Oracle® Enterprise Manager

System Monitoring Plug-in Troubleshooting Guide

Release 12 (12.0)

E10314-11

November 2010

This document provides various troubleshooting scenarios that you might encounter while working with Oracle Enterprise Manager System Monitoring Plug-ins.

1 Troubleshooting Common Issues for All Plug-Ins

The following sections provide common troubleshooting scenarios related to all plug-ins.

1.1 Installation and Deployment Issues

This section addresses installation and deployment issues.

1.1.1 Preferred Credentials Not Set

You might encounter the following error if you have not set the preferred credentials when you attempt to undeploy the plug-in:

```
The preferred credentials are not set for host
```

Possible Cause— Preferred credentials are not set for the host. It is mandatory to set preferred credentials on all Agents where you want to deploy the plug-in.

Action— Do the following:

1. From the 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 Host Target Type, enter the normal user name and password and click **Test** to ensure that the entered values are valid. If the Test returns successful, then click **Apply**.

    Enter the same user name and password for the Agent Target Type for this host.

4. In the page that appears, set the credentials.

1.1.2 Preferred Credentials Error

You might encounter this error while deploying the plug-in leading to a deployment failure.

Possible Cause— The Domain User set in the Management Agent service properties to start the service does not have required privileges.

ORACLE®

Action— Do the following:

1. Locally on the Windows node hosting the Management Agent, check that the user starting the Management 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 Management 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 Management Agent service if it is running.

4. Set the Preferred Credentials for the Management Agent in the Grid Control.

5. Deploy the plug-in and discover the instances.

To verify the preferred credentials, do the following:

1. Validate the credentials set in the Host and Cluster Preferred Credentials page.

   a. Log in to Enterprise Manager Grid Control.

   b. Click **Preferences** from the top-right corner of the page.

   c. From the left menu bar, click **Preferred Credentials**.

   d. In the Preferred Credentials page, in the table, for the Host target type, from the **Set Credentials** column, click the icon.

   e. 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, and click **Test**. If you test runs successfully, your credentials are set correctly.

2. Run the OS Command job for the Management Agent where the plug-in has to be deployed.

   a. Log in to Enterprise Manager Grid Control.

   b. Click the **Jobs** tab.

   c. In the Job Activity page, from the **Create Job** list, select OS Command, and click **Go**.

   d. 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.

1.2 Failure in loading Classpath: Could not create instance : <JDBC DRIVER>

Possible Cause— The JDBC Driver Name in target properties or/and the JDBC Driver in Agent's classpath.lst file is/are incorrect.

Action— Do the following:

- Specify the correct JDBC Driver Name in target properties

- Specify the correct path of JDBC Driver in Agent's classpath.lst file

2 Troubleshooting Microsoft SQL Server Plug-In

The following sections provide troubleshooting scenarios related to Microsoft SQL Server plug-in.

2.1 How To Diagnose

The following sections help you diagnose issues that you may encounter while working with the Microsoft SQL Server plug-in.

2.1.1 Diagnostic Tools

This section provides details of the diagnostic tools.

2.1.1.1 WBEMTEST

This tool is available on Windows OS and is packaged along with the OS.

To launch the tool, go to the Start menu, click **Run,** and in the open field, enter `WBEMTEST,` and click **OK.**

Example 1

To check whether the WMI calls are working correctly for the namespace `root\cimv2` outside the Enterprise Manager environment,

> **Note:** You must be logged in as a user belonging to the local Administrators Group. Preferably, this should be a domain account.

1. Launch WBEMTEST locally on the system where SQL Server is installed.
2. Click **Connect.**
3. Provide `root\cimv2` in the `Server\Namespace` text field.
4. Click **Login.**
5. Click **Query** (which is now enabled).
6. Enter the following query and click **Apply.**

   ```
   select * from win32_service
   ```

Example 2

Applicable for Microsoft SQL Server 2000: To check whether the WMI calls are working correctly for the namespace `root\MicrosoftSQLServer` outside the Enterprise Manager environment,

> **Note:** You must be logged in as a user belonging to the local Administrators Group. Preferably, this should be a domain account.

1. Launch WBEMTEST locally on the system where SQL Server is installed.
2. Click **Connect.**

3. Provide `root\MicrosoftSQLServer` in the `Server\Namespace` text field.

4. Click **Login.**

5. Click **Query** (which is now enabled).

6. Enter the following query and click **Apply**:

   ```
   select name, clustered, package, versionstring from
   mssql_sqlserver
   ```

   > **Note:** Example 2 applies only to SQL server 2000.

Example 3

To check whether WMI calls are working correctly for the name space `root\default` outside the Oracle Enterprise Manager environment.

> **Note:** You must be logged in as a user belonging to the local Administrators Group. Preferably, this should be a domain account.

1. Launch WBEMTEST locally on the system where SQL Server is installed.

2. Click **Connect**.

3. Provide `root\default` in the **Server\Namespace** text field.

4. Click **Execute Method**.

5. Enter `stdRegProv` in the object path.

6. Select `getStringValue` from the **Method** drop-down list.

7. Click **Edit in Parameters**.

8. Select the property `sSubKeyName` and then click **Add Property**.

9. Specify the value. For example:

   For SQL Server default (no-name) instance:

   ```
   SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\CurrentVersion
   ```

   For SQL Server non-default instance:

   ```
   SOFTWARE\Microsoft\MicrosoftSQLServer\<DATA_
   ROOT>\MSSQLServer\CurrentVersion
   ```

   Where <DATAROOT> will have values such as MSSQL.1, MSSQL.2, and so on.

10. Select the property `sSubkeyValue` and then click **Add Property**.

11. Specify the value. For example, `CurrentVersion`.

12. Click **Save Object**.

13. Click **Execute**.

14. A pop-up with message *'Successfully Executed'* is displayed. Click **Edit Out Parameters**. Verify the value of `sValueName`.

2.1.1.2 CIM Studio

To use CIM Studio, you require `Wmitools.exe`.

To download, go to the following URL:

`http://www.microsoft.com/downloads/details.aspx?familyid=643`
`0f853-1120-48db-8cc5-f2abdc3ed314&displaylang=en`

Example 1

1. Install WMI CIM Studio.

2. From Windows Start menu, launch WMI CIM Studio (from Start menu, select **Programs**, **WMI Tools** and then **WMI CIM Studio**).

    Connect to namespace dialog box appears.

3. Specify the required name space, for example `root\CIMV2`.

    > **Note:** WMI CIM Studio can be launched using Internet Explorer. Ensure that you have disabled the pop-up blocker.

4. Click **OK.**

5. In the screen that appears, click the search icon (search for class) in the left pane and enter `win32_service` in the text-field.

6. Click **GO.**

    This lists all the classes that contains `win32_service` string. If not, it indicates that there are issues with WMI installation.

7. Select `win32_service` from the search results and click **OK.**

8. Click WQL queries icon in the right pane.

9. In the Query dialog box, enter `select * from win32_service` in the Query text box and click **Execute.**

    This lists all services running on the system.

Example 2

1. Specify the required name space `root\MicrosoftSQLServer`.

    > **Note:** WMI CIM Studio can be launched using Internet Explorer. Ensure that you have disabled the pop-up blocker.

2. Click **OK**.

3. In the screen that appears, click the Search icon (search for class) in the left pane and enter `mssql_sqlserver` in the text field.

4. Click **Go**.

    This lists all the classes that contains `mssql_sqlserver` string. If not, it indicates that there are issues with WMI installation.

5. Select `mssql_sqlserver` from the search results and click **OK**.

6. Click WQL queries icon in the right pane.

7. In the Query dialog box, enter `select * from mssql_sqlserver` in the Query text box and click **Execute**.

> **Note:** This is applicable only for Microsoft SQL Server 2000.

