Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for IBM DB2 Database

Release 7 (3.2.1.0.0)

E12306-02

May 2008

This document provides a brief description about the Oracle System Monitoring Plug-In for IBM DB2 Database, details on the versions the plug-in supports, prerequisites for installing the plug-in, and step-by-step instructions on how to download, install, verify, and validate the plug-in.

Description

The System Monitoring Plug-in for IBM DB2 Database extends Oracle Enterprise Manager Grid Control to add support for managing IBM DB2 Database instances. By deploying the plug-in in your Grid Control environment, you gain the following management features:

- Monitor DB2 Database instances.
- Gather configuration data and track configuration changes for DB2 Database instances.
- Raise alerts and violations based on thresholds set on monitored targets and configuration data.
- Provide rich out-of-box reports based on the gathered data.
- Support monitoring by a remote Agent. For remote monitoring, the agent need not be on the same host as IBM DB2.

Platforms Supported

The plug-in supports monitoring of IBM DB2 UDB (LUW) on all the platforms where IBM DB2 UDB can be installed.

Versions Supported

This plug-in supports the following versions of products:

- Enterprise Manager Grid Control 10.2.0.1 or higher (Oracle Management Service and Oracle Management Agent)
- Single-partitionIBM DB2 Universal Database (UDB) for Linux, UNIX, and Windows (LUW) Version 8.2 FixPak 2 (equivalent to version 8.1 FixPak 9) or higher.

Prerequisites

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

ORACLE®

- Install the following:
  - Enterprise Manager Grid Control 10.2.0.1 or higher
  - IBM DB2 Universal JDBC Type 4 driver for IBM DB2 Database (see Setting Up the JDBC Driver)
  - IBM DB2 Universal Database
- Create a suitable operating system user to access the table functions used in IBM DB2. For information about creating a user, see Using a Suitable Operating System User and Assigning Authorities and Privileges.
- To avoid metric collection errors for *Database Monitoring* metrics, create the table STMG_DBSIZE_INFO. For more information, see Configurations Required for Avoiding Metric Collection Errors for Database Monitoring Metrics.
- If you want to generate alerts using the IBM DB2 Diagnostic Log file (db2diag.log), then do the following:
  - Define your match patterns in the `Diag_log_file_match_pattern_file.txt` file that is present in `$ORACLE_HOME/sysman/admin/scripts/emx/ibm_db2_database/`.
  - Defined your ignore patterns in the `Diag_log_file_no_match_pattern_file.txt` file that is present in `$ORACLE_HOME/sysman/admin/scripts/emx/ibm_db2_database/`.
  - Set the DIAG_PATH configuration paramater of the database manager (instance) to correspond to the monitored IBM DB2 database.

  Based on the patters defined in the two files, the System Monitoring Plug-in for IBM DB2 parses the Diagnostic Log file and generates alerts for the satisfied conditions. First, the plug-in validates the two files to see if any patterns are defined. If no patterns are defined, then the plug-in does not parse the Diagnostic Log file. If matching patterns are not defined, but ignore patterns are defined, then the plug-in parses every entry in the Diagnostic Log file and checks if ignore patterns are satisfied. If matching patterns are also defined, then the plug-in first parses only those entries that satisfy the matching patterns, and then for those satisfied entries, the plug-in checks if ignore patterns are satisfied.

  Also, if multiple alerts are generated in a collection interval, and if the alerts have a common function name, then only one alert is generated represent the function name. This alert is based on the last log entry with a common function name, present in the Diagnostic Log file.

  Note: This feature is supported only for local monitoring, that is, when the IBM DB2 database on a host is monitored by an Oracle Management Agent that is running on the same host.

