Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for Microsoft SQL Server

Release 11 (4.1.3.1.0)

E16546-03

August 2010

This document provides a brief description about the Oracle System Monitoring Plug-in for 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 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.
- Supports both SQL Authentication and Windows Integrated Authentication
- Gather configuration data and track configuration changes for SQL Server instances.
- Raise alerts and violations based on thresholds set on monitored metrics and configuration data.
- Provide rich out-of-box reports based on the gathered data.
- Support monitoring by a local or remote Agent. Local Agent is an agent running on the same host as the SQL Server. Remote Agent is an agent running on a host that is different from the host where SQL Server is running.

Versions Supported

This plug-in supports the following versions of products:

- Enterprise Manager Grid Control 10.2.0.3 or higher
- Oracle Management Agent 10.2.0.1 or higher for Windows
- Standard, Enterprise, and Workgroup editions of Microsoft SQL Server 2000, Microsoft SQL Server 2005, and Microsoft SQL Server 2008 as detailed below:
  - Microsoft SQL Server 2000 (32-bit)
  - Microsoft SQL Server 2005 (32-bit)
  - Microsoft SQL Server 2005 (64-bit) running on x64 or Itanium-based servers

  - Microsoft SQL Server 2008 (32-bit)
  - Microsoft SQL Server 2008 (64-bit) running on x64 or Itanium-based servers
- Microsoft SQL Server 2005 Cluster: Active/Active and Active/Passive

Prerequisites

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

- Install the following components of Oracle Enterprise Manager Grid Control:
  - Oracle Enterprise Manager Grid Control 10.2.0.3 or higher
  - Oracle Management Agent for Windows 10.2.0.1 or higher

    For 10.2.0.1 Agent, apply the one-off patch for bug #5587980. Refer to *My Oracle Support* and Oracle bug #5587980 for more information.

    For 10.2.0.2 Agent, apply the one-off patch for bug# 5587980. Refer to *My Oracle Support* and Oracle bug #5587980 for more information.

    You can install the Agent on the same computer as SQL Server 2000 or SQL Server 2005 and SQL Server 2008 (referred to as local Agent monitoring), or you can install the Agent on a different computer from SQL Server (referred to as remote Agent monitoring).

    If Oracle Enterprise Manager 10.2.0.4 Agent where the plug-in is deployed, resides on a Windows Vista/Windows Server 2008 machine, apply the one-off patch for bug #6596234. Refer to My Oracle Support and Oracle bug #6596234 for more information.
- For the plug-in to establish connection to SQL Server instance using Windows Integrated Authentication mode, when deployed on a 64-bit (X64 or IA64) copy of Enterprise Manager Agent running on 64-bit Windows operating system, do the following:
  - Depending on the JVM version, copy the respective version of `sqljdbc_auth.dll` to the folder `$AgentHome\sysman\jdbcdriver`. If the directory does not exist, create it. The file `sqljdbc_auth.dll` is available as part of Type 4 Microsoft SQL Server 2005 JDBC Driver version 1.2 (after unzipping, you will find three files with same name, that is, `auth\x86\sqljdbc_auth.dll`, `auth\x64\sqljdbc_auth.dll`, and `auth\ia64\sqljdbc_auth.dll`)
    - For X64 version of Enterprise Manager Agent installed on X64 (Xeon or AMD) Windows systems, copy the file `auth\x64\sqljdbc_auth.dll` to `$AgentHome\sysman\jdbcdriver` (the dll file should be copied directly under the folder specified. No sub-directories should be created.)
    - For IA64 version of Enterprise Manager Agent installed on IA64 Windows systems, copy the file `auth\ia64\sqljdbc_auth.dll` to `$AgentHome\sysman\jdbcdriver`

    Note: ·No manual step needs to be performed when the plug-in is deployed on 32-bit copy of Enterprise Manager Agent (running on 32-bit or 64-bit Windows).