2.1.1.3 SQL Server Enterprise Manager

This tool is packaged along with Microsoft SQL Server.

For diagnosis using SQL Server Enterprise Manager:

1. From the Start menu, select **All Programs, SQL Server, Enterprise Manager** and then **SQL Query Analyzer.**

2. Connect to the database instance.

2.1.2 Diagnostic Steps

To monitor a Microsoft SQL Server target, you need to go through 4 phases:

- **Phase 1—** Import the Plug-in on Enterprise Manager Grid Control. See also "Phase 1 Checklist".

- **Phase 2—** Deploy the Plug-in to the Central Agent that will monitor the SQL Server target(s). See also "Phase 2 Checklist".

- **Phase 3—** Discover the SQL Server targets. See also "Phase 3 Checklist".

- **Phase 4—** Ensure that various features for monitoring the discovered SQL Server target are available and display the right behavior. See also "Phase 4 Checklist".

Phase 1 Checklist

Before importing SQL Server Plug-in into Enterprise Manager Grid Control, go to My Oracle Support and review the Certification Note 412431.1 to check which release of the SQL Server Plug-in is certified with which release of:

- Grid Control OMS/Agent

- Microsoft SQL Server

Phase 2 Checklist

(For Microsoft SQL Server 2000 only)

Before deploying the Plug-in to the Central Agent, ensure that Windows Management Instrumentation (WMI) setup.exe was successfully installed.

Ensure that the namespace `root\MicrosoftSQLServer` is present and check if

- Service WMI is up and running (From **Start** menu, go to **Control Panel**, and then **Services** to verify).

- WMI calls (for root/cimv2 and root/MicrosoftSQLServer) work effectively outside the Management Agent. Use any of the Microsoft Diagnostic Tools documented in Section 2.1.1, "Diagnostic Tools".

- Also, ensure that JDBC calls work effectively outside the Management Agent.

Phase 3 Checklist
Verify the following:

Before discovering SQL Server targets, ensure that you meet all discovery-related pre-requisites. The checklist to follow is:

- Preferred Credentials have been set in Grid Control for the Central Agent which monitors the SQL Server instances and for the host on which the Central Agent is running.

- **(For Release 1 or Release 2 of the Plug-in only)** Verify the exact name of the SQL Server Host and the SQL Server instance from the SQL Server Enterprise Manager.

- Check that TCP/IP is enabled and verify the TCP/IP port. For details, Section 2.2.2, "Enabling TCP/IP Port" and Section 2.1.3, "Finding TCP/IP Port".

- If the target is remote, necessary configuration for remote connection must be done as a pre-requisite.

Phase 4 Checklist

For monitoring of SQL Server targets to occur ensure that you meet the following conditions:

1. The SQL Server instance has been successfully discovered.

   To do this:

   1. In the Enterprise Manager Grid Control, click **Targets.**

   2. In All Targets page, enter `Microsoft SQL Server` in Search, and then click **Go.**

   3. Verify if SQL Server instance you added is listed.

      Click the SQL Server name for details

2. Check if the status of the SQL Server Instance is correct.

   To do this:

   1. Go to SQL Server Instance Home page.

   2. Verify the status.

      Ensure that the status is not `Pending`.

3. In the Alerts page, ensure that SQL Server instance is not listed in the Unknown Availability section.

4. In the Alerts page, ensure that there are no errors listed in the Errors section for SQL Server instance.

5. In the SQL Server Instance Home page, ensure that in All Metrics section, date and timestamp is displayed in the column Last Upload.

> **Note:**
>
> - Wait for the Schedule Interval (this can be 24 hours) to check that a specific metric is collected.
>
> - Some metrics might not be collected (for example, Backups or Jobs if no backup and no job were ever run for that SQL Server instance).
>
> - Some metrics might not be collected depending on the release of the Microsoft SQL Server or if some Windows services are not started (for example, the SQL Server Agent)

6. In the SQL Server instance Home Page, go to Reports section and check if all the reports are available in the List View Reports.

> **Note:** Some reports might be empty or might display `No data found.`
>
> In this case, check that the Schedule Interval of the corresponding metric and wait for the Schedule Interval.

2.1.3 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.

2.1.4 Microsoft URL for WMI Errors

To get a list of WMI Return Codes, go to the following Microsoft URL:

http://msdn2.microsoft.com/en-us/library/aa394559.aspx

2.2 How To Fix

The following sections help you fix issues that you may encounter while working with the Microsoft SQL Server plug-in.

2.2.1 Downloading the Latest Version of the Plug-in

Download the latest version of the plug-in from Oracle Technology Network (OTN) using the following URL:

```
http://www.oracle.com/technology/software/htdocs/devlic.html
?url=http://www.oracle.com/technology/software/products/oem/
htdocs/plugin-ms_sql.html
```

2.2.2 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

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.

2.2.3 Modifying Permissions

The following sections only provide steps to modify various permissions. For detailed documentation on any of these procedures, refer to Microsoft Web site.

2.2.3.1 Modifying Windows Management Instrumentation Control Permissions

For a secure Windows Management Instrumentation (WMI) namespace access, modify WMI Control Permissions for System or Job Username.

To do this, on the SQL Server, for the user you are going to use for monitoring and executing 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 **WMI Control.**

3. Right-click **WMI Control** and select **Properties.**

   The WMI Control Properties dialog box appears.

4. In the Security tab, go to the namespace navigation panel, double-click **Root,** select **CIMV2,** and click **Security.**

5. Click **Add** and select the specified user (or group) from the Select Users, Computers, or Groups dialog box.

6. In the WMI Control Properties dialog box, select the specified user (or group) under Name.

7. In the Permissions section, under Allow, check **Enable Account** and **Remote Enable.** Uncheck the remaining options.

   > **Note:** To execute jobs, ensure that you check **Execute Method** in addition to **Enable Account** and **Remote Enable**.

8. Go to WMI Control Properties dialog box and repeat the steps from 5 to 9 for Microsoft SQL Server (double-click **Root** and select **Microsoft SQL Server**) and Computer Management (double-click **Root, Microsoft,** and then select **ComputerManagement**).

   See Also:

   http://www.microsoft.com/technet/scriptcenter/resour
   ces/wmifaq.mspx#EABAC

2.2.3.2 Modifying Registry Permissions

For a secure registry access, modify WMI and registry permissions for System Username. To do this, follow the procedures given below.

WMI Modifications

To do this, on the SQL Server, for the user you are going to use for monitoring and executing 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 **WMI Control.**

3. Right-click **WMI Control** and select **Properties.**

   The WMI Control Properties dialog box appears.

4. In the Security tab, go to the namespace navigation panel, double-click **Root,** select **DEFAULT,** and click **Security.**

5. Click **Add** and select the specified user (or group) from the Select Users, Computers, or Groups dialog box.

6. In the WMI Control Properties dialog box, select the specified user (or group) under Name.

7. In the Permissions section, under Allow, check **Execute Methods, Enable Account**, and **Remote Enable.** Uncheck remaining options.

Registry Editor Modifications

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

2. Type `regedt32.exe` in the Open field.

3. Click **OK.**

   The Registry Editor appears.

4. In the left panel, navigate down to Microsoft SQL Server by double-clicking **HKEY_LOCAL_MACHINE, SOFTWARE,** and then **Microsoft.**

5. Select **Microsoft SQL Server,** go to the Registry Editor main menu and click **Security** and then **Permissions.** The Permissions for Microsoft dialog box appears.

