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.
**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:
   - Log in to Enterprise Manager Grid Control.
   - Click **Preferences** from the top-right corner of the page.
   - From the left menu bar, click **Preferred Credentials**.
   - In the Preferred Credentials page, in the table, for the Host target type, from the **Set Credentials** column, click the icon.
   - 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:
   - Log in to Enterprise Manager Grid Control.
   - Click the **Jobs** tab.
   - In the Job Activity page, from the **Create Job** list, select OS Command, and click **Go**.
   - Fill up the details required in the following pages, and click **Submit** to run the job. If the job runs successfully, your credentials are set correctly.

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,

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 <DATA_ROOT> 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:

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

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 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.
   
   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:


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.
2.2 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:

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:
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.

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.

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.

**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](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:

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.
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:

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:

2.2.3.6 Modifying Access Privileges of SQL Server Services

Follow these steps to modify access privileges of SQL 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
```

   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:

   ```
   at servicedesk
   ```

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

   ```
   ```

Note: Execute the following commands only if the Windows box in which SQL Server resides is Windows 2003 SP1 or later.
d. If the privileges for AU (Authenticated Users) are not same as (A;;CCLCSWRWPDPDTLOCRRC;;;AU), set it using the following command by replacing (A;;CR;;;AU) with (A;;CCLCSWRWPDPDTLOCRRC;;;AU):

```
sc sdset SQLServer_service_name
```
```
```

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:


### 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 JDBIc 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 field 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.
2.3.1.6 Target is In Broken State: Metric Collection Errors Encountered

**Note:** When this error is found for a 32-bit version of SQL Server installed on 64-bit system, instead of using the default smiadap executable, look for the smiadap executable under <WINDOWS\SYSTEM32\SYSWOW64>, for example, C:\WINDOWS\SysWOW64. Run this copy of smiadap.exe with the options mentioned above.

**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:

```bash
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 these 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\SQLSRV\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:
   - Check if `exec master.dbo.sysdatabases` gives the same error.
   - See if you find NULL value for the second column for query `select name, suser_sname(sid) from master.dbo.sysdatabases`.
   - 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.
     ```
   - 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.
   - 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 - en_error=en_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.
21