- The minimum version required in SQL Server 2000 for Windows Integrated Authentication based monitoring is SQL Server 2000 Service Pack 4 or later.
- Local monitoring of Microsoft SQL Server 2005 Cluster requires configuring Grid Control Agents in Windows HA - Failover Cluster Environments, see My Oracle Support note 464191.1.
- Access privileges required for non-admin System user to perform Remote Monitoring of SQL Server instance.
  - For more information, see Configuring Remote Connections to Monitor Targets.
- As part of JDBC URL, either IP Address or host name can be provided. Ensure that the host name can be resolved consistently on the network. Standard TCP tools such as "nslookup" and "traceroute" can be used to verify the host name. Validate using the following commands on Management Agent where plug-in is deployed:
  - `nslookup <hostname>`

    This returns the IP address and fully qualified host name.
  - `nslookup <IP>`

    This returns the IP address and fully qualified host name.

  Note: The hostname provided in the JDBC URL should be a fully qualified name (that is, must include the domain name also).

- (For SQL Server 2000) Windows Management Instrumentation (WMI) provider of the SQL Server are installed and enabled. Enable support by running the setup.exe file located in the SQL Server Installation CD. For more information, see Installing and Enabling Windows Management Instrumentation.

  ```
  <CD_Drive>/x86/other/wmi
  ```
- Windows Management Instrumentation Service is up and running.
- Preferred credentials are set and validated on all Agents where you want to deploy the plug-in. For more information, see Configuring the Management Agent to Deploy the Plug-In.
- (For Agent running on Microsoft Windows) OS privileges for the user (set in the Preferred Credentials for the Agent) must meet the requirements documented in "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.

- Enable TCP/IP for the SQL Server instance. For more information, see Enabling and Finding TCP/IP Port Information.
- Enable SQL or Mixed Authentication on the SQL Server instance. For more information, Enabling SQL Authentication or Mixed Authentication.
- Create a suitable DB user with 'sysadmin' fixed server role.
- To monitor the SQL Server instance using non-sysadmin user, create a user with non-syadmin role and provide the following access to it:

  1. Execute this command to give access to the user:

     ```
     GRANT VIEW SERVER STATE TO "login name"
     ```

  2. Provide database access to the user.
  3. Provide `SQLAgentOperatorRole` fixed database role in `msdb` to the user.

Configuring the Management Agent to Deploy the Plug-In

To configure the Agent, you must first ensure that the user starting the Agent service belongs to the Local Administrators Group. Also, you must set the preferred credentials on all Agents where you want to deploy the plug-in. To do so, follow the instructions given in the following sections.

Assigning Advanced Privileges to User

To assign advanced privileges, do the following:

1. Locally on the Microsoft Windows node hosting the Agent, check that the user starting the Agent service belongs to the Local Administrators Group. If not, add it.
2. Open the Local Security Settings Windows Tool and give the following Advanced Privileges to the user starting the Agent service:
   - Act as part of the operating system
   - Adjust memory quotas for a process
   - Logon as batch job
   - Replace a process level token
3. Restart the Agent service if it is running.
4. Set the Preferred Credentials for the Host and the Agent in the Grid Control. For more information, see Setting and Validating Preferred Credentials.
   - The OS user set in the Preferred Credentials must belong to the Local Administrators Group.
   - This OS user must have the following Advanced Privileges:
     – Act as part of the operating system

- Adjust memory quotas for a process
- Logon as batch job
- Replace a process level token

Setting and Validating Preferred Credentials

To set the preferred credentials on all Agents where you want to deploy the plug-in, do the following:

1. In Enterprise Manager Grid Control, click **Preferences.**
2. In the Preferences page, click **Preferred Credentials** in the left pane.