6. Click **Add** and select the specified user (or group) from the Select Users, Computers, or Groups dialog box.

7. In the Permissions for Microsoft dialog box, select the specified user (or group) under Name.

8. In the Permissions section, under Allow, check **Read.** Uncheck the remaining options.

9. Repeat the steps from step 5 to 8 after selecting **MSSQLServer**, if the SQL Server target to be monitored is the default (no-name) instance.

   > **Note:** If a 32-bit version of SQL Server is installed on a 64-bit system (Xeon or AMD), the key in step 5 above will be HKEY_LOCAL_ MACHINE\SOFTWARE\Wow6432Node\Microsoft\Microsoft SQL Server. Similarly, the key mentioned in step 9 will be HKEY_LOCAL_ MACHINE\SOFTWARE\Wow6432Node\Microsoft\MSSQLServer (if the SQL Server target to be monitored is the default (no-name) instance).

   > **See Also:** http://support.microsoft.com/kb/153183

2.2.3.3 Modifying Permissions for Database Authentication

To do this, on the SQL Server, for the user you are going to use for monitoring and executing 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

2.2.3.4 Assigning User Rights

The OS privileges for the user (set in the Preferred Credentials for the Agent) should 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

2.2.3.5 Modifying DCOM Remote Access Permissions

1. Click **Start**, click **Run**, type **DCOMCNFG**, and then click **OK**.

2. In the **Component Services** window, expand **Component Services**, expand **Computers**, and then right-click **My Computer** and click **Properties**.

3. In the **My Computer Properties** window, click the **COM Security** tab.

4. Under **Launch and Activation Permissions**, click **Edit Limits**.

5. In the **Launch Permission** dialog box, follow these steps if your name or group does not appear in the Groups or User Names list:

   a. In the **Launch Permission** dialog box, click **Add**.

   b. In the **Select Users, Computers, or Groups** dialog box, add your name and the group in the **Enter the object names to select** field, and then click **OK**.

   c. In the **Launch Permission** dialog box, select your user and group in the **Group or User Names** field. In the **Allow** column under **Permissions for User**, select **Remote Launch** and select **Remote Activation**, and then click **OK**.

For more information about modifying DCOM settings and securing a remote WMI connection, refer to the following URL:

http://msdn2.microsoft.com/en-us/library/aa393266.aspx

2.2.3.6 Modifying Access Privileges of SQL Server Services

> **Note:** Execute the following commands only if the Windows box in which SQL Server resides, is Windows 2003 SP1 or later.

Follow these steps to modify access privileges of SLQL Server services:

1. Grant authenticated users the right to remotely access Service Control Manager:

   a. Click **Start**, click **Run**, type cmd, and then click **OK**.

   b. Type the following command at the command prompt, and then press **Enter**:

   ```
   sc sdset SCMANAGER
   D:(A;;CCLCRPRC;;;AU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)S:(AU;FA;KA;;;WD)
   (AU;OIIOFA;GA;;;WD)
   ```

   For more information, see
   http://support.microsoft.com/kb/907460/.

2. Assign Access right to SQL Server Services:

   a. Click **Start**, click **Run**, type cmd, and then click **OK**.

   b. Type the following command at the command prompt, and then press **Enter**:

   c. Check the AU (Authenticated Users) access privileges in the output. For example, the default value is:

   ```
   D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;
   ;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CR;;;AU)(A;;CCLCSWRPWPDT
   ```

```
LOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

The above output lists CR (Control Access) privilege for Authenticated Users (A;;CR;;;AU).

d. If the privileges for AU (Authenticated Users) are not same as (A;;CCLCSWRPWPDTLOCRRC;;;AU), set it using the following command by replacing (A;;CR;;;AU) with (A;;CCLCSWRPWPDTLOCRRC;;;AU):

```
sc sdset SQLServer_service_name
D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;
;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;AU)
(A;;CCLCSWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

Repeat steps (a) to (c) for SQLServer Agent service also, by replacing SQLServer_service_name in step (a) with the SQLServer_agent_service_ name.

For more information, see the following links:

http://msdn.microsoft.com/en-us/library/aa379570%28VS.85%29.aspx

http://msdn.microsoft.com/en-us/library/aa374928%28VS.85%29.aspx

http://msdn.microsoft.com/en-us/library/aa379602%28VS.85%29.aspx

2.3 General Issues

The following sections list the general issues and workarounds, if any, that can be used to resolve the issues that you may encounter while working with the Microsoft SQL Server plug-in.

2.3.1 Monitoring Issues

This section addresses monitoring issues.

2.3.1.1   DLL file $AgentHome\sysman\jdbcdriver\ sqljdbc_auth.dll is found missing or was never copied manually. Please copy AMD64 version of sqljdbc_auth.dll at the above location and re-try.

Possible Cause — 64-bit version of sqljdbc_auth.dll is either missing or not copied manually in the specified directory

Action— Download Type 4 Microsoft SQL Server 2005 JDBC Driver version 1.2 and copy the X64 version of sqljdbc_auth.dll to $Agent_ home\sysman\jdbcdriver directory. 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)

2.3.1.2   DLL file $AgentHome\sysman\jdbcdriver\ sqljdbc_auth.dll is found missing or was never copied manually. Please copy IA64 version of sqljdbc_ auth.dll at the above location and re-try.

Possible Cause — 64-bit version of `sqljdbc_auth.dll` is either missing or not copied manually in the specified directory

Action— Download Type 4 Microsoft SQL Server 2005 JDBC Driver version 1.2 and copy the IA64 version of `sqljdbc_auth.dll` to `$Agent_home\sysman\jdbcdriver` directory. 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`)

2.3.1.3 Error: Bad arg length for Socket::inet_ntoa, length is 0, should be 4

Possible Cause — DNS resolution has failed. This may be due to incorrect host name specified in the JDBC URL field, failed attempts to contact DNS server, or "down" status of the DNS server.

Action— Check `ping` and `nslookup` for the host name specified in the JDBC URL field. If these commands fail, then include the IP address in the JDBC URL field, instead of host name, and check the behavior.

2.3.1.4 Error: Error in adding target - _Wbem_Remote_Determination_ DynamicProperty - Couldn't determine the IP address of the SQL Server Host. Possible reasons are - Host Name or IP address provided in the JDBC URL is not correct - Domain Name Server (DNS) is down or Domain Name resolution failed. Please contact your system/network administrator to resolve the DNS configuration.

Possible Cause — DNS resolution has failed. This may be due to incorrect host name specified in the JDBC URL field, failed attempts to contact DNS server, or "down" status of the DNS server.

Action— Check ping and nslookup of the SQL Server target host machine (provided in the JDBC URL) field from the Enterprise Manager Agent system.

2.3.1.5 Error: 0x80041010

Possible Cause — WMI repository is not up-to-date. As the class is part of root\cimv2 namespace, it should be available as part of default WMI installation.

Action— Do the following:

1. At command prompt, repeat running the following command twice or thrice in sequence:

   ```
   wmiadap /f
   ```

   ```
   wmiadap /resyncperf
   ```

2. Restart Windows Management Instrumentation service.

> **Note:** This applies only if you use SQL Server plug-in version 3.0.2.0.0 or higher.

> **Note:** When this error is found for a 32-bit version of SQL Server installed on 64-bit system, instead of using the default `wmiadap` executable, look for the `wmiadap` executable under `<WINDOWS_ROOT>\SysWOW64`, for example, C:\WINDOWS\SysWOW64. Run this copy of `wmiadap.exe` with the options mentioned above.

2.3.1.6 Target is In Broken State: Metric Collection Errors Encountered

> **Note:** This bug has been fixed for Oracle Enterprise Manager Agent version 10.2.0.3 and higher. You might encounter this issue only for Agent versions lower than 10.2.0.3.