**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:

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>
<thead>
<tr>
<th>Report Name</th>
<th>Report Elements</th>
<th>Dependent Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server Cache and Buffer</td>
<td>Memory Status, Buffer Performance, Buffer Allocation, Cache Performance, Memory Allocation, Memory Allocation Chart</td>
<td>Memory Manager, Buffer Manager, Buffer Manager, Cache Manager, Memory Manager, Memory Manager</td>
</tr>
<tr>
<td>Microsoft SQL Server Cluster</td>
<td>Cluster Nodes Summary, SQL Cluster Nodes Summary, Nodes in Cluster, Cluster Resources and Activity</td>
<td>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</td>
</tr>
<tr>
<td>Microsoft SQL Server Database Configuration</td>
<td>Databases, Database Settings</td>
<td>Database Setting (Configuration Metric)</td>
</tr>
<tr>
<td>Microsoft SQL Server Database Backups and Jobs</td>
<td>Database Backups, Database Jobs</td>
<td>SQL Server (Configuration Metric), Database Job, Database, Database, SQL Server (Configuration Metric)</td>
</tr>
<tr>
<td>Microsoft SQL Server Space Usage</td>
<td>Database Space Usage, Top 5 Databases by Space Used (%), Database Files</td>
<td>Microsoft SQL DatabaseFile</td>
</tr>
<tr>
<td>Report Name</td>
<td>Report Elements</td>
<td>Dependent Metrics</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>------------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Microsoft SQL Server Alert Log and Alert Events</td>
<td>Error Logs</td>
<td>Registry Setting (Configuration Metric)</td>
</tr>
<tr>
<td></td>
<td>Event Summary (in current log)</td>
<td>SQL Server (Configuration Metric)</td>
</tr>
<tr>
<td></td>
<td>Server and Agent Errors</td>
<td>Event Log Entry</td>
</tr>
<tr>
<td></td>
<td>Server and Agent Warnings</td>
<td>SQL Server (Configuration Metric)</td>
</tr>
<tr>
<td></td>
<td>Server Alerts</td>
<td>Event Log Entry</td>
</tr>
<tr>
<td>Microsoft SQL Server Process Info and Locks</td>
<td>Summary</td>
<td>SQL Server Process</td>
</tr>
<tr>
<td></td>
<td>Process States</td>
<td>SQL Server Process</td>
</tr>
<tr>
<td></td>
<td>Process Info</td>
<td>SQL Server (Configuration Metric)</td>
</tr>
<tr>
<td></td>
<td>Process Locks</td>
<td>Database Lock</td>
</tr>
<tr>
<td></td>
<td>Lock Analysis</td>
<td>SQL Server (Configuration Metric)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SQL Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Locks</td>
</tr>
<tr>
<td>Microsoft SQL Server Memory Statistics</td>
<td>Server Statistics</td>
<td>Memory Statistics</td>
</tr>
<tr>
<td></td>
<td>Buffer Cache Hit Ratio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cache Hit Ratio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Average Latch Wait Time (ms)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total Lock Wait Time (ms)</td>
<td></td>
</tr>
<tr>
<td>Microsoft SQL Server Performance</td>
<td>Host CPU load percentage</td>
<td>Processor</td>
</tr>
<tr>
<td></td>
<td>Top SQL Server Processes by CPU Time</td>
<td>SQL Server Process</td>
</tr>
<tr>
<td></td>
<td>Memory Manager</td>
<td>SQL Server (Configuration Metric)</td>
</tr>
<tr>
<td></td>
<td>Top Server Processes by Memory Usage</td>
<td>Memory Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SQL Server Process</td>
</tr>
<tr>
<td>Microsoft SQL Server Users and Privileges</td>
<td>Logins</td>
<td>Login</td>
</tr>
<tr>
<td></td>
<td>Server roles</td>
<td>SQL Server Role</td>
</tr>
<tr>
<td></td>
<td>Database users</td>
<td>User</td>
</tr>
<tr>
<td></td>
<td>Top 10 User Logins Based on CPU Usage (ms)</td>
<td>User Statistics</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Report Elements</th>
<th>Dependent Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server Statistics</td>
<td>• Server Statistics</td>
<td>• Server Statistics</td>
</tr>
<tr>
<td></td>
<td>• Rate of Errors</td>
<td>• Server Statistics</td>
</tr>
<tr>
<td></td>
<td>• Packet Error Ratio</td>
<td>• Server Statistics</td>
</tr>
<tr>
<td></td>
<td>• Rate of Reads</td>
<td>• Server Statistics</td>
</tr>
<tr>
<td></td>
<td>• Rate of Writes</td>
<td>• Server Statistics</td>
</tr>
<tr>
<td></td>
<td>• Statistics (per Database)</td>
<td>• SQL Server (Configuration Metric)</td>
</tr>
<tr>
<td></td>
<td>• Statistics (aggregated for all Databases)</td>
<td>• Database Performance</td>
</tr>
<tr>
<td></td>
<td>• Server Statistics</td>
<td>• SQL Server (Configuration Metric)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• General Statistics</td>
</tr>
<tr>
<td>Microsoft SQL Server System</td>
<td>• Instance Information</td>
<td>• SQL Server (Configuration Metric)</td>
</tr>
<tr>
<td>Configuration</td>
<td>• Registry</td>
<td>• Response</td>
</tr>
<tr>
<td></td>
<td>• Security</td>
<td>• Agent Status</td>
</tr>
<tr>
<td></td>
<td>• Server Parameters</td>
<td>• SQL Server (Configuration Metric)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Registry Setting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Integrated Security Setting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Database Parameter</td>
</tr>
</tbody>
</table>
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
   ```

   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:
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.


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\ems\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 JZ016: 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>
<thead>
<tr>
<th>Metric</th>
<th>Configuration Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive Server Engines Statistics</td>