   The Preferred Credentials page appears.
3. For the corresponding Target Type, for the Host target type, from the **Set Credentials** column, click the icon.
4. In the Host Preferred Credentials page, in the Target Credentials section, for the host that is running the Management Agent where the plug-in has to be deployed, specify the user name and password.
5. After setting the credentials, on the same page, click **Test**. If you test runs successfully, your credentials are set correctly.
6. Run the OS Command job for the Management Agent where the plug-in has to be deployed.
   - Log in to Enterprise Manager Grid Control.
   - Click the **Jobs** tab.
   - In the Job Activity page, from the Create Job list, select **OS Command**, and click **Go**.
   - Fill up the details required in the following pages, and click **Submit** to run the job. If the job runs successfully, your credentials are set correctly.

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.

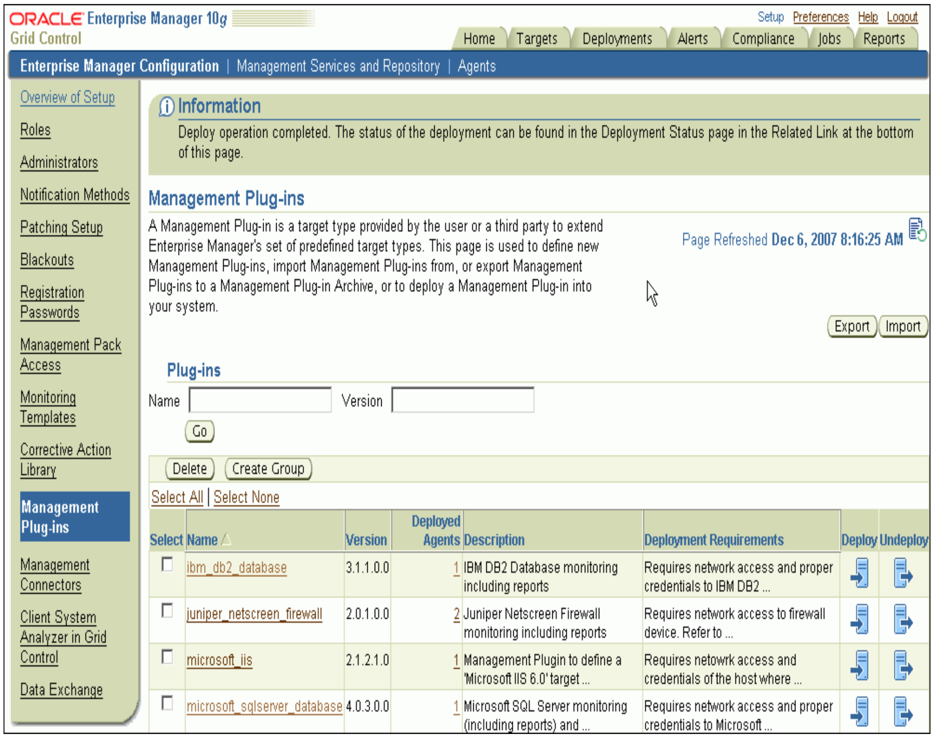
10. Click **Add Agents**, then select one or more Agents to which you want to deploy the plug-in. The wizard reappears and displays the Agent you selected.

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.

    If there are no errors, then you will see the following screen:

Figure 1 Successful Deployment



Information

Deploy operation completed. The status of the deployment can be found in the Deployment Status page in the Related Link at the bottom of this page.

Management Plug-ins

A Management Plug-in is a target type provided by the user or a third party to extend Enterprise Manager's set of predefined target types. This page is used to define new Management Plug-ins, import Management Plug-ins from, or export Management Plug-ins to a Management Plug-in Archive, or to deploy a Management Plug-in into your system.

