

# Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for Sybase Adaptive Server Enterprise (ASE)

Release 7 (1.1.1.0.0) to Release 12 (1.3.1.1.0)

E12775-05

November 2010

---

This document provides a brief description about the Oracle System Monitoring Plug-in for Sybase Adaptive Server Enterprise, 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 Sybase Adaptive Server Enterprise extends Oracle Enterprise Manager Grid Control to add support for managing Sybase Adaptive Server instances. By deploying the plug-in within your Grid Control environment, you gain the following management features:

- Monitor Sybase Adaptive Server instances.
- Gather configuration data and track configuration changes for Sybase Adaptive Server instances.
- Raise alerts and violations based on thresholds set on monitored metrics and configuration data.
- Provide rich out-of-box reports based on the gathered data.
- Support monitoring by a remote Agent. Local Agent is an agent running on the same host as the Sybase Adaptive Server. Remote Agent is an agent running on a host that is different from the host where Sybase Adaptive Server is running.

## Versions Supported

This plug-in supports the following versions of products:

- Enterprise Manager 11g Grid Control Release 1 (11.1.0.1) or higher, or Enterprise Manager 10g Grid Control Release 2 (10.2.0.1) or higher (*Oracle Management Service and Oracle Management Agent*)
- Version 12.5.4 or higher of Express (XE), Enterprise (EE), and Developer (DE) editions of Sybase Adaptive Server

---

---

**Note:** The system monitoring plug-in for Sybase Adaptive Server is not certified for monitoring Sybase Adaptive Server Clusters. For more information, refer to the known issues described in the *Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide* available at:

<http://www.oracle.com/technetwork/oem/grid-control/documentation/index.html>

---

---

## Prerequisites

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

- Sybase Adaptive Server Enterprise version 12.5.4 or higher is installed.
- The following components of Oracle Enterprise Manager Grid Control are installed and running:
  - Oracle Enterprise Manager Grid Control 10.2.0.1 or higher
  - Oracle Management Agent 10.2.0.1 or higher (any platform supported by this release of agent)

You can install the agent on the same computer as Sybase Adaptive Server (referred to as local agent monitoring), or you can install the agent on a different computer from Sybase Adaptive Server (referred to as remote agent monitoring).

- Preferred credentials are set and validated on all agents where you want to deploy the plug-in. For more information, see "[Configure the Management Agent to Deploy the Plug-In](#)".
- (For Agent running on Microsoft Windows) The OS privileges for the user (set in the Preferred Credentials for the Agent) must meet the requirements documented in the "*Setting Credentials for the Job System to Work with Enterprise Manager*" section of the *Oracle Database Installation Guide for Microsoft Windows* available at the following locations:

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

[http://www.oracle.com/pls/db112/portal.portal\\_db?selected=11&frame=#microsoft\\_windows\\_installation\\_guides](http://www.oracle.com/pls/db112/portal.portal_db?selected=11&frame=#microsoft_windows_installation_guides)

- **Oracle Database 11g Release 1 (11.1)**

[http://www.oracle.com/pls/db111/portal.portal\\_db?selected=11&frame=#microsoft\\_windows\\_installation\\_guides](http://www.oracle.com/pls/db111/portal.portal_db?selected=11&frame=#microsoft_windows_installation_guides)

- **Oracle Database 10g Release 2 (10.2)**

<http://www.oracle.com/pls/db102/homepage>

---

---

**Note:** If you do not assign the correct privileges for users, the deployment will fail.

---

---

- The MDA tables must be installed before they can be queried. The MDA tables only exist on 12.5.0.3 and higher. To install MDA tables, do the following:

1. Ensure that the configuration parameter enable cis is set to 1. If not, restart ASE. Run the following command:

```
sp_configure 'enable cis', 1
go
```

2. Add 'loopback' server name alias (assuming @@servername is also defined in the interfaces file). This step is no longer required in 15.0 ESD#2 or later.

```
use master
go
sp_addserver loopback, null, @@servername
go
```

3. Test this configuration. This step is no longer required in 15.0 ESD#2 or later.

```
set cis_rpc_handling on
go
```

Alternatively, run the following command and then disconnect and reconnect your session:

```
sp_configure 'cis rpc handling', 1
exec loopback...sp_who -- note: 3 dots!
go
```