Setting Up the JDBC Driver

The JDBC driver is available from IBM, and consists of the following files that the Agent must be able to access:

- db2jcc.jar
- db2jcc_javax.jar

- db2jcc_license_cu.jar

To set up the IBM DB2 Universal Type 4 JDBC driver, do the following:

1. Create a `jdbcdriver` directory under `agent/sysman/` and place the `.jar` files listed above in that directory.
2. Add the location of each individual driver `.jar` file to the `classpath.lst` file under the `$ORACLE_HOME/sysman/config` directory.
3. If the Agent is installed on a system that is part of an OS cluster, then you need to edit the `classpath.lst` file under the `$ORACLE_HOME/<node_name>/sysman/config` directory, where `node_name` is the name of the system where the Agent is installed.

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

   ```
   /home/usera/agent/sysman/jdbcdriver/ibm/db2jcc.jar
   /home/usera/agent/sysman/jdbcdriver/ibm/db2jcc_javax.jar
   /home/usera/agent/sysman/jdbcdriver/ibm/db2jcc_license_cu.jar
   ```

Using a Suitable Operating System User and Assigning Authorities and Privileges

The System Monitoring Plug-In for IBM DB2 accesses the table functions used in IBM DB2. For the plug-in to have access to the table functions, you have to use a suitable operating system user and assign this new user to a user group. The operating ssytem user must have at least the minimum privileges. In addition, you have to assign the correct authority levels to this user.

> **Note:** IBM DB2 users must be operating system users. IBM DB2 cannot have its own database users because it relies on the host operating system for security.

If you do not have an operating system user already created, first, create one on the host where IBM DB2 is running. Then, follow these steps to assign this user to a new or existing UserGroup.

1. Open the IBM DB2 Control Center.
2. From the tree view, select the database or database alias to which you want to connect.
3. Connect as an admin user.
4. From the tree view, select **User and Group Objects**.
5. From the right pane, select the already-created operating system user.
6. From the Authorities panel, select **Connect to Database**.
7. To verify the applied changes, try connecting to the database.

Note: These steps can also be performed from command line using IBM DB2 SQL.

Also, assign authorities and privileges for the operating system UserGroup. The authorities supported with IBM DB2 are SYSADM, SYSCTRL, SYSMAINT, DBADM, and LOAD. The SYSADM, SYSCTRL, and SYSMAINT authorities cannot be granted using the GRANT SQL statement. These special authorities can only be set from the database manager configuration file. DBADM privilege can only be granted by user at SYSADM authorization level.

SYSMON authority level is required to monitor IBM DB2. This level is required to access the table functions, such as SYSPROC.SNAPSHOT_DATABASE, which are used in IBM DB2.

Follow these steps to set SYSMON authority level to your UserGroup:

1. At the db2=> prompt, run the following commands:

```
db2=> update dbm cfg using sysmon_group USERGROUP
db2 => db2stop
db2 => db2start
```

2. To check whether the changes are effective, run the following command:

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

The following will be the output of the previous command:

```
Database Manager Configuration
Node type = Enterprise Server Edition with local and remote clients
.....
   SYSADM group name     (SYSADM_GROUP)   =
   SYSCTRL group name    (SYSCTRL_GROUP)  =
   SYSMAINT group name   (SYSMAINT_GROUP) =
   SYSMON group name     (SYSMON_GROUP)   = USERGROUP
......
```

Note: To understand how authorities and privileges are implemented in IBM DB2, access the IBM Web site.

