Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for Oracle Virtual Networking

Release 12.1.0.2.0

E40873-02

October 2013

This document describes how to install and use the System Monitoring plug-in to monitor Oracle Virtual Networking systems within Oracle Enterprise Manager.

The following topics are discussed in this document:

- Introduction to the Oracle Virtual Networking Plug-in
- Requirements
- Obtain and Deploy the Plug-in
- Verify and Validate the Plug-in
- View Monitoring Information
- Undeploy the Plug-in
- Troubleshooting the Plug-in

Introduction to the Oracle Virtual Networking Plug-in

The System Monitoring plug-in for Oracle Virtual Networking (OVN) extends Oracle Enterprise Manager Cloud Control to add support for monitoring Oracle Virtual Networking systems.

The Oracle Fabric Manager (OFM), also known as the Xsigo Fabric Manager (XFM), monitors the Oracle Virtual Networking systems. When you deploy and configure the plug-in in your Enterprise Manager Cloud Control 12c environment, a summary of the network components, change information, alerts, and violations are visible in the UI.

For more information about the data that is monitored by this plug-in, see View Monitoring Information.

Requirements

This section describes what is needed to enable monitoring of the Oracle Virtual Networking systems:

- Supported Versions
- Prerequisites

Supported Versions

The plug-in supports the following Oracle Enterprise Manager versions:

- Oracle Enterprise Manager 12c Cloud Control Release 3 (12.1.0.3.0) or higher.

- Oracle Enterprise Manager Management Agent version 12.1.0.3.0 or higher.

Prerequisites

Perform the following tasks before deploying the plug-in:

- Make sure you have Oracle Enterprise Manager 12c Cloud Control Release 3 (12.1.0.3.0) or a higher version installed.
- Ensure that the Management Agent has access to the computer on which Oracle Fabric Manager is running.
- Install the Xsigo Fabric Manager 4.1.0 / Oracle Fabric Manager 4.2.0 or higher with "Enterprise Manager" plug-in. For more information, refer to the readme file included in the plug-in.
- In the machine on which the agent is installed, import the Oracle Fabric Manager certificate into a new or existing TrustStore. The OFM certificate file should be provided by the OFM Administrator.

  Use the JDK keytool to import the Oracle Fabric Manager certificate into a TrustStore as follows:

  ```
  keytool -import -file <certificate_filename> -alias <alias> -keystore
  <truststore_filename>
  ```

  For more information about the certificate configuration for Oracle Fabric Manager or Xsigo Fabric Manager, visit the *User Guide* at:

  http://docs.oracle.com/cd/E38500_01/

Obtain and Deploy the Plug-in

Complete the following tasks to obtain and deploy the plug-in:

1. Download the Plug-in From the Enterprise Manager Store
2. Deploy the Plug-in to the Management Server
3. Add Targets for Monitoring

The Oracle Enterprise Manager Store is an external site that contains functional updates, including the latest version of the management plug-in files. Enterprise Manager Cloud Control checks the site periodically to provide you with the latest version. You can download the plug-in from the Oracle Enterprise Manager Store to the Software Library (the local store).

> **Note:** Oracle Enterprise Manager must have Internet access to download the plug-in from the Oracle Enterprise Manager Store.

Things to Know

The following are things you should know before you deploy the plug-in:

- You can import multiple versions of the same plug-in. However, you can only deploy one version on the Oracle Management Service (OMS) at any given time.
- The Management Agent can have the same or earlier version of the plug-in that is deployed on the OMS host.

- The Management Agent cannot have a later version than the version that is on the OMS host.
- The Management Repository SYSMAN user password is required to complete the deployment process.

Download the Plug-in From the Enterprise Manager Store

This procedure assumes that you are connected to the Internet and describes how to download the plug-in immediately. Alternatively, you can choose to schedule the download to occur at a specified time.

1. From the **Setup** menu, click **Extensibility**, then click **Self Update** to get the list of updates.
2. Click **Plug-in** from the list.
3. Select **Oracle Virtual Networking** from the list, then click **Download**.
4. Select **Immediately**, then click **Select** to start downloading the update.

   The plug-in deployment page appears when the download completes.

Deploy the Plug-in to the Management Server

The Management Repository SYSMAN user password is required to complete the deployment process.

1. On the Plug-in Deployment page, select the Enterprise Manager for Oracle Virtual Networking plug-in.

   If you are not on the Plug-in Deployment page, expand the **Setup** menu and click **Extensibility**, then click **Plug-ins**.
2. Click **Deploy On**, then click **Management Servers**.
3. Complete the required details on the Deploy Plug-in dialog box.

   In the Version of Plug-in to Deploy section, select the Plug-in version from the Plug-in drop-down. The Target Type information is displayed in the table. Enter the Repository SYSMAN password, then click **Continue**.
4. Complete the steps in the Deploy Plug-in dialog box.
5. Click **Deploy** to deploy the selected plug-in on all Enterprise Manager Servers.