Page Refreshed Dec 6, 2007 8:16:25 AM

Plug-ins

Name

Version

Select	Name △	Version	Deployed Agents	Description	Deployment Requirements	Deploy	Undeploy
□	ibm_db2_database	3.1.1.0.0	1	IBM DB2 Database monitoring including reports	Requires network access and proper credentials to IBM DB2 ...		
□	juniper_netscreen_firewall	2.0.1.0.0	2	Juniper Netscreen Firewall monitoring including reports	Requires network access to firewall device. Refer to ...		
□	microsoft_iis	2.1.2.1.0	1	Management Plugin to define a 'Microsoft IIS 6.0' target ...	Requires netowrk access and credentials of the host where ...		
□	microsoft_sqlserver_database	4.0.3.0.0	1	Microsoft SQL Server monitoring (including reports) and ...	Requires network access and proper credentials to Microsoft ...		

12. To check the deployment status, go to Related Links and click the link **Deployment Status.**

Enabling and Finding TCP/IP Port Information

The following sections provide information you require to enable the TCP/IP port and to find the TCP/IP port for a particular SQL server instance.

Enabling TCP/IP Port

For SQL Server 2000

1. From the SQL Server Enterprise Manager, right-click the SQL Server instance in the left panel and select **Properties.** SQL Server Properties dialog box appears.
2. In General tab, click **Network Configuration.** The SQL Server Network Utility dialog box appears.
3. Ensure that TCP/IP is listed in the Enabled protocols list.

For SQL Server 2005 and SQL Server 2008

1. From the **SQL Server Configuration Manager,** select **SQL Server 2005 Network Configuration** in the left panel and navigate to the SQL Server instance.

   The right panel displays all protocols for the specified SQL Server instance and their status.
2. Ensure that TCP/IP is enabled.
3. (If TCP/IP is disabled), right-click **TCP/IP** and select **Properties.** The TCP/IP Properties dialog box appears.
4. In the Protocol tab, select **enabled,** and click **Apply.**
5. Restart the SQL Server instance.

Finding TCP/IP Port

After enabling the TCP/IP protocol, restart the SQL Server to apply the changes.

For SQL Server 2000

1. From the **SQL Server Enterprise Manager**, right-click the SQL Server instance in the left panel and select **Properties**. The SQL Server Properties dialog box appears.
2. In the **General** tab, click **Network Configuration**. The SQL Server Network Utility dialog box appears.
3. Select **TCP/IP**, click on the **Properties** dialog box to know the TCP/IP port.

For SQL Server 2005 and SQL Server 2008

1. From the **SQL Server Configuration Manager**, select **SQL Server 2005 Network Configuratio**n in the left panel and navigate to the SQL Server instance.

   The right panel displays all protocols for the specified SQL Server instance and their status.

   In the **IP Addresses** tab, TCP Dynamic Ports row of IP All will give the TCP/IP port of instance.

Enabling SQL Authentication or Mixed Authentication

Modify the permissions for database authentication so that you enable SQL authentication or mixed authentication, and set sysadmin role for the database user that you are going to use for discovering the target and running jobs.

On the SQL Server, for the user you are going to use for monitoring and running jobs, set the write permissions by following these steps:

> **Note:** If you do not have a user, then create one. To do so, from the task bar, go to Start, select **Settings**, and then **Control Panel**. In the Control Panel, double-click **Users and Passwords** and click **Add** in the Users tab.

1. In the Control Panel, double-click **Administrative Tools** and then **Computer Management.** The Computer Management screen appears.
2. In the left panel, go to Services and Applications and select the Microsoft SQL Server and navigate down to Security.
3. Double-click **Security**, and select **Logins.**
4. Right-click Logins and click NewLogin. The SQL Server Login Properties-New Login dialog box appears.
5. Click **General** tab, specify the name for the new login, select **SQL Server Authentication** and specify a unique password to use when connecting to the server using SQL Authentication.
6. Click **Server Roles** tab and ensure that **sysadmin** is selected in the Server Roles section.
7. Click **Database Access** tab, and ensure that in the Permit in Database Role section, no role is selected for any database.