Deploying the Plug-in

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

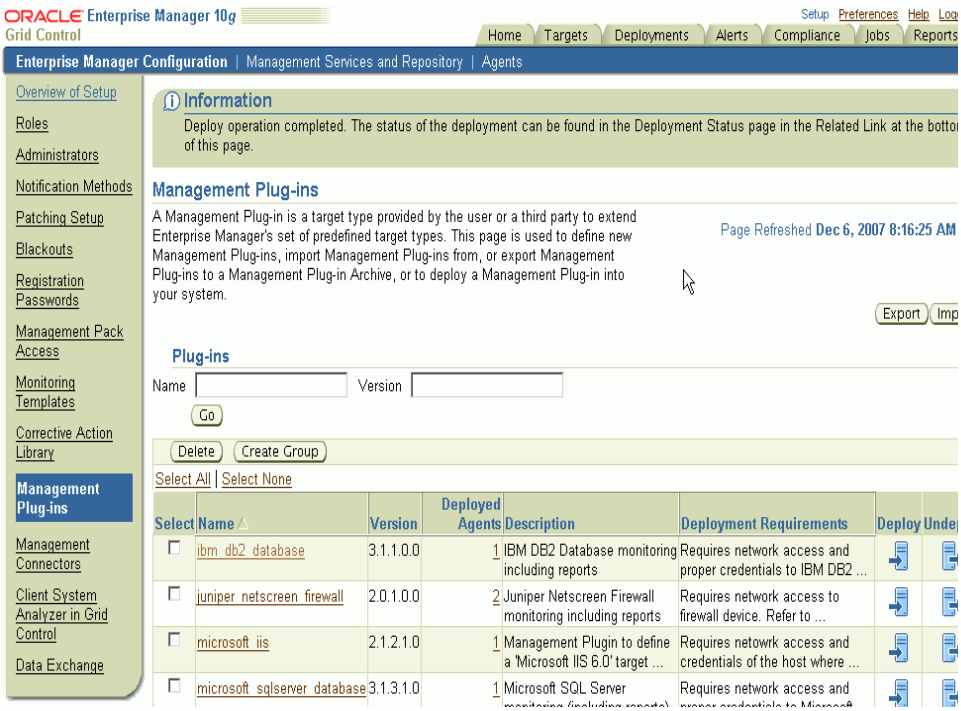
1. Download the IBM DB2 Database Plug-in archive to your desktop or computer on which the browser is launched. You can download the archive from the Oracle Technology Network (OTN).
2. Log in to Enterprise Manager Grid Control as a Super Administrator.
3. Click the **Setup** link in the upper right corner of the Grid Control Home page, then click the **Management Plug-ins** link on the left side of the Setup page.
4. Click **Import**.

5. Click **Browse** and select the plug-in archive.
6. Click **List Archive**.
7. Select the plug-in and click **OK**.
8. Verify that you have set preferred credentials on all Agents where you want to deploy the plug-in.
9. In the Management Plug-ins page, click the icon in the **Deploy** column for the DB2 Database plug-in. The Deploy Management Plug-in wizard appears.
10. Click **Add Agents**, then select one or more Agents to which you want to deploy the plug-in. The wizard reappears and displays the Agent you selected.
11. Click **Next**, then click **Finish**.

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

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

Figure 1 Successful Deployment



Configuring IBM DB2 for Health Indicator Metrics and Database Monitoring Metrics

The following sections explain the postinstallation configuration steps you need to perform on IBM DB2.

Configurations Required for Health Indicator Metrics

The health indicators for instance and database objects are enabled and disabled using the database manager configuration parameter -- HEALTH_MON. Then, the table functions -- HEALTH_TBS_HI, HEALTH_DB_HI, and HEALTH_DBM_HI get populated. These functions are used by the plug-in to show the alerts triggered based on the thresholds of health indicators.

> **Note:** Enabling these settings may result in some overheads, such as CPU and memory. Therefore, follow these 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 ste.

Configurations Required for Avoiding Metric Collection Errors for Database Monitoring Metrics

To avoid metric collection errors for for the "Database Monitoring" metrics, 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 BIM Web site.

Adding Instances for Monitoring

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

1. From the Agent home page where the plug-in was deployed, select the **IBM DB2 Database** target type from the **Add** drop-down list, then click **Go**. The Add IBM DB2 Database page appears.
2. Provide the following information for the properties:
   - **Name** — Name for the plug-in
   - **JDBC URL** — URL name for the IBM DB2 JDBC Driver connectivity.

     For example,

     `jdbc:db2://<server>:<port>/<database>`

     The JDBC URL argument represents a data source. Parameter definitions are as follows:

     – **jdbc:db2** — Indicates that the connection is to a DB2 UDB server.