Add Targets for Monitoring

You must associate the Oracle Virtual Networking Plug-in to existing Oracle Enterprise Manager Cloud Control agents to enable centralized monitoring.

See the *Oracle Enterprise Manager Cloud Control 12c Administrator's Guide* for how to add new targets in Oracle Enterprise Manager Cloud Control.

1. Log in to Oracle Enterprise Manager Cloud Control as SYSMAN.
2. From the **Setup** menu, click **Add Target**, then click **Add Targets Manually**.
3. Select **Add Targets Declaratively by Specifying Target Monitoring Properties**, then select the **Oracle Virtual Networking** target type, select a Monitoring Agent, then click **Add Manually**.
4. Complete the following information:

a. **Target Name**: The unique target name that is displayed in the Oracle Enterprise Manager Cloud Control UI.

b. **Store Location**: The path to the TrustStore file.

c. **Store Type**: The file format must be JKS.

d. **Store Password**: Any value is accepted.

e. **Oracle Virtual Networking User Name**: The user log in name for the Oracle Fabric Manager.

f. **Oracle Virtual Networking Password**: The corresponding password for the Oracle Fabric Manager.

g. **Oracle Virtual Networking Host Name**: The host name or IP address for the Oracle Fabric Manager.

5. Click **OK** to add the new target.

After deploying and configuring 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 specific needs of your environment.

Verify and Validate 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 Oracle Enterprise Manager Cloud Control is properly monitoring the plug-in target:

1. Click the Oracle Virtual Networking target link from the Monitoring Target table on the Agent home page.
2. Verify that no metric collection errors are reported in the Metric table.

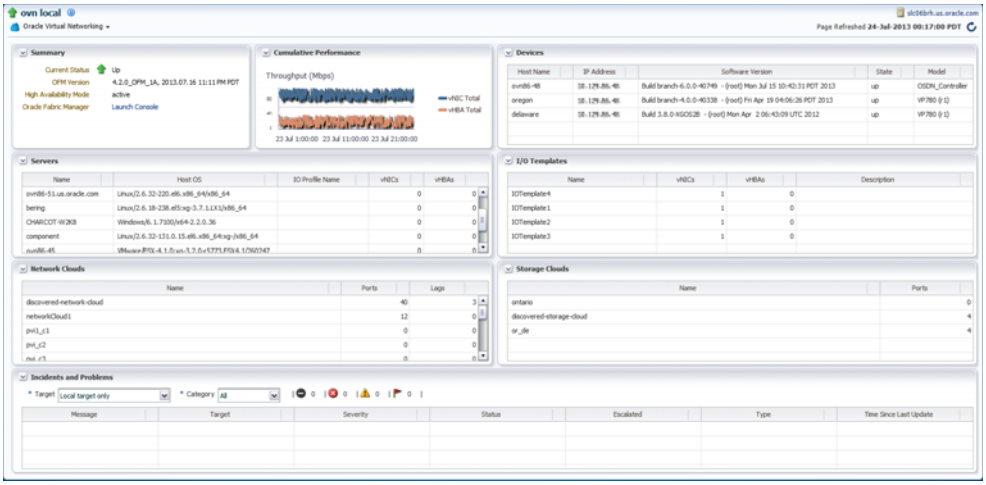
View Monitoring Information

You can monitor the information about the Oracle Fabric Manager, cumulative performance, the managed devices, the discovered servers, the configured I/O templates, network and storage clouds, and the alarms tracked by the Oracle Fabric Manager.

To view this monitoring information, do the following:

1. Select the All Targets option from the Targets menu.
2. Click the Oracle Virtual Networking target from the All Targets table.

Figure 1 Oracle Virtual Networking Plug-in UI



Summary

Oracle Fabric Manager supports high availability mode, in which multiple Fabric Manager servers are associated with each other to provide a system of Fabric Manager servers that operate in active or passive roles.

In the summary section of the OVN plug-in UI, you can find the current Oracle Fabric Manager's status and version, and the high availability mode.

Cumulative Performance

When vNICs and vHBAs are configured and deployed on the host server, you can see in a graph the network and storage total throughput.

Devices

Information about the Oracle Fabric Interconnect chassis and the Oracle SDN that are managed through the Oracle Fabric Manager is displayed in the OVN plug-in UI. You can see the host name of each managed device, the device IP address, the software version currently installed on each managed device, the current state of the managed device and the model of the device.

Servers

Oracle Fabric Manager discovers servers that are connected through the devices and have Oracle Virtual Networking Drivers installed.

You can see in the OVN plug-in UI the host name of each server that Oracle Fabric Manager has discovered, the operating system currently in use on the host server, the name of the I/O profile bound to each server, and the total number of vNICs and vHBAs that are configured on the server.

I/O Templates

When I/O templates are configured, they are listed in the OVN plug-in UI regardless of whether they are deployed to a host server or not.

You can see the name of each configured I/O template, the total number of vNICs and vHBAs configured in each I/O template, and the description that was applied to the I/O template.