Installing and Enabling Windows Management Instrumentation

(For SQL Server 2000) Install and enable Windows Management Instrumentation (WMI) provider of the SQL Server. Enable support by running the setup.exe file located in the SQL Server Installation CD:

```
<CD_Drive>/x86/other/wmi
```

Modifying Permissions

Modify Windows Management Instrumentation Control permissions, registry permissions, and DCOM remote access permissions as described in the section *Modifying Permissions* in the *Enterprise Manager System Monitoring Plug-in Troubleshooting Guide* available at the following location:

http://www.oracle.com/technology/documentation/oem.html

Adding Instances for Monitoring

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.

   Note: If you are performing a local monitoring of Microsoft SQL Server 2005 Cluster, then the Agent home page will be the Virtual Agent Service home page.

2. Provide the following information for the properties:

   - **Name** — Unique target name across all the Grid Control targets, such as SqlServer2k_Hostname. This is the display name in the Grid Control. It represents this SQL Server target across all user interfaces within Grid Control.
   - **JDBC URL** — URL for JDBC.

     For example,

     ```
     jdbc:sqlserver://<host>:<port>
     ```

- **JDBC Driver** — (Optional) Microsoft SQL Server 2005 JDBC driver class name.

  For example,

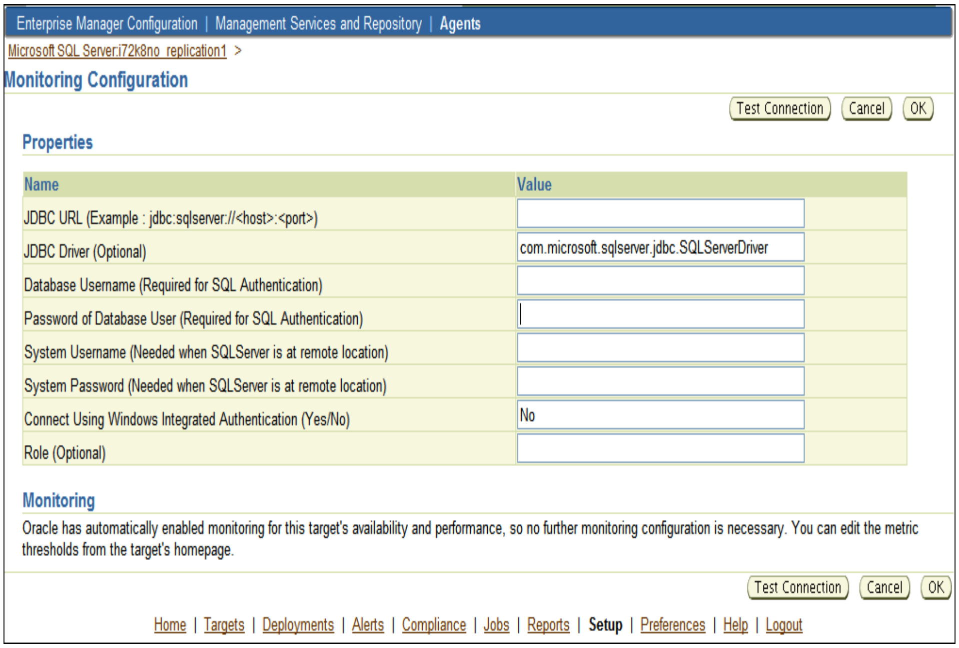
  ```
  com.microsoft.sqlserver.jdbc.SQLServerDriver
  ```

- **Database Username** (Required for SQL Authentication) — Valid user for the database in sysadmin fixed server role.
- **Password for the Database User** (Required for SQL Authentication) — Corresponding password for the database user
- **System Username** (Needed when SQLServer is at remote location) — Valid host user name. Required only for remote Agent monitoring. For more information, see Configuring Remote Connections to Monitor Targets.
- **System Password** (Needed when SQLServer is at remote location) — Password for the Username. Required only for remote Agent monitoring.
- **Connect Using Windows Integrated Authentication** (Yes/No) — Yes for Windows Integrated Authentication, No for SQL Authentication
- **Role** — (Optional)

3. Click Test Connection to make sure the parameters you entered are correct.
4. For Oracle Management Service version 10*g* Release 3 (10.2.0.3) or lower, reenter the encrypted parameters from step 2 if the connection test was successful, then click **OK**.

