuration details.

Note: For a remote Agent, the platform to which the Agent is installed can be any Windows type that may not be supported for the SQL Server. For example, if the SQL Server is running on Windows 2003, you can install the remote Agent on Windows XP to monitor it.

Undeploying the Plug-in

Follow these steps to undeploy the plug-in from an Agent:

1. Log in to Enterprise Manager Grid Control as a Super Administrator.

2. Select the **Targets** tab, then the **All Targets** subtab. The All Targets page appears.

3. Select the Microsoft SQL Server Plug-in target and click **Remove**. You must do this step for all targets of the plug-in.

4. Make sure that the preferred credentials are set on the Agents where the plug-in is deployed.

5. Click the **Setup** link in the upper right corner of the All Targets page, then click the Management Plug-ins link on the left side of the Setup page. The Management Plug-ins page appears.

6. Click the icon in the **Undeploy** column for the Microsoft SQL Server Plug-in. The Undeploy Management Plug-in page appears.

7. Check all the Agents that are currently deployed with the Microsoft SQL Server Plug-in and click **OK**.

   You must undeploy the plug-in from every Agent in the system to completely remove it from the enterprise.

8. Select the Microsoft SQL Server Plug-in on the Management Plug-in page and click **Delete**.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at
http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.