<td>enable monitoring</td>
</tr>
<tr>
<td>Data Caches statistics</td>
<td>enable monitoring</td>
</tr>
<tr>
<td>Procedure Cache statistics</td>
<td>enable monitoring</td>
</tr>
<tr>
<td>Open Databases statistics</td>
<td>enable monitoring</td>
</tr>
<tr>
<td>Server-wide worker threads statistics</td>
<td>enable monitoring</td>
</tr>
<tr>
<td>Network I/O Statistics</td>
<td>enable monitoring</td>
</tr>
<tr>
<td>Most recent error messages</td>
<td>enable monitoring, errorlog pipe max messages, errorlog pipe active</td>
</tr>
<tr>
<td>Locks Information</td>
<td>enable monitoring</td>
</tr>
<tr>
<td>Deadlock Statistics</td>
<td>enable monitoring, deadlock pipe max messages, and deadlock pipe active</td>
</tr>
<tr>
<td>Cache Pools Statistics</td>
<td>enable monitoring</td>
</tr>
<tr>
<td>Open Objects Statistics</td>
<td>enable monitoring, per object statistics active</td>
</tr>
<tr>
<td>Device Data and IO log statistics</td>
<td>enable monitoring</td>
</tr>
<tr>
<td>Devices Statistics</td>
<td>enable monitoring</td>
</tr>
<tr>
<td>Waiting Events Statistics</td>
<td>enable monitoring, wait event timing</td>
</tr>
<tr>
<td>Process Statistics</td>
<td>enable monitoring, wait event timing</td>
</tr>
<tr>
<td>Processes activity statistics</td>
<td>enable monitoring, wait event timing, per object statistics active</td>
</tr>
<tr>
<td>Processes Network I/O activity</td>
<td>enable monitoring</td>
</tr>
<tr>
<td>Process Objects Information</td>
<td>enable monitoring, per object statistics active</td>
</tr>
<tr>
<td>Waiting Process Statistics</td>
<td>enable monitoring, wait event timing, process wait events</td>
</tr>
<tr>
<td>Currently Executing Queries</td>
<td>enable monitoring, wait event timing, per object statistics active, statement statistics active</td>
</tr>
<tr>
<td>Currently Executing SQL Text Information</td>
<td>enable monitoring, max SQL text monitored, SQL batch capture</td>
</tr>
<tr>
<td>Most recently executed statement statistics</td>
<td>enable monitoring, wait event timing, per object statistics active, statement pipe max messages, statement statistics active</td>
</tr>
<tr>
<td>Recently (currently being) executed SQL Text</td>
<td>enable monitoring, max SQL text monitored, SQL batch capture, SQL text pipe max messages, SQL text pipe active</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Report Name</th>
<th>Report Elements</th>
<th>Dependent Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sybase ASE Performance</td>
<td>• CPU Utilization</td>
<td>Adaptive Server</td>
</tr>
<tr>
<td>Sybase ASE Performance</td>
<td>• IO Utilization</td>
<td>Statistics</td>
</tr>
<tr>
<td>Sybase ASE Performance</td>
<td>• ASE State Summary</td>
<td>Adaptive Server</td>
</tr>
<tr>
<td>Sybase ASE Performance</td>
<td>• ASE State Summary...</td>
<td>State</td>
</tr>
<tr>
<td>Sybase ASE Engines</td>
<td>• System CPU (by all Engine’s) Utilization</td>
<td>Adaptive Server</td>
</tr>
<tr>
<td>Sybase ASE Engines</td>
<td>• User CPU (by all Engine’s) Utilization</td>
<td>Engine Statistics</td>
</tr>
<tr>
<td>Sybase ASE Engines</td>
<td>• Top 10 Engines by System CPU Utilization</td>
<td></td>
</tr>
<tr>
<td>Sybase ASE Engines</td>
<td>• Top 10 Engines by User CPU Utilization</td>
<td></td>
</tr>
<tr>
<td>Sybase ASE Databases</td>
<td>Top 5 Databases by Data Space Utilization</td>
<td>Database Instances</td>
</tr>
<tr>
<td>Sybase ASE Databases</td>
<td>Top 5 Databases by Log Space Utilization</td>
<td></td>
</tr>
<tr>
<td>Sybase ASE Databases</td>
<td>Top 10 Databases by Data Space Utilization</td>
<td></td>
</tr>
<tr>
<td>Sybase ASE Databases</td>
<td>Top 10 Databases by Log Space Utilization</td>
<td></td>
</tr>
<tr>
<td>Sybase ASE Databases</td>
<td>Databases Backup Related Summary</td>
<td>Open Databases statistics</td>
</tr>
<tr>
<td>Sybase ASE Device IO</td>
<td>• User Data Devices IO Operations Vs Waiting time</td>
<td>Device Data and IO</td>
</tr>
<tr>
<td>Sybase ASE Device IO</td>
<td>• User Log Devices IO Operations Vs Waiting Time</td>
<td>log statistics</td>
</tr>
<tr>
<td>Sybase ASE Device IO</td>
<td>• User Data Devices IO Summary</td>
<td></td>
</tr>
<tr>
<td>Sybase ASE Device IO</td>
<td>• User Log Devices IO Summary</td>
<td></td>
</tr>
<tr>
<td>Sybase ASE Device IO</td>
<td>• Tempdb Data Devices IO Operations Vs Waiting Time</td>
<td></td>
</tr>
<tr>
<td>Sybase ASE Device IO</td>
<td>• Tempdb Log Devices IO Operations Vs Waiting Time</td>
<td></td>
</tr>
<tr>
<td>Sybase ASE Device IO</td>
<td>• Tempdb Data Devices IO Summary</td>
<td></td>
</tr>
<tr>
<td>Sybase ASE Device IO</td>
<td>• Tempdb Log Devices IO Summary</td>
<td></td>
</tr>
<tr>
<td>Report Name</td>
<td>Report Elements</td>
<td>Dependent Metrics</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Sybase ASE Data Cache Statistics</td>
<td>Data Cache Hit Rate History</td>
<td>Data Caches statistics</td>
</tr>
<tr>
<td></td>
<td>Data Cache Hit Rates Summary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Cache Memory Usage</td>
<td>Cached Objects Statistics</td>
</tr>
<tr>
<td></td>
<td>Cached Object Accesses by Processes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top 10 Big Objects in Data Cache</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top 10 Popular Objects in Data Cache</td>
<td></td>
</tr>
<tr>
<td>Sybase ASE Procedure Cache Statistics</td>
<td>Procedure Cache Hit Rate History</td>
<td>Procedure Cache statistics</td>
</tr>
<tr>
<td></td>
<td>Procedure Cache Memory Usage History</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top 10 Objects in Procedure Cache by Memory Usage</td>