Cause — This behavior occurs when target, agent, or both and/or target system become slow or heavily loaded and computation of dynamic properties take longer than the default timeout value.

Workaround — Execute the following command:

```
emctl reload agent dynamicproperties <target name>:<target type>
```

OR

You can alternatively resubmit the target instance properties:

1. Click on the Monitoring Configuration link (under the Related Links section on the plug-in target home page).

2. Re-enter the encrypted properties.

3. Click **OK.**

2.3.2 Test Connection
This section addresses the test connection issues.

2.3.2.1 General Test Connection Issues

This section addresses general test connection issues.

Error: Missing Properties or WMI Error (with error code)
This may be any of the following:

- Missing Properties : [STDINWBEM_HOST]

- Missing Properties Error [servername_from_jdbc]

- Missing Properties : [version]

- Error 0x80007005

- Error 0x80041003

Possible Cause — This may be seen when the Management Agent encounters an error while computing any of the Dynamic Properties. To verify the behavior of the computation of Dynamic Properties, try **Test Connection**. You can try the connection from either the Add Target page (if the target is not already added) or the Target Home page (from the **Related Links** section, click **Monitoring Configuration**).

The reason for the failure in Dynamic Property computation may be because the Management Agent process owner and/or the provided System User Name (*if the target is on a remote location that is different from the host where the Management Agent is running*) do not have adequate privileges and permissions to monitor these targets.

Action — The Dynamic Property computation error needs to be resolved. Details on how to resolve the issue are mentioned below:

- If you tested the connection, then after successful testing of the connection, re-enter the password details. On the refreshed page, the password fields may show some encrypted values but those are incorrect values, as the credentials are not cached. So re-enter the passwords and then click **OK**.

- To check whether the user has adequate privileges, try out a test connection using WBEMTEST or CIM Studio. Test the connection by executing queries using these tools from the agent machine to the local or remote target machine.

  A failure or error message while connecting to the namespaces `root\default, root\cimv2`

  and/or

  `root\MicrosoftSQLServer` (in the case of SQL Server 2000) helps to find the exact problem.

  After confirming this, modify the permissions so that you can add targets. For instructions to modify permissions, refer to Section 2.2.3, "Modifying Permissions".

  However, if you do not see any error in the connection (or while running the query) through WBEMTEST for `root\cimv2` or `root\MicrosoftSQLServer` (only in the case of SQL Server 2000) namespaces, then check the owner of the Management Agent process and the user that you logged in as and ran the WBEMTEST query. If the above two are not the same, then change the owner of the Management Agent process to the same user that ran the query through WBEMTEST (preferably, this should be a domain account) and check the behavior of the plug-in target or Test Connection.

- Check the server name retrieved with JDBC is null. A null value makes the discovery fail.

  Action— Refer to the related article on Microsoft Website:

  http://support.microsoft.com/kb/303774/

  The article 303774 documents the Microsoft bug 354825 and states how the servername can be NULL and how to fix the issue.

  > **Important:** Contact Microsoft Support before applying the steps provided at the above URL.

Error: The host name/ IP address specified in JDBC URL is of Oracle Enterprise Manager Agent system. However, System Username is specified. For a SQL Server target on the same box as OEM Agent, System Username should not be specified.

Possible Cause — In case of Local Monitoring scenario, System User is specified in the System User Name field while adding target.

Action — Remove the System User Name from the System User Name field and re-try.

Error: Failed to connect, Network Error. Possible reasons are: Either JDBC URL is wrongly formed or one of its parameters are wrong

Possible Cause — Incorrect host name in the JDBC URL

Action — Provide the correct SQL Server hostname in the JDBC URL and re-try.

Error : Failed to connect, Login Failure. Possible reasons are: Encrypted properties are not provided. Provided Database Username or Password or both are not correct. Provided Database User may not exist. Login failed for user 'sa'.

Possible Cause —Incorrect credentials (Database Username or Database Password) for the Database user

Action — Provide the correct credentials.

Error: Failed to connect, The TCP/IP connection to the host has failed. java.net.ConnectException: Connection refused: connect

Possible Cause — The following could be one of the causes:

- TCP/IP port and/or Hostname may be wrong

- TCP/IP port may not be enabled

- SQL Server is not running

Action — Check the correct port number for the target. For information about checking the port number, see Enabling TCP/IP Port.

Error: Cannot find the key : SOFTWARE\Microsoft\Microsoft SQL Server\SQLSRVR_ 2000\MSSQLServer\CurrentVersion\\CurrentVersion. Could not connect. Error code = 0x80041003 em_error=Failed while connecting to WMI.

Possible Cause — Following could be the causes of this error:

- System user does not have the privilege to access the particular registry key

- The registry key does not exist.

Action — Assign Read permission to the registry key(s) as documented. Replace permission entries on all child objects in the Advanced mode.

Error: MSSQL_NumClusterNodes - Error Querying: The user does not have permission to perform this action.

Possible Cause — Database User specified does not have privilege/role to the SQL Server instance.

Action — Assign sysadmin server role to the Database User as mentioned in the above article.

2.3.2.2 JDBC Test Connection Issues

This section addresses JDBC-related test connection issues.

No Owner for One or More Databases

When you do a test connection, you might encounter this error while adding the target.

Possible Cause: There is no owner for one or more databases in the SQL Server instance.

Action: Do the following:

1. Ensure that the output of the following are same:

   - Output of the query `select @@servername` when ran from Microsoft Query Analyzer tool (after connecting to the database)

   - The following registry key from the SQL Server target system

     `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server`

     Note: If 32-bit version of SQL Server is installed on 64-bit system, the registry key to be checked on the SQL Server target system is `HKEY_ LOCAL_ MACHINE\SOFTWARE\Wow6432Node\Microsoft\Microsoft SQL Server`.

     ---

2. Using Microsoft SQL Query Analyzer:

   a. Check if `exec master.dbo.sysdatabases` gives the same error.

   b. See if you find NULL value for the second column for query `select name, suser_sname(sid) from master.dbo.sysdatabases`.

   c. Run the following command for all the database for which the second column is found NULL:

      `* *Use <database_name>`

      `* *exec sp_changedbowner *username*`

      The *username* can be the name of any database owner.

   d. Rerun the following query:

      `select name, suser_sname(sid) from master.dbo.sysdatabases`

      Now, you should not find the value in the second column NULL.

   e. Run the following query and ensure that the error is rectified:

      `exec master.dbo.sysdatabases`

Error While Obtaining Connection

Possible Cause — The port number provided is wrong.

Action — Provide the correct port number for the target. See Section 2.1.3, "Finding TCP/IP Port" for details.

JDBC Connection Fails

If the JDBC connection fails, ensure the following:

- The specified user exists in the Manage Logins dialog box for the SQL Server instance.

- The user has the sysadmin fixed server role.

- The SQL Server Authentication method is enabled for the particular instance.

- The query select @@servername, @@servicename is not returning a NULL value for the SQL Server instance.

Error : Metric collection error :" The server principal "<username>" is not able to access the database "<dbname>" under the current security context......"

Action — Provide access to that database for the login user.

Error while obtaining connection.[Microsoft][SQLServer 2000 Driver for JDBC]Error Establishing Socket or Failed to Connect.

Possible Cause — The reason can be one of these:

- Incorrect port with correct host name

- Incorrect host name with correct port

- Incorrect port and host name

- SQL Server is not running

- TCP/IP port is not enabled on SQL Server instance

Action — Provide the correct port and host name. If the SQL Server is not running, then start it. Ensure that the TCP/IP port is enabled on the SQL Server instance.