     – **server** — Domain name or IP address of the database server.

     – **port** — TCP/IP server port number assigned to the database server, which is an integer between 0 and 65535.

     – **database** — Database alias, which refers to the DB2 database catalog entry on the DB2 client.

     The database name is determined by the DB2 server being used:

     DB2 for Linux, Unix, and Windows Servers — If the connection is to DB2 UDB for Linux, UNIX, and Windows servers, `database` is the database name defined during installation.
   - **JDBC Driver** — (Optional) Name of the DB2 Universal JDBC Driver.

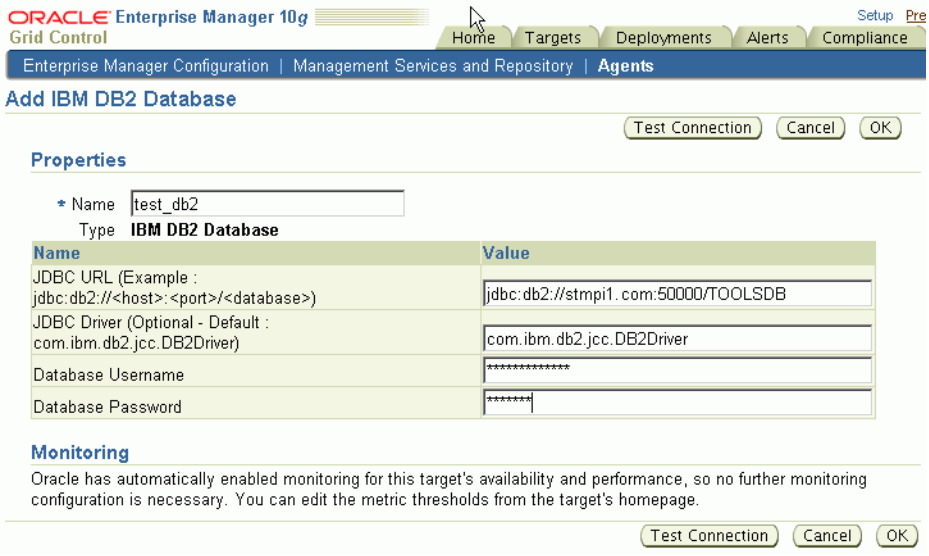
     For example,

     `com.ibm.db2.jcc.DB2Driver`
   - **Username** — Valid user name for the database.

     For more information, see Using a Suitable Operating System User and Assigning Authorities and Privileges.
   - **Password** — Password for the user.
3. Click **Test Connection** to make sure the parameters you entered are correct.