<td>Cached Procedures Statistics</td>
</tr>
<tr>
<td>Sybase ASE Network I/O Monitoring Report</td>
<td>Incoming Traffic History</td>
<td>Network I/O Statistics</td>
</tr>
<tr>
<td></td>
<td>Outgoing Traffic History</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incoming Packet Traffic History</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Outgoing Packet Traffic History</td>
<td></td>
</tr>
<tr>
<td>Sybase ASE Database Log Statistics</td>
<td>Overall Append Log Requests Rate Vs Rate</td>
<td>Open Databases statistics</td>
</tr>
<tr>
<td></td>
<td>Tempdb Append Log Requests Rate Vs Wait Rate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Overall Append Log Waits Percentage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tempdb Append Log Waits Percentage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Databases Log Related Summary</td>
<td></td>
</tr>
<tr>
<td>Sybase ASE User Statistics</td>
<td>Attempted Logins History</td>
<td>Adaptive Server Statistics</td>
</tr>
<tr>
<td></td>
<td>Top 5 User SQL Statistics Summary</td>
<td>Recently (currently being executed) SQL Text</td>
</tr>
</tbody>
</table>
### Table 3  (Cont.) Report Elements and Dependent Metrics

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Report Elements</th>
<th>Dependent Metrics</th>
</tr>
</thead>
</table>
| 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  
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 Writes | Open Objects Statistics |
| Sybase ASE Deadlock Statistics | Top 10 Processes by Lock Wait Time  
Deadlock Detail Table | Deadlock Statistics |
<table>
<thead>
<tr>
<th>Report Name</th>
<th>Report Elements</th>
<th>Dependent Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sybase ASE Worker Threads</td>
<td>• Attempted Parallel Queries History</td>
<td>Server-wide worker</td>
</tr>
<tr>
<td></td>
<td>• Altered Plans History</td>
<td>threads statistics</td>
</tr>
<tr>
<td></td>
<td>• Worker Threads Summary</td>
<td></td>
</tr>
<tr>
<td>Sybase ASE Error Statistics</td>
<td>• Errors Production Rate (per hr)</td>
<td>Most recent error</td>
</tr>
<tr>
<td></td>
<td>• Recent Error Messages Summary</td>
<td>messages</td>
</tr>
<tr>
<td></td>
<td>• Recent Error Messages with Severity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10 to 16</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Recent Error Messages with Severity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>17 to 18</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Recent Error Messages with Severity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>19 to 26</td>
<td></td>
</tr>
<tr>
<td>Report Name</td>
<td>Report Elements</td>
<td>Dependent Metrics</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Sybase ASE Configuration</td>
<td>Sybase ASE Version</td>
<td>Configuration metric with the same name.</td>
</tr>
<tr>
<td></td>
<td>System Listeners</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information about Databases</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installed Scripts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Charsets Information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Backup/Recovery Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cache Manager Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Component Integration Services Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration Options Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DTM Administration Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Diagnostics Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Disk I/O Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Error Log Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Extended Stored Procedure Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>General Information Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Java Services Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Languages Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lock Manager Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory Use Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Monitoring Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Communication Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>O/S Resources Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical Memory Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical Resources Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Processors Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rep Agent Thread Administration Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Related Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SQL Server Administration Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unicode Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User Environment Configuration Parameters</td>
<td></td>
</tr>
</tbody>
</table>
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 of the timeout:

dynamicPropsComputeTimeout_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.
If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-15, Commercial Computer Software License (December 2007).

Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, you shall be responsible to take all appropriate fail-safes, backups, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and explicitly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, cost, or damage incurred due to your access to or use of third-party content, products, or services.