The following error is encountered:

```
# _Wbem_Remote_Determination_DynamicProperty - Missing Properties :
[iscluster]
# MSSQL_NumClusterNodes - Error Querying: The user does not have permission
to perform this action.
# _MSSQL_Existence_TestMetric - em_error=em_error=Can't find the key :
SOFTWARE\Microsoft\Microsoft SQL Server\SQLSRVR_
2005\MSSQLServer\CurrentVersion\\CurrentVersion
```

Action — Execute the following command from sysadmin user:

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

2.3.2.3 WMI Test Connection Issues

This section addresses WMI-related test connection issues.

Metric Collection Error

While doing a test connection, you might encounter the following error:

```
Can't get query descriptor or execution descriptor
```

Possible Cause— (Failed to compute wbemremote) - *is cluster* missing due to wrong URL, wrong credential or wrong sqljdbc.dll file location.

Action— Check the `sqljdbc.dll` file location, SQL Server status (if status is not Up, start Microsoft SQL Server), URL, and credentials.

WMI Error 0x8004100E

Possible Cause— The 0x8004100E error indicates the `Namespace specified could not be found` error string.

Action— In this case, ensure the `root\MicrosoftSQLServer` namespace is enabled. Otherwise the test connection will fail.

> **Note:** This applies only to SQL server 2000.

Could Not Connect. Error:0x80041064

You might encounter this error leading to a connection failure with a message explaining the failure to connect to WMI.

Possible Cause—For Local Agent Monitoring, System Username and password are provided.

Action— Remove the System Username and password using the Monitoring Configuration link.

Possible Cause— For Remote Agent Monitoring, System Username and Password are either incorrect or are fields are left blank.

Action— Provide System Username and Password using the Monitoring Configuration link.

Error: On Win2k computers- em_error=Could not connect. Error code = 0x80041003 em_ error=Failed while connecting to WMI.

Error: On non-Win2k computers- em_error=Could not connect. Error code = 0x80070005 em_ error=Failed while connecting to WMI.

You might encounter this error leading to a connection failure, stating Failed while connecting to WMI.

Possible Cause — The following may be the possible causes:

- WMI Error code '0x80041003' or '0x80070005' is ACCESS_DENIED. System User doesn't have permission to access root\default namespace

- System User does not have the required access to DCOM

Action — Do the following:

1. Assign access (Remote Enable) for root\Default namespace and root\cimv2. For detailed steps, see Modifying Permissions.

2. Assign "Launch and Activate Permission – Edit Limits" for DCOM. For detailed steps, see Modifying DCOM Remote Access Permissions.

Error: em_error=Could not connect. Error code = 0x800706ba em_error=Failed while connecting to WMI.

Possible Cause — Access denied because RPC Server is Unavailable. This may happen if:

- RPC Server is 'really' down. Or,

- Due to Firewall configuration

Action — Allow Remote Administration Exception in Windows Firewall setting. See the following link for more details:

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

Error: After Deploying the Plug-in To Management Agents Running on Cluster Nodes, Target-Type "Microsoft SQL Server" Is Not Displayed on the "Virtual Agent Service" Home Page in Enterprise Manager Grid Control

Possible Cause — Reload of virtual Management Agent is not performed after the plug-in is deployed to Management Agents running on 'real' nodes.

Action — From the ORACLE_HOME of the 'virtual' Management Agent, reload the Management Agent by running the following command:

```
emctl reload agent
```

2.3.3 Windows Authentication Issues

You might encounter the following general Windows authentication issues:

Error: DB Credentials should not be provided for Windows Integrated Security Connections

Possible Cause — Database credentials have been provided for Windows Authentication

Action — Remove the DB credentials and retry.

Error : Failed to connect, Login Failure. Possible reasons are: Encrypted properties are not provided. Provided Database Username or Password or both are not correct. Provided Database User may not exist. Login failed for user 'NT AUTHORITY\ANONYMOUS LOGON'.

Possible Cause — For remote monitoring scenario, user desires to use Windows Authentication, but System Username is not provided.

Action — Provide the System credentials and retry.

Error: Exception occurred while Logon: Logon failure: the user has not been granted the requested logon type at this computer.

Possible Cause — System User specified does not have login privilege on agent system.

Action — Assign 'Log on as Batch Job' to the Target System User on Agent system. To do this, follow these steps:

1. Open the local security setting by clicking **Start**, then **All Programs**, and selecting **Administrative Tools**.

2. Select **Local Policies** and then click **User Right Assignments**.

3. Add the user in the **Log on Batch Job** policy.

Error: Failed to connect, Login Failure. Possible reasons are: Encrypted properties are not provided. Provided Database Username or Password or both are not correct. Provided Database User may not exist. Login failed for user (provided user)

Possible Cause — System user does not have login access to Database server.

Action — Provide System User login access to the instance. For detailed steps, see Modifying Permissions for Database Authentication.

Error : Error Querying: The user does not have permission to perform this action.

Possible Cause — System User specified does not have the required privilege/role to the Microsoft SQL Server instance.

Action — Assign sysadmin server role to the System User. For detailed steps, see Modifying Permissions for Database Authentication.

2.4 Report Elements and Dependent Metrics

The following table lists the report elements and dependent metrics for Microsoft SQL Server plug-in.

Table 1   Report Elements and Dependent Metrics

Report Name	Report Elements	Dependent Metrics
Microsoft SQL Server Cache and Buffer	- Memory Status - Buffer Performance - Buffer Allocation - Cache Performance - Memory Allocation - Memory Allocation Chart	- Memory Manager - Buffer Manager - Buffer Manager - Cache Manager - Memory Manager - Memory Manager
Microsoft SQL Server Cluster	- Cluster Nodes Summary - SQL Cluster Nodes Summary - Nodes in Cluster - Cluster Resources and Activity	- Windows Cluster Name - SQL Cluster Number of Nodes - Windows Cluster Nodes SQL Cluster Nodes Information Cluster Active Resource And Node - Cluster Active Resource And Node Cluster Resource and Owner Node Name Cluster Resources
Microsoft SQL Server Database Configuration	Databases Database Settings	Database Database Setting (Configuration Metric)
Microsoft SQL Server Database Backups and Jobs	- Database Backups - Database Jobs	- SQL Server (Configuration Metric) - Database Job
Microsoft SQL Server Space Usage	- Database Space Usage - Top 5 Databases by Space Used (%) - Database Files	- Database - Database - SQL Server (Configuration Metric) Microsoft SQL DatabaseFile

Table 1   (Cont.) Report Elements and Dependent Metrics

Report Name	Report Elements	Dependent Metrics
Microsoft SQL Server Alert Log and Alert Events	■ Error Logs ■ Event Summary (in current log) ■ Server and Agent Errors ■ Server and Agent Warnings ■ Server Alerts	■ Registry Setting (Configuration Metric) ■ SQL Server (Configuration Metric) Event Log Entry ■ SQL Server (Configuration Metric) Event Log Entry ■ SQL Server (Configuration Metric) Event Log Entry ■ Server Alerts
Microsoft SQL Server Process Info and Locks	■ Summary ■ Process States ■ Process Info ■ Process Locks ■ Lock Analysis	■ SQL Server Process ■ SQL Server Process ■ SQL Server (Configuration Metric) SQL Server Process ■ Database Lock ■ SQL Server (Configuration Metric) SQL Server ■ Locks
Microsoft SQL Server Memory Statistics	■ Server Statistics ■ Buffer Cache Hit Ratio ■ Cache Hit Ratio ■ Average Latch Wait Time (ms) ■ Total Lock Wait Time (ms)	Memory Statistics
Microsoft SQL Server Performance	■ Host CPU load percentage ■ Top SQL Server Processes by CPU Time ■ Memory Manager ■ Top Server Processes by Memory Usage	■ Processor ■ SQL Server Process ■ SQL Server (Configuration Metric) Memory Manager ■ SQL Server Process
Microsoft SQL Server Users and Privileges	■ Logins ■ Server roles ■ Database users ■ Top 10 User Logins Based on CPU Usage (ms)	■ Login ■ SQL Server Role ■ User ■ User Statistics