4. Install the MDA tables. Do not run this script with 'sqsh' as it will cause errors. 'sqsh' sees a '\$' as the start of a sqsh variable, and this distorts the native RPC names, since these start with a '\$' as well. Instead, either use 'isql' as below, or run 'sqsh' with the '-Lexpand=0' option to disable sqsh variable expansion feature. For ASE 15.0.2 and higher, this script is included in the installmaster.

```
isql -U sa -P yourpassword -S YOURSERVER \
-i $$SYBASE/$$SYBASE_ASE/scripts/installmontables
```

5. Assign mon\_role to logins allowed MDA access. This also applies to the 'sa' login.

```
use master
go
grant role mon_role to sa
go
```

6. Test basic MDA configuration as follows. You may need to disconnect and reconnect to activate mon\_role when you grant this role to the login you are currently using.

```
select * from master..monState
go
```

7. Enable all configuration parameters. These are all dynamic (except the per object statistics active parameter). For all 'pipe' tables, the number of messages is set to 100 here, but you can choose a larger size.

```

sp_configure "enable monitoring", 1
go
sp_configure "sql text pipe active", 1
go
sp_configure "sql text pipe max messages", 100
go
sp_configure "plan text pipe active", 1
go
sp_configure "plan text pipe max messages", 100
go
sp_configure "statement pipe active", 1
go
sp_configure "statement pipe max messages", 100
go
sp_configure "errorlog pipe active", 1
go
sp_configure "errorlog pipe max messages", 100
go
sp_configure "deadlock pipe active", 1
go
sp_configure "deadlock pipe max messages", 100
go
sp_configure "wait event timing", 1
go
sp_configure "process wait events", 1
go
sp_configure "object lockwait timing", 1
go
sp_configure "SQL batch capture", 1
go
sp_configure "statement statistics active", 1
go
sp_configure "per object statistics active", 1
go

```

8. For ASE 15.0.2, also run the following command:

```

sp_configure "enable stmt cache monitoring", 1
go

```

9. Set the following static parameter to a higher value (the setting is in bytes per user connection) if you're expecting a lot of (or long) SQL batches:

```

sp_configure "max SQL text monitored", 2048
go

```

---



---

**Note:** Enabling the following configuration parameters will result in >5% performance overhead:

```

sp_configure "sql text pipe active", 1
sp_configure "sql text pipe max messages", 100
sp_configure "max SQL text monitored", 2048
sp_configure "plan text pipe active", 1
sp_configure "plan text pipe max messages", 100
sp_configure "statement pipe active", 1
sp_configure "statement pipe max messages", 100
sp_configure "statement statistics active", 1
sp_configure "per object statistics active", 1

```

---



---

- As part of JDBC URL, either IP Address or host name can be provided. Ensure that the host name can be resolved consistently on the network. Standard TCP tools such as "nslookup" and "tracert" can be used to verify the host name. Validate using the following commands on Management Agent where plug-in is deployed:
  - nslookup <hostname>  
This returns the IP address and fully qualified host name.
  - nslookup <IP>  
This returns the IP address and fully qualified host name.
- The plug-in may sometimes depend on the cache size of the TemDB.
- For Release 11, if the monitoring user does not have permission on all databases in Sybase ASE target, provide permission to query SYSSEGMENTS table to monitoring user or else create guest user account in each database.

## Configuring Sybase Adaptive Server for Monitoring

To monitor the Sybase Adaptive Server target using Enterprise Manager, the Sybase Adaptive Server user must have the role mon\_role. In addition to mon\_role permissions, the monitoring user must also have Select permissions to access the following sys tables:

- syslisteners
- sysloginroles
- sysserverroles

The following commands will grant Select permission to the monitoring user:

```
grant select on syslisteners to public
go
grant select on sysloginroles to public
go
grant select on sysserverroles (name, srid) to public
go
```

The above steps will give Select permission to all existing users in the database. To grant Select permission to only the monitoring user, referred to as monuser below, run the following commands. To execute these commands, the user must have sa\_role permissions.