Note: For Oracle Management Service 10g Release 3 (10.2.0.3), if you do not reenter the encrypted parameters (*Database Username, Password for the Database User, System Username, System Password*) before clicking **OK**, you might encounter an error informing you that the login failed.

Figure 2 Add Microsoft SQL Server


Enterprise Manager Configuration | Management Services and Repository | Agents
Microsoft SQL Server:i72k8no_replication1 >
Test Connection
Cancel
OK

Monitoring Configuration

Properties

Name	Value
JDBC URL (Example : jdbc:sqlserver://<host>:<port>)	
JDBC Driver (Optional)	com.microsoft.sqlserver.jdbc.SQLServerDriver
Database Username (Required for SQL Authentication)	
Password of Database User (Required for SQL Authentication)	
System Username (Needed when SQLServer is at remote location)	
System Password (Needed when SQLServer is at remote location)	
Connect Using Windows Integrated Authentication (Yes/No)	No
Role (Optional)	

Monitoring

Oracle has automatically enabled monitoring for this target's availability and performance, so no further monitoring configuration is necessary. You can edit the metric thresholds from the target's homepage.

Test Connection
Cancel
OK
Home | Targets | Deployments | Alerts | Compliance | Jobs | Reports | Setup | Preferences | Help | Logout

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.

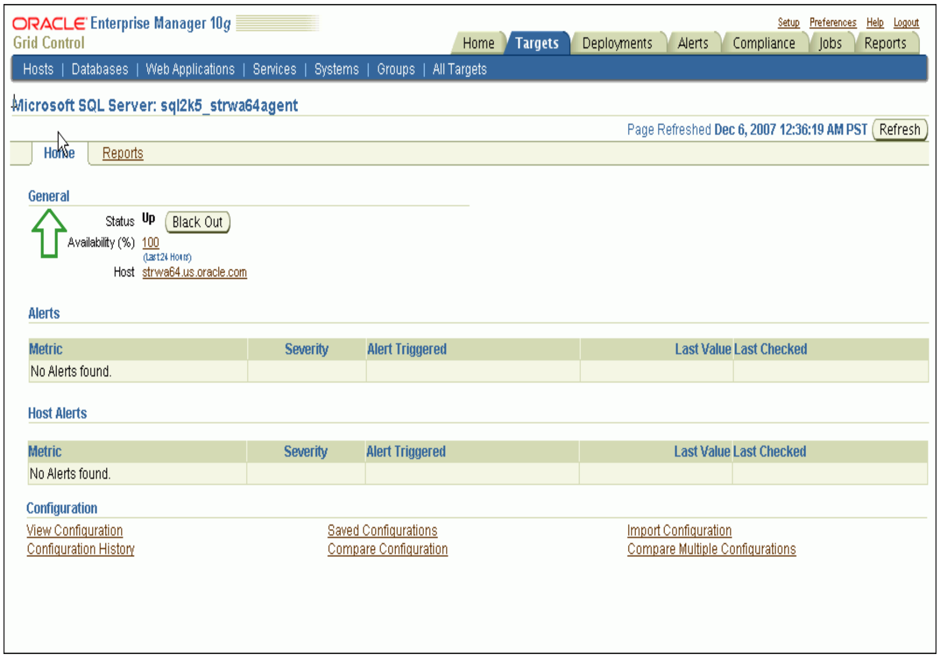
Verifying and Validating the Plug-in

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.