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

Figure 2 Add IBM DB2 Database



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

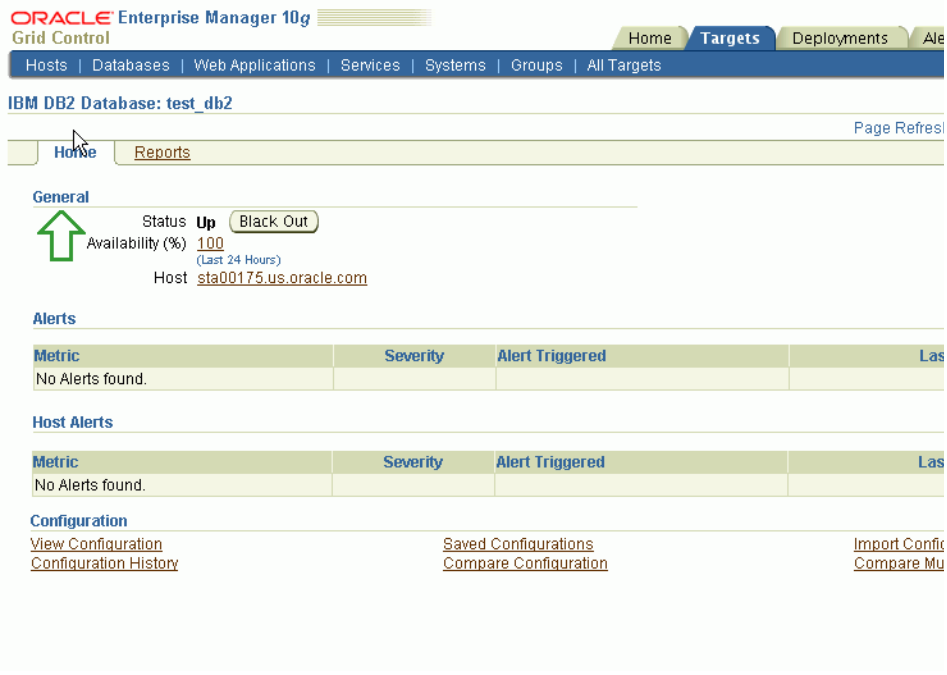
Verifying and Validating the Plug-in

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

1. Click the IBM DB2 Database target link from the Agent home page Monitored Targets table.

   The IBM DB2 Database home page appears.

Figure 3 IBM DB2 Database Home Page



2. Verify that no metric collection errors are reported in the Metrics table.
3. Ensure that reports can be seen by selecting the **Reports** property page.
4. Ensure that configuration data can be seen by clicking the **View Configuration** link in the Configuration section. If configuration data does not immediately appear, click **Refresh** in the View Configuration page.

Upgrading the Plug-in

Follow these steps to upgrade the plug-in:

1. Download the IBM DB2 Plug-in archive to your desktop or computer on which the browser is launched. You can download the archive from the Oracle Technology Network (OTN).
2. Log into Enterprise Manager Grid Control as a Super Administrator.
3. Click the **Setup** link in the upper right corner of the Grid Control Home page, then click the **Management Plug-ins** link on the left side of the Setup page.
4. Click **Import**.
5. Click **Browse** and select the plug-in archive that you have downloaded for upgrading.
6. Click **List Archive**.
7. Select the plug-in and click **OK.**
8. Verify that preferred credentials are set on all Agents to which you want to deploy the plug-in.

9. Blackout the IBM DB2 targets for agents to which you want to deploy higher version of the plug-in. Ensure that you select immediate blackout.
10. In the Management Plug-ins page, click the icon in the **Deploy** column for the IDM DB2 plug-in. The Deploy Management Plug-in wizard appears.
11. Click **Add Agents**, then select one or more Agents to which you want to deploy the plug-in. The wizard reappears and displays the Agent you selected.
12. Click **Next**, then click **Finish.**

    If you see an error message stating that the preferred credential is not set up, go to the Preferences page and add the preferred credentials for the Agent target type.
13. Remove blackout for the targets (required only if Step 9 applies).

Undeploying the Plug-in

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

1. Log in to Enterprise Manager Grid Control as a Super Administrator.
2. Select the **Targets** tab, then the **All Targets** subtab.
3. Select the DB2 Database Plug-in target and click **Remove**. You must do this step for all instances of the plug-in.
4. Make sure that the preferred credentials are set on the Agents where the plug-in is deployed.
5. Click the **Setup** link in the upper right corner of the All Targets page, then click the **Management Plug-ins** link on the left side of the Setup page. The Management Plug-ins page appears.
6. Click the icon in the **Undeploy** column for the IBM DB2 Database plug-in. The Undeploy Management Plug-in page appears.
7. Check all the Agents that are currently deployed with the DB2 Database Management plug-in and click **OK**.

   You must undeploy the plug-in from every Agent in the system to completely remove it from the enterprise.
8. Select the IBM DB2 Database Management Plug-in on the Management Plug-ins page and click **Delete**.

Troubleshooting the Plug-In

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

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

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

System Monitoring Plug-in Installation Guide for IBM DB2 Database, Release 7 (3.2.1.0.0)
E12306-02

Copyright © 2008, Oracle. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States 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, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software—Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.