Table 1   (Cont.) Report Elements and Dependent Metrics

Report Name	Report Elements	Dependent Metrics
Microsoft SQL Server Statistics	■ Server Statistics ■ Rate of Errors ■ Packet Error Ratio ■ Rate of Reads ■ Rate of Writes ■ Statistics (per Database) ■ Statistics (aggregated for all Databases) ■ Server Statistics	■ Server Statistics ■ Server Statistics ■ Server Statistics ■ Server Statistics ■ Server Statistics ■ SQL Server (Configuration Metric) Database Performance ■ SQL Server (Configuration Metric) Database Performance ■ SQL Server (Configuration Metric) General Statistics
Microsoft SQL Server System Configuration	■ Instance Information ■ Registry ■ Security ■ Server Parameters	■ SQL Server (Configuration Metric) Response ■ Agent Status ■ SQL Server (Configuration Metric) Registry Setting (Configuration Metric) ■ Integrated Security Setting ■ Database Parameter

3 Troubleshooting IBM DB2 Plug-In

The following sections provide troubleshooting scenarios related to IBM DB2 plug-in.

3.1 How To Diagnose

The following sections help you diagnose issues that you may encounter while working with the IBM DB2 plug-in.

### 3.1.1 Finding TCP/IP Port

The communication port to access the remote IBM DB2 instance can be configured. The default value is 50000.

To find the port for a particular IBM DB2 instance, do the following:

For UNIX Platforms

1. Open a command prompt.

2. Enter cd /usr/etc.

3. Enter cat services.

4. Start of changeScroll through the list of services until you find the connection port number for the database instance of the remote database.

The instance name is usually listed as a comment. If it is not listed, then complete the following steps to find the port:

a. Open a DB2 command prompt.

b. At the DB2 command prompt, run the following command to verify that you are on the correct instance. IBM DB2 will report the current instance.

```
get instance
```

c. Run the following command to find the service name for your instance:

```
get dbm cfg | grep SVCE
```

IBM DB2 will report the service name.

For example:

```
TCP/IP Service name SVCENAME) = db2cdb2inst24
```

d. Use the service name to find the port number in the services file.

For example, enter the following command:

```
grep service_name /etc/services
```

IBM DB2 will return the information.

For example:

```
service_name   50012/tcp   # Connection port for DB2 instance
instance
```

For Microsoft Windows Platforms

1. Open the DB2 Control Center on the remote Windows server.

2. Right-click one of the available instances for the local machine.

3. Click **Setup Communications**.

4. Click **Properties**.

The port number is listed in the Properties window.

For z/OS Platforms

1. Connect to the z/OS system.

2. Run the following command:

```
-DISPLAY DDF
```

The TCPPORT value in the results is the port number.

3.2 How To Fix

The following sections help you fix issues that you may encounter while working with the IBM DB2 plug-in.

3.2.1 Using a Suitable Operating System User and Assigning Authorities and Privileges

You might see the following error on the Monitoring Configuration page of the Enterprise Manager Grid Control console:

Figure 1   Error Message When Incorrect Privileges Are Used and When OK is Clicked

Figure 2   Error Message When Incorrect Privileges Are Used and When Test Connection is Clicked
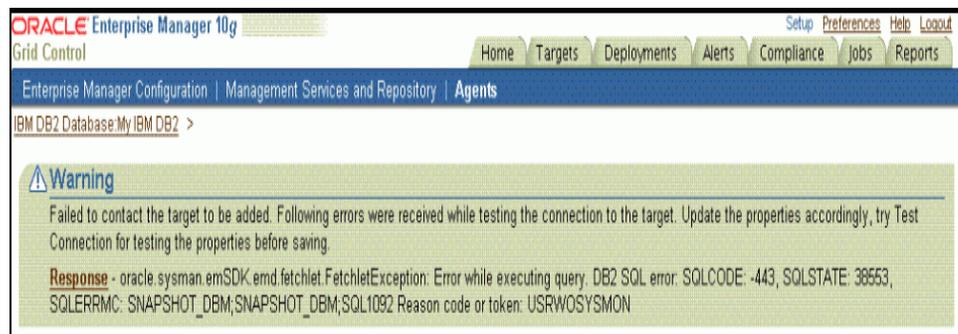
Possible Cause -- You are not using a user or the user you are using does not have the correct privileges.

Action -- Use a user that has at least the minimum privileges. For information about creating a suitable operating system user and assigning authorities and privileges to that user, see *Enterprise Manager System Monitoring Plug-in Installation Guide for IBM DB2 Database* available at:

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

3.2.2 Incorrect Credentials Used

You might see the following error:

```
Failed to contact the target to be added. Following errors were received
while testing the connection to the target. Update the properties
accordingly, try Test Connection for testing the properties before saving.
```

Response - oracle.sysman.emSDK.emd.fetchlet.FetchletException: Error while obtaining connection.Connection authorization failure occurred. Reason: password invalid.

Possible Cause -- You are using incorrect credentials.

Action -- Use correct credentials.

3.2.3 No Data for Health Indicator Metrics

You may not see any data for Health Indicator metrics.

Possible Cause -- You have not enabled the *HEALTH_MON* database manager configuration parameter.

Action -- For data to be collected for the **Health Indicators** metric, you have to enable the *HEALTH_MON* database manager configuration parameter. Only then the table functions -- HEALTH_TBS_HI, HEALTH_DB_HI, and HEALTH_DBM_HI get populated.

> **Note:**   Enabling these settings may result in some overheads, such as CPU and memory. Therefore, follow these troubleshooting steps only if you want to view the Health Indicator metrics.

To enable or disable the HEALTH_MON by CLP (Command Line Processor), run the following command:

```
db2==> update dbm cfg using HEALTH_MON [on;off]
```

To check if your changes are effective, run the following command:

```
db2==> get dbm cfg
```

The following is the output:

```
.....
.....
.....
Monitor health of instance and databases (HEALTH_MON) = ON
.....
.....
.....
```

For more information, access the IBM Web site.

3.2.4 Metric Collection Error for Database Monitoring Metrics

You may see the following error:

Error: oracle.sysman.emSDK.emd.fetchlet.FetchletException: Error while executing query. DB2 SQL error: SQLCODE: -204, SQLSTATE: 42704, SQLERRMC: SYSTOOLS.STMG_ DBSIZE_INFO

Possible Cause -- The table STMG_DBSIZE_INFO is not created.

Action -- For data to be collected for the Database Monitoring metric, make a call to the GET_DBSIZE_INFO package so that the STMG_DBSIZE_INFO table gets created and populated with the required data.

The GET_DBSIZE_INFO procedure calculates the database size and maximum capacity. The calculated values are returned as procedure output parameters and cached in the SYSTOOLS.STMG_DBSIZE_INFO table. The procedure caches these values because the calculations are costly.

The SYSTOOLS.STMG_DBSIZE_INFO table is created automatically the first time the procedure runs. If there are values cached in the SYSTOOLS.STMG_ DBSIZE_INFO table and they are current enough, as determined by the

snapshot-timestamp and refresh-window values, then these cached values are returned.

If the cached values are not current enough, new cached values are calculated, inserted into the SYSTOOLS.STMG_DBSIZE_INFO table and returned, and the snapshot-timestamp value is updated. The last parameter in the GET_DBSIZE_ INFO call is refresh window.