### 1. Create a group.

```
sp_addgroup OracleEMGroup
go
```

### 2. Add the user monuser to the group.

```
sp_adduser monuser, null, OracleEMGroup
go
```

### 3. Grant Select permission on the tables to OracleEMGroup.

```
grant select on syslisteners to OracleEMGroup
go
grant select on sysloginroles to OracleEMGroup
go
```

```
grant select on sys$sys$roles (name, srid) to OracleEMGroup
go
```

## Configure the Management Agent to Deploy the Plug-In

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

### Assigning Advanced Privileges to User

(For Microsoft Windows ONLY) To assign advanced privileges in a Microsoft Windows environment, do the following:

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

### Setting and Validating Preferred Credentials

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

1. In Enterprise Manager Grid Control, click **Preferences**.
2. In the Preferences page, click **Preferred Credentials** in the left pane.  
The Preferred Credentials page appears.
3. For the corresponding Target Type, for the Host target type, from the **Set Credentials** column, click the icon.

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

## Deploying the Plug-in

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

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

Figure 1 shows the Management Plug-ins page.

**Figure 1 Management Plug-ins Deployment Page**

The screenshot displays the Oracle Enterprise Manager 10g interface for the Management Plug-ins page. The top navigation bar includes links for Home, Targets, Deployments, Alerts, Compliance, Jobs, and Reports. The left sidebar contains various configuration options like Roles, Administrators, Notification Methods, Patching Setup, Blackouts, Registration Passwords, Management Pack Access, Monitoring Templates, Corrective Action Library, Management Plug-ins, Management Connectors, Client System Analyzer in Grid Control, and Data Exchange. The main content area features an information box stating 'Deploy operation completed. The status of the deployment can be found in the Deployment Status page in the Related Link at the bottom of this page.' Below this is a section titled 'Management Plug-ins' with a search bar and buttons for Delete, Export, and Import. A table lists the installed plug-ins:

Select	Name	Version	Deployed Agents	Description	Deployment Requirements	Deploy	Undeploy
<input type="checkbox"/>	sybase_ase	1.0.3.0.0	1	This plug-in offers monitoring, configuration and ...	Requires network access and proper credentials to Sybase ...		

Below the table, there are 'Related Links' including 'Deployment Status'.

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 Sybase Adaptive Server plug-in. The Deploy Management Plug-in wizard appears.
10. Click **Add Agents**, then select one or more agents to which you want to deploy the plug-in. The wizard reappears and displays the agent you selected.
11. Click **Next**, then click **Finish**.  

If you see an error message stating that the preferred credential is not set up, go to the Preferences page and add the preferred credentials for the Agent target type.
12. To check the deployment status, go to Related Links and click the link **Deployment Status**.

## Setting up the JDBC Driver

Following are the steps to set up jConnect for the Sybase Adaptive Server plugin:

1. Download the jConnect JDBC driver version 6.0 from [www.sybase.com](http://www.sybase.com).
2. Create a `jdbcdriver` directory under `$ORACLE_HOME/sysman` and place the .jar files listed above in that directory.
3. Add the location of the driver .jar file to the `classpath.lst` file under the `$ORACLE_HOME/sysman/config` directory.
4. If the agent is installed on a system that is part of an OS cluster, 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 clustered node where the agent is running.

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/sybase/jConn3.jar
```

## TCP/IP Port Information

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

## Enabling TCP/IP Port

### For all editions of Sybase Adaptive Server

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

The right panel displays all protocols for the specified Sybase Adaptive 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 Sybase Adaptive Server instance.

## Finding TCP/IP Port

To find the TCP/IP port number for a particular Sybase Adaptive Server instance, run the following query:

