Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for Microsoft SQL Server

Release 12.1.0.2.0 for Windows

E35211-05

September 2012

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 Cloud Control 12*c* to add support for managing Microsoft SQL Server instances. By deploying the plug-in within your Cloud 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 Cloud Control 12*c* Release 1 (12.1.0.2.0) or higher *(Oracle Management Service and Oracle Management Agent)*
- 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
  - Microsoft SQL Server 2008 R2 (32-bit)
  - Microsoft SQL Server 2008 R2 (64-bit) running on x64

- Microsoft SQL Server 2008 R2 Cluster: Active/Active and Active/Passive

Prerequisites

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

- Install the following:

  Enterprise Manager Cloud Control 12*c* Release 1 (12.1.0.2.0) or higher (Oracle Management Service and Oracle Management Agent)

- 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 Oracle Management Agent running on 64-bit Windows operating system, do the following:

  - Depending on the JVM version, copy the respective version of the `sqljdbc_auth.dll` file to the following location:

    ```
    Drive:\<agent_base>\agent\plugins\oracle.em.smss.agent.plugin_
    12.1.0.2.0\depen dencies\oracle.em.smss\jdbcdriver
    ```

    If the directory does not exist, then create it. The `sqljdbc_auth.dll` file 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 Oracle Management 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 Oracle Management 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 Oracle Management 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 Cloud 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 Agent running on Microsoft Windows) The OS privileges for the user (set in the Preferred Credentials for the Agent) must meet the requirements documented in the "*Setting Credentials for the Job System to Work with Enterprise Manager*" section of the *Oracle Database Installation Guide for Microsoft Windows* available at:

  - **Oracle Database 11g Release 2 (11.2)**

    `http://www.oracle.com/pls/db112/portal.portal_db?selected=11&frame=#microsoft_windows_installation_guides`

    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-sysadmin 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.

Deploying the Plug-in

See the *Plug-in Manager* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to deploy the plug-in:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mngr.htm

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.

> **See Also:**
>
> http://msdn2.microsoft.com/en-us/library/aa933458(SQL.80).aspx

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
```

Adding Instances for Monitoring

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

1. From the **Setup** menu, select **Add Target** and then **Add Targets Manually**.

2. In the Add Targets Manually page, select **Add Non-Host Targets by Specifying Target Monitoring Properties**, select **Target Type** as **Microsoft SQL Server**, select a **Monitoring Agent** and click **Add Manually**.

   In the Add Microsoft SQL Server page, provide the following information for the properties

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

     For example,

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

     Note: You can specify either IP Address or host name. However, 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. Also, if you are monitoring a Microsoft SQL Server 2005 Cluster, then specify the IP address or host name of the virtual SQL Server of the cluster.

   - **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.

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 Microsoft SQL Server target link from the All Targets page. The Microsoft SQL Server home page appears.
2. Verify that no metric collection errors are reported by clicking **Monitoring** and then **Metric Collection Errors** from the **Target** menu.
3. Ensure that reports can be seen and no errors are reported by clicking **Information Publisher Reports** in the **Target** menu and viewing reports for the Microsoft SQL Server target type.
4. Ensure that configuration data can be seen by clicking **Configuration** and then **Last Collected** in the **Target** menu. If configuration data does not immediately appear, click **Refresh** in the Latest Configuration page.

Undeploying the Plug-in

See the *Plug-in Manager* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to undeploy the plug-in:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mngr.htm

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.
- Restrict access to the registry from a remote computer.
- Set DCOM Security to allow user to access remotely.
- 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.
- Set privileges for System User of target on Oracle Management 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.
- Set DCOM Security to allow user to access a computer remotely.

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`

- Document 367797.1 on *My Oracle Support*:

  `https://support.oracle.com`

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 Enterprise Manager Cloud Control 12*c*, click **Enterprise**, then **Job**, then click **Activity**.
2. On the Job Activity page, select a job type from the **Create Job** menu and click **Go**.

   Select one of the following:

   - 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)

   Cloud 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 Cloud Control console. From the left-vertical navigation bar, click **Preferred Credentials**. Cloud 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.

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

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

System Monitoring Plug-in Installation Guide for Microsoft SQL Server, Release 12.1.0.2.0 for Windows
E35211-05