Default value refresh window (time difference between successive calls) is 30 minutes. If your database is growing at a faster rate, then you can set a lower value.

To make a call to GET_DBSIZE_INFO by CLP (Command Line Processor), run the following command:

```
db2==>CALL GET_DBSIZE_INFO(?, ?, ?, -1)
```

In this case, the refresh window is 30 minutes.

For more information, access the IBM Web site.

Error:

```
Target - <target_name>
      Type - IBM DB2 Database
      Metric - DB2 Diag Log File Monitoring
      Collection - Timestamp Apr 1, 2009 10:19:59 AM
     Error Type - Collection Failure
     Message - Use of uninitialized value in string eq at
    e:\oracle\agent10g/sysman/admin/scripts/emx/ibm_db2_database/logmine.pl
line 188. The DB2 Database Manager Configuration Parameter DIAGPATH needs to
be set
```

Possible Cause— Following could be the causes of the error:

- DIAGPATH is not set

- Database is down

Action— If DIAGPATH is not set, set the DIAGPATH run from the command line as follows:

```
db2 update dbm cfg using  diagpath <path>
```

On Windows systems, the path is `<db2 installation directory>\<instance name>`

On Linux or AIX systems, the path is `<instancehome>/sqllib/db2dump`

If the DIAGPATH is already set, metric collection errors will occur if the database is down.

4 Troubleshooting Sybase Adaptive Server Enterprise Plug-In

The following sections provide troubleshooting scenarios related to Sybase Adaptive Server Enterprise plug-in.

4.1 How To Fix

The following sections help you fix issues that you may encounter while working with the Sybase Adaptive Server Enterprise plug-in.

4.1.1 Failed to connect, JZ006: Caught IOException: java.net.ConnectException: Connection refused

Possible Cause— Port number is incorrect.

Action— Specify the correct port number in the JDBC URL.

4.1.2 Failed to connect, JZ00L: Login failed. Examine the SQLWarnings chained to this exception for the reason(s)

Possible Cause— The DB user name and password are incorrect.

Action— Specify the correct DB user name and password.

4.1.3 JZ006: Caught IOException: java.io.IOException OR JZ0I6: An error occurred converting UNICODE to the charset used by the server OR Error message: java.io.CharConversionException:java.io.UnsupportedEncodingException: hp-roman8

Possible Cause— ?charset=iso_1 last is not set in the JDBC URL.

Action— Add `?charset=iso_1 last` in the JDBC URL as shown below:

```
jdbc:sybase:Tds:<HOST>:<PORT>/?charset=iso_1
```

4.1.4 SELECT permission denied on object <Object Name>, database master, owner dbo

Possible Cause— The user who is currently monitoring the target does not have the required role and permissions.

Action— Check whether the user has all the required roles and permissions as described in the *Configuring Sybase Adaptive Server for Monitoring* section of the installation guide. If not, grant the required permissions.

4.1.5 <TABLE NAME> not found. Specify owner.objectname or use sp_help to check whether the object exists (sp_help may produce lots of output).

Possible Cause— The <TABLENAME> is not available on the target side. If <TABLENAME> is either master..mon<*> or mon<*>, then the required MDA table is not available.

Action— Check whether the MDA tables are installed. If they are not, install them.

4.1.6 Error Querying: Collection of monitoring data for table '<TABLE NAME>' requires that the '<PARAMETER(S)>' configuration option(s) be enabled. To set the necessary configuration, contact a user who has the System Administrator (SA) role

Possible Cause— The <PARAMETER> shown in the error message has not been enabled.

Action— Enable the <PARAMETER> that is shown in the error message. To understand how configuration parameters can be enabled, refer to the *Prerequisites* section of the installation guide.

The following shows the configuration parameters to be enabled for each metric.

Table 2   Configuration Parameters to be Enabled for Metrics

Metric	Configuration Parameter
Adaptive Server Engines Statistics	enable monitoring
Data Caches statistics	enable monitoring
Procedure Cache statistics	enable monitoring
Open Databases statistics	enable monitoring
Server-wide worker threads statistics	enable monitoring
Network I/O Statistics	enable monitoring
Most recent error messages	enable monitoring, errorlog pipe max messages, errorlog pipe active
Locks Information	enable monitoring
Deadlock Statistics	enable monitoring, deadlock pipe max messages, and deadlock pipe active
Cache Pools Statistics	enable monitoring
Open Objects Statistics	enable monitoring, per object statistics active
Device Data and IO log statistics	enable monitoring
Devices Statistics	enable monitoring
Waiting Events Statistics	enable monitoring, wait event timing
Process Statistics	enable monitoring, wait event timing
Processes activity statistics	enable monitoring, wait event timing, per object statistics active
Processes Network IO activity	enable monitoring
Process Objects Information	enable monitoring, per object statistics active
Waiting Process Statistics	enable monitoring, wait event timing, process wait events
Currently Executing Queries	enable monitoring, wait event timing, per object statistics active, statement statistics active
Currently Executing SQL Text Information	enable monitoring, max SQL text monitored, SQL batch capture
Most recently executed statement statistics	enable monitoring, wait event timing, per object statistics active, statement pipe max messages, statement statistics active
Recently (currently being) executed SQL Text	enable monitoring, max SQL text monitored, SQL batch capture, SQL text pipe max messages, SQL text pipe active

4.1.7 Report Element Showing "No Data Found" or "No Rows Returned"

Possible Cause— The underlying metric data has not been collected or the data has not been rolled up into hourly views.

Action— For the report element (chart or table) that shows this message, first identify the dependent metric and then check whether metric data has been collected for it.

The following shows the report elements and their dependent metrics. Using this table, identify the dependent metric. Once that is done, go to the All Metrics page of the target in Enterprise Manager Grid Control, and check whether metric data has been collected for that dependent metric. If data has not been collected yet, then check the collection frequency and wait until the collection happens.

Table 3   Report Elements and Dependent Metrics

Report Name	Report Elements	Dependent Metrics
Sybase ASE Performance Statistics	■ CPU Utilization ■ IO Utilization	Adaptive Server Statistics
	■ ASE State Summary ■ ASE State Summary...	Adaptive Server State
Sybase ASE Engines Statistics	■ System CPU (by all Engine's) Utilization ■ User CPU (by all Engine's) Utilization ■ Top 10 Engines by System CPU Utilization ■ Top 10 Engines by User CPU Utilization	Adaptive Server Engines Statistics
Sybase ASE Databases Space Statistics	Top 5 Databases by Data Space Utilization Top 5 Databases by Log Space Utilization Top 10 Databases by Data Space Utilization Top 10 Databases by Log Space Utilization	Database Instances
	Databases Backup Related Summary	Open Databases statistics
Sybase ASE Device IO Statistics	■ User Data Devices IO Operations Vs Waiting time ■ User Log Devices IO Operations Vs Waiting Time ■ User Data Devices IO Summary ■ User Log Devices IO Summary ■ Tempdb Data Devices IO Operations Vs Waiting Time ■ Tempdb Log Devices IO Operations Vs Waiting Time ■ Tempdb Data Devices IO Summary ■ Tempdb Log Devices IO Summary	Device Data and IO log statistics