Figure 3   Microsoft SQL Server Home Page


ORACLE Enterprise Manager 10g
Grid Control
Setup Preferences Help Logout
Home
Targets
Deployments
Alerts
Compliance
Jobs
Reports
Hosts | Databases | Web Applications | Services | Systems | Groups | All Targets
Home
Reports
Refresh
Black Out

Microsoft SQL Server: sql2k5_strwa64agent

Page Refreshed Dec 6, 2007 12:36:19 AM PST

General

Status Up

Availability (%) 100 (Last 24 Hours)

Host strwa64.us.oracle.com

Alerts

Metric	Severity	Alert Triggered	Last Value	Last Checked
No Alerts found.				

Host Alerts

Metric	Severity	Alert Triggered	Last Value	Last Checked
No Alerts found.				

Configuration

View Configuration
Configuration History
Saved Configurations
Compare Configuration
Import Configuration
Compare Multiple Configurations

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.

Upgrading the Plug-in

Follow these steps to upgrade 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 that you have downloaded for upgrading.
6. Click **List Archive**.
7. Select the plug-in and click **OK.**
8. Verify that preferred credentials are set on all Agents to which you want to deploy the plug-in.

9. Blackout the Microsoft SQL Server targets for agents to which you want to deploy higher version of the plug-in. Ensure that you select immediate blackout.
10. 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.
11. 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.
12. 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.
13. Remove blackout for the targets (required only if Step 9 applies).

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 specific version 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**.

Configuring Connections

This section provides details about configuring connections for monitoring targets and executing jobs.

Configuring Remote Connections to Monitor Targets

If you want to monitor targets using remote Agents, then Oracle recommends that you do the following security configurations on every system where SQL Server target resides.

- Set WMI namespace security (Refer to the ’Modifying Windows Management Instrumentation Control Permissions’ section of the *Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide*.)
- Restrict access to the registry from a remote computer (Refer to the ’Modifying Registry Permissions’ section of the *Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide*.)
- Set DCOM Security to allow user to access remotely (Refer to the ’Modifying DCOM Remote Access Permissions’ section of the *Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide*.)
- Set privileges for System User to access Windows performance counters remotely as follows:

  1. Locally on the Microsoft Windows node hosting the Agent, open the **Local Security Settings** Windows Tool. Go to **Start**, select **Control Panel**, and then select **Administrative Tools**, select **Computer Management**, select **System Tools**, then **Local Users and Groups**, and select **Groups**.)
  2. Add System Username to **Performance Monitor Group**.

- Set access privileges of SQL Server Services to allow user to access a computer remotely (Refer to the ‘Modifying Access Privileges of SQL Server Services’ section of the *Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide*.)
- Set privileges for System User of target on Oracle Enterprise Manager Agent for Windows Integrated Authentication based monitoring.

  1. Locally on the Microsoft Windows node hosting the Agent, open the **Local Security Settings** Windows Tool. Go to **Start**, select **Control Panel**, and then select **Administrative Tools**, and select **Local Security Policy**.
  2. Click on **Local Policies** and then **User Rights Assignment**.
  3. Assign the following right to the System User of the target:

     ```
     Logon as batch job
     ```

- Configure **Allow Remote Administration Exception in Windows Firewall** if Windows firewall is enabled on the SQL Server target system.

  - Refer to the following link for steps to configure Windows firewall. Follow the steps that include using Group policy editor (Gpedit.msc).

    http://msdn.microsoft.com/en-us/library/aa389286(VS.85).aspx

Configuring Connections to Execute Jobs

If you want to execute jobs using local or remote Agents, then Oracle recommends that you do the following security configurations on every system where SQL Server target resides.

- Set WMI namespace security (Refer to the ’Modifying Windows Management Instrumentation Control Permissions’ section of the *Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide*.)
- Set DCOM Security to allow user to access a computer remotely (Refer to the ’Modifying DCOM Remote Access Permissions’ section of the *Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide*.)

For configuration details, refer to the following:

- Microsoft Help and Support Web site.

  To access the Web site, go to the following URL:

  `http://support.microsoft.com`

- *Oracle Enterprise Manager Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide* available at the following URL:

  `http://www.oracle.com/technology/documentation/oem.html`

- Document 367797.1 on *My Oracle Support*.