```
Select address_info from syslisteners
```

The above query returns the host address followed by the port number.

## 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 Sybase Adaptive Server target type from the **Add** drop-down list, then click **Go**. The Add Sybase Adaptive Server page appears as shown in [Figure 2](#).

**Figure 2 Configuration Properties Page**

The screenshot shows the Oracle Enterprise Manager 10g interface. The page title is "Add Sybase Adaptive Server Enterprise". The "Properties" section is expanded, showing the following table:

Name	Value
JDBC URL	jdbc:sybase:Tds:stmp2.idc.oracle.com:4100
JDBC Driver	com.sybase.jdbc3.jdbc.SybDriver
Database Username	**
Database Password	*****

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

2. Provide the following information for the properties:

- **Name** — Unique target name across all the Grid Control targets, such as SybaseServer\_Hostname. This is the display name in the Grid Control. It represents this Sybase Adaptive Server target across all user interfaces within Grid Control.
  - **JDBC URL** — Provide the URL in the format  
jdbc:sybase:Tds:<system>:<tcp/ip port>  
For example, jdbc:sybase:Tds:stmpi2.idc.oracle.com:5000
  - **JDBC Driver** — Optional parameter. Provide this value in the format com.sybase.jdbc3.jdbc.SybDriver
  - **Database Username** — Valid user for the database in mon\_role.
  - **Password for the Database User** — Corresponding password for the database 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**.

---

---

**Important:** If you do not reenter the encrypted parameters before clicking **OK**, you might encounter an error suggesting that the login failed.

---

---

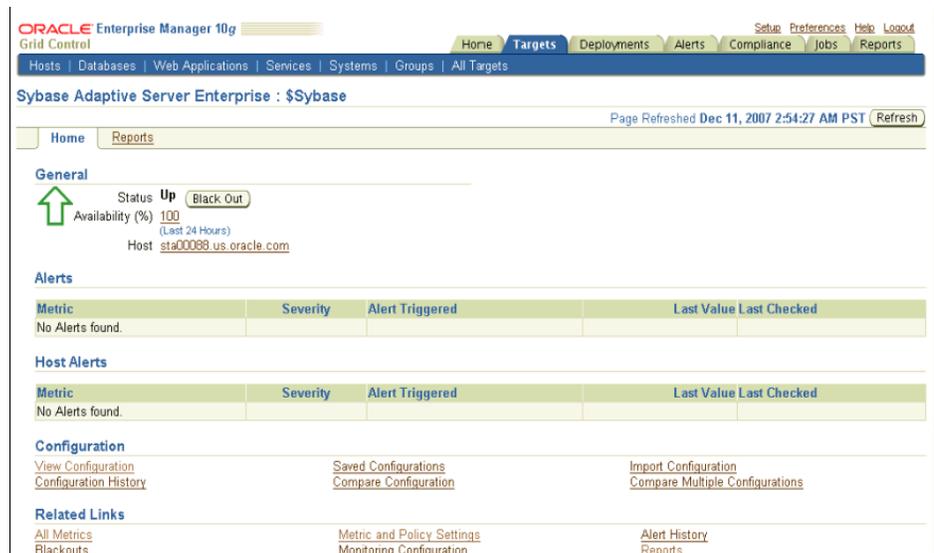
After you deploy and configure the plug-in to monitor one or more targets in the environment, you can customize the monitoring settings of the plug-in. This alters the collection intervals and threshold settings of the metrics to meet the particular needs of your environment. If you decide to disable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

## Verifying and Validating the Plug-in

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

1. Click the Sybase Adaptive Server target link from the Agent home page Monitored Targets table. The Sybase Adaptive Server home page appears.  
The Sybase Adaptive Server home page appears as shown in [Figure 3](#).

**Figure 3 Sybase Adaptive Server Home Page**



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

## Undeploying the Plug-in

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

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

You must undeploy the plug-in from every agent in the system to completely remove it from the enterprise.

8. Select the Sybase Adaptive Server Plug-in on the Management Plug-in page and click **Delete**.

## Troubleshooting the Plug-In

If the following parameters are not enabled for the Sybase Adaptive Server plug-in, metric collection errors may occur:

```
sp_configure "sql text pipe active", 1
sp_configure "sql text pipe max messages", 100
sp_configure "max SQL text monitored", 2048
sp_configure "plan text pipe active", 1
sp_configure "plan text pipe max messages", 100
sp_configure "statement pipe active", 1
sp_configure "statement pipe max messages", 100
sp_configure "statement statistics active", 1
sp_configure "per object statistics active", 1
```

## Documentation Accessibility

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

### Accessibility of Code Examples in Documentation

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

### Accessibility of Links to External Web Sites in Documentation

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

### Deaf/Hard of Hearing Access to Oracle Support Services

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

---

System Monitoring Plug-in Installation Guide for Sybase Adaptive Server Enterprise (ASE), Release 7 (1.1.1.0.0) to Release 12 (1.3.1.1.0) E12775-05

Copyright © 2010, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please

report them to us in writing.

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 52.227-19, 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, then you shall be responsible to take all appropriate fail-safe, backup, 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 expressly 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, costs, or damages incurred due to your access to or use of third-party content, products, or services.