Table 3   (Cont.) Report Elements and Dependent Metrics

Report Name	Report Elements	Dependent Metrics
	■ Device Reads Rate Vs Writes Rate Vs APF Reads Rate	Devices Statistics
	■ Devices Semaphore Requests Rate Vs Waits Rate Device IO Operations Summary	
Sybase ASE Data Cache Statistics	■ Data Cache Hit Rate History ■ Data Cache Hit Rates Summary	Data Caches statistics
	■ Data Cache Memory Usage ■ Cached Object Accesses by Processes ■ Top 10 Big Objects in Data Cache ■ Top 10 Popular Objects in Data Cache	Cached Objects Statistics
Sybase ASE Procedure Cache Statistics	Procedure Cache Hit Rate History Procedure Cache Memory Usage History	Procedure Cache statistics
	■ Top 10 Objects in Procedure Cache by Memory Usage	Cached Procedures Statistics
Sybase ASE Network IO Monitoring Report	■ Incoming Traffic History ■ Outgoing Traffic History ■ Incoming Packet Traffic History ■ Outgoing Packet Traffic History	Network I/O Statistics
Sybase ASE Database Log Statistics	■ Overall Append Log Requests ■ Rate Vs Waits Rate ■ Tempdb Append Log Requests Rate Vs Waits Rate ■ Overall Append Log Waits Percentage ■ Tempdb Append Log Waits Percentage ■ Databases Log Related Summary	Open Databases statistics
Sybase ASE User Statistics	Attempted Logins History	Adaptive Server Statistics
	Top 5 User SQL Statistics Summary	Recently (currently being) executed SQL Text

Table 3   (Cont.) Report Elements and Dependent Metrics

Report Name	Report Elements	Dependent Metrics
	■ Top 3 Users by CPU Time ■ Top 3 Users by DiskIO ■ Top 3 Users by CPU Time - Summary ■ Top 3 Users by DiskIO Time - Summary	Processes activity statistics
	■ Top 3 Users by Incoming Network Traffic ■ Top 3 Users by Outgoing Network Traffic ■ Top 3 Users by Incoming Network Traffic - Summary ■ Top 3 Users by Outgoing Network Traffic - Summary	Processes Network IO activity
Sybase ASE Process Statistics	■ Top 10 Processes by CPU Time ■ Top 10 Processes by Waiting Time ■ Top 10 Processes by Memory Usage ■ Top 10 Processes by User Log Cache(ULC) Writes Top 10 Processes by Transactions Rate ■ Top 10 Processes by DiskIO Rate	Processes activity statistics
	■ Top 10 Processes by Incoming Network Traffic ■ Top 10 Processes by Outgoing Network Traffic	Processes Network IO activity
Sybase ASE SQL Statistics	■ Top 3 CPU Intensive SQL Commands ■ Top 3 Disco Intensive SQL Commands ■ Top 3 Memory Intensive SQL Commands ■ Top 3 Long Waited SQL Commands	Most recently executed statement statistics, Recently (currently being) executed SQL Text
Sybase ASE Open Objects Statistics	■ Top 5 Hot Objects by Logical Reads ■ Top 5 Hot Objects by Physical Reads ■ Top 5 Hot Objects by APF Reads ■ Top 5 Hot Objects by APF Reads ■ Top 5 Hot Objects by Physical Writes	Open Objects Statistics
Sybase ASE Deadlock Statistics	Top 10 Processes by Lock Wait Time	Locks Information
	·Deadlock Detail Table	Deadlock Statistics

Table 3   (Cont.) Report Elements and Dependent Metrics

Report Name	Report Elements	Dependent Metrics
Sybase ASE Worker Threads Statistics	■ Attempted Parallel Queries History ■ Altered Plans History ■ Worker Threads Summary	Server-wide worker threads statistics
Sybase ASE Error Statistics	■ Errors Production Rate (per hr) ■ Recent Error Messages Summary ■ Recent Error Messages with Severity 10 to 16 ■ Recent Error Messages with Severity 17 to 18 ■ Recent Error Messages with Severity 19 to 26	Most recent error messages

Table 3   (Cont.) Report Elements and Dependent Metrics

Report Name	Report Elements	Dependent Metrics
Sybase ASE Configuration	▪ Sybase ASE Version	Configuration metric with the same name.
	▪ System Listeners	
	▪ Information about Databases	
	▪ Installed Scripts	
	▪ Charsets Information	
	▪ Backup/Recovery Configuration Parameters	
	▪ Cache Manager Configuration Parameters	
	▪ Component Integration Services Configuration Parameters	
	▪ Configuration Options Configuration Parameters	
	▪ DTM Administration Configuration Parameters	
	▪ Diagnostics Configuration	
	▪ Disk I/O Configuration Parameters	
	▪ Error Log Configuration Parameters	
	▪ Extended Stored Procedure Configuration Parameters	
	▪ General Information Configuration Parameters	
	▪ Java Services Configuration Parameters	
	▪ Languages Configuration Parameters	
	▪ Lock Manager Configuration Parameters	
	▪ Memory Use Configuration Parameters	
	▪ Monitoring Configuration Parameters	
	▪ Network Communication Configuration Parameters	
	▪ O/S Resources Configuration Parameters	
	▪ Physical Memory Configuration Parameters	
	▪ Physical Resources Configuration Parameters	
	▪ Processors Configuration Parameters	
	▪ Rep Agent Thread Administration Configuration Parameters	
	▪ Security Related Configuration Parameters	
	▪ SQL Server Administration Configuration Parameters	
	▪ Unicode Configuration Parameters	
	▪ User Environment Configuration Parameters	

4.1.8 For Segment Usage metric, there is an error when querying: Server user id <USERID> is not a valid user in database '<DATABASE>'

Possible Cause— The monitoring user does not have permission on all databases in Sybase ASE target.

Action— Provide permission to query SYSSEGMENTS table to monitoring user or else create guest user account in each database.

5 Troubleshooting VMware ESX Server Plug-In

The following sections provide troubleshooting scenarios related to VMware ESX Server plug-in.

5.1 How To Fix

The following sections help you fix issues that you may encounter while working with the VMware ESX Server plug-in.

5.1.1 Calculation of Dynamic Properties Time Out

The VMware ESX Server target instance has a number of dynamic instance properties that are calculated by the Management Agent when a new target instance is added. This calculation also occurs for an existing target instance as a result of one of the following:

- Emctl reload agent dynamicproperties <target_name>:vmware_esx_server

- Emctl reload agent (and the target type definition has changed, that is, metadata has been updated)

- The plug-in is upgraded (and the target type definition has changed)

The Management Agent has a default timeout of 30 seconds as to how long it will try to recalculate the dynamic properties. It is possible for the calculation of the dynamic properties to time out.

Possible Cause -- The calculation of the dynamic properties can time out when the Management Agent is under heavy load.

The ESX Server target type has a dynamic property named *version* that is used to provide different versions of metric definitions for different versions of ESX Server. If *version* does not get computed within the timeout period, then metric collection errors will occur with a message similar to the following one:

```
Error encountered while retrieving metric VMConfigSumm.  Exception in thread
"main" java.lang.NumberFormatException: For input string: "%version%"
at
java.lang.NumberFormatException.forInputString(NumberFormatException.java:48)
at java.lang.Integer.parseInt(Integer.java:489)
at java.lang.Integer.valueOf(Integer.java:595)
at oracle.sysman.mpi.vmware.esx_
server.MetricCollector.main(MetricCollector.java:269)
```

Action -- You can resolve this issue in one of the following ways:

1. The `emctl reload agent dynamicproperties` command can be rerun while the Management Agent is under lighter load.

2. It is possible to increase the default value of 30 seconds for the timeout period.

In `$AGENT_HOME/sysman/config/emd.properties`, there is a Management Agent property named `dynamicPropsComputeTimeout`. You can uncomment that definition and increase the value of the timeout period, for example, to 120 seconds. This will then apply to all target types.

It is also possible to increase the timeout period for a particular target type by adding the following declaration where nn is the number of seconds for the timeout:

```
dynamicProspComputeTimeout_vmware_esx_server=nn
```

When either of these values are added or changed, the Management Agent must be refreshed with an `emctl reload agent` command in order to recognize the new value.

6 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.