  To locate document 367797.1:

  1. Go to the following URL:

     `http://metalink.oracle.com`

  2. Click **Advanced** at the top of the Oracle *My Oracle Support* page.
  3. Enter 367797.1 in the **Document ID** field and click **Submit.**

Creating and Editing Jobs

To create and edit jobs, follow these steps:

> **Note:** Currently jobs are supported only for stand-alone Microsoft SQL Server instances. Jobs submitted for Microsoft SQL Server 2005 cluster instances will fail with the appropriate error message.

1. In Grid Control, click the **Jobs** tab. Grid Control displays the Job Activity page.
2. Select a job type from the **Create Job** menu and click **Go**.

   You can select one of these:

   - Microsoft SQL Server and/or SQL Agent Start
   - Microsoft SQL Server and/or SQL Agent Stop
   - Microsoft SQL Server Pause or Resume

   > **Note:** If you want to edit a job, then select an existing job from the list and click **Edit**.

3. In the **General** tab of the Create <*Job Type*> Job page, provide a name for the job and add the individual targets or one composite target such as a Group.

   > **Note:** If you are editing a job, then modify the job name and the selected targets.

4. In the **Parameters** tab of the Create <*Job Type*> Job page, from the **Options** menu, select an appropriate option to make the job function accordingly when it starts.

You can select one of these options:

Table 1 Job Parameters Options

Job Type	Available Options
Microsoft SQL Server and/or SQL Agent Start	■ Start SQL Server and SQL Server Agent services (You will select this option when both, SQL Server and SQL Server Agent, are stopped or when SQL Server is running but the SQL Server Agent is stopped) ■ Start SQL Server service (You will select this option when both, SQL Server and SQL Server Agent, are stopped and if you want to start only the SQL Sever)
Microsoft SQL Server and/or SQL Agent Stop	■ Stop SQL Server and SQL Server Agent services (You will select this option when both, SQL Server and SQL Server Agent, are running, when SQL Server is paused but the SQL Server Agent is running, when SQL Server is running/paused but the SQL Server Agent is stopped) ■ Stop SQL Server Agent service (You will select this option when you want to stop a running SQL Server Agent)
Microsoft SQL Server Pause or Resume	■ Pause SQL Server service (You will select this option when you want to pause a running SQL Server) ■ Resume SQL Server service (You will select this option when you want to resume a paused SQL Server)

Grid Control starts the SQL server and agent services according to the selection made.

Note: If you are editing a job, then modify the options for that job.

5. In the **Credentials** tab of the Create <*Job Type*> Job page, select an appropriate option for credentials.

   You can choose to use the preferred credentials that are already set or override the preferred credentials with new credentials. In either case, you need to provide the credentials for agent host and database host.

   To set the preferred credentials, click **Preferences** at the top-right corner of the Grid Control console. From the left-vertical navigation bar, click **Preferred Credentials**. Grid Control displays the Preferred Credentials page. On this page, you can set the preferred credentials

   Note: If you are editing a job, then modify the credentials set for that job.

6. In the **Schedule** tab of the Create <*Job Type*> Job page, schedule the job.

7. In the **Access tab** of the Create <*Job Type*> Job page, define or modify the access you want other users to have to this job.

   Note: If you want to edit, then modify the access levels for that job.

8. Click **Submit** to create the job.

Troubleshooting the Plug-In

To resolve various issues that you might encounter while using the plug-in, see the *Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide* available at the following URL:

`http://www.oracle.com/technology/documentation/oem.html`

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. 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.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at `http://www.fcc.gov/cgb/consumerfacts/trs.html`, and a list of phone numbers is available at `http://www.fcc.gov/cgb/dro/trsphonebk.html`.

System Monitoring Plug-in Installation Guide for Microsoft SQL Server, Release 11 (4.1.3.1.0)
E16546-03