Network Clouds

Information about the Private Virtual Interconnect (PVI) clouds is displayed in the OVN plug-in UI.

If Oracle Fabric Interconnect is attached you can see the name of each configured cloud, the number of Ethernet ports, and link aggregation groups (LAGs) in the cloud.

Storage Clouds (only for Oracle Fabric Interconnect)

Information about the configured storage clouds is displayed in the OVN plug-in UI. You can see the name of each configured cloud, and the number of Fibre Channel ports in the storage cloud.

Alarms

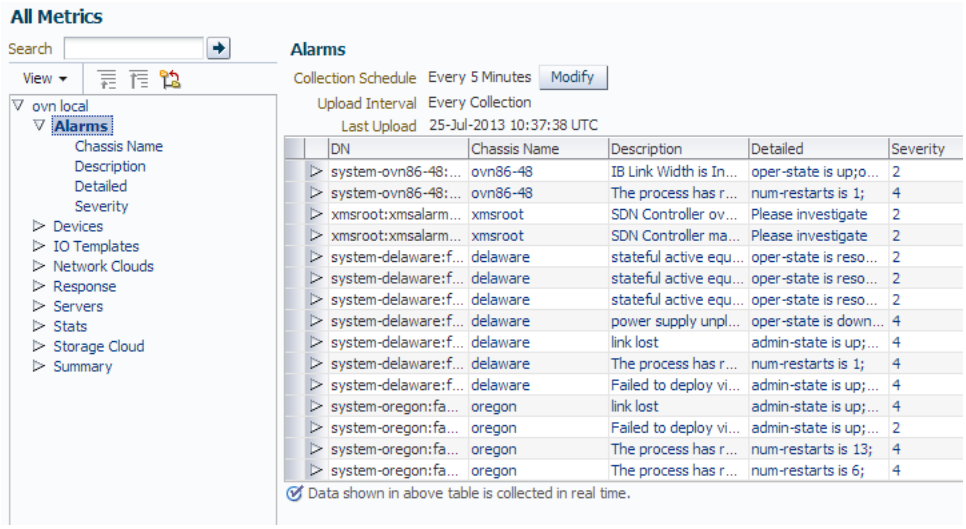
The Oracle Virtual Networking plug-in monitors system events and network management alarms tracked by the Oracle Fabric Manager.

The alarms shown in the OVN plug-in UI are of one of the following severities:

- Critical
- Major
- Minor
- Warning

To view critical, major, minor, and warning alarms go to the All Metrics page, and select the Alarms metric. Critical alarms are displayed in the Incidents and Problems section of the OVN plug-in UI. Major, warning and minor alarms can also appear on the Incidents and Problems section, if the user activates a rule for this purpose.

Figure 2 Alarms Shown in the All Metrics Page



For more information about the monitoring information tracked by the Oracle Fabric Manager, see the following:

- *Oracle Fabric Manager User's Guide*
- Oracle Fabric Interconnect Documentation

These documents are available at http://docs.oracle.com/cd/E38500_01/.

Undeploy the Plug-in

Removing a plug-in removes all of its metadata from the Management Repository.

1. From the Setup menu, click **Extensibility**, then click **Plug-ins**.
2. Select the row for the plug-in you want to remove in the table.
3. Click **Undeploy From**, then click either **Management Servers** or **Management Agent**. You can then select the OMS or Management Agent you want to remove the plug-in from.
4. Confirm the plug-in removal. Enterprise Manager notifies the connected and relevant Enterprise Manager users and begins the deconfiguration process.

For more information about how to remove or undeploy a plug-in, refer to the Oracle Enterprise Manager documentation.

Troubleshooting the Plug-in

This section contains information to help you troubleshoot issues you encounter while installing the Oracle Virtual Networking plug-in.

Alert Issues

Only the Critical Alert displayed on the Incidents Problems Region

Action –You should create an incident rule to view other Oracle Virtual Networking systems alarms.

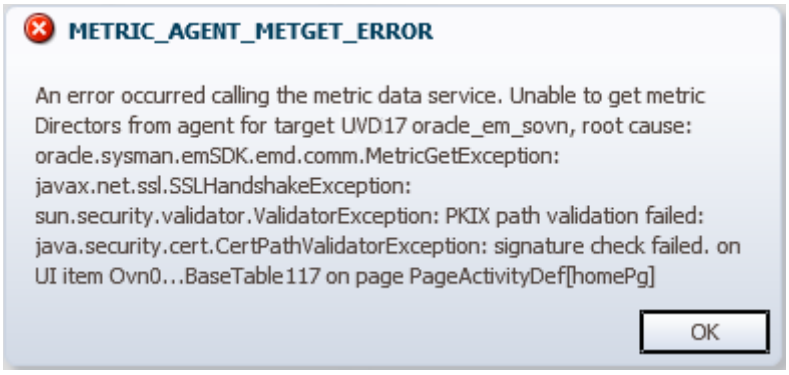
Metric Collection Issues

The following issues are related to metrics that do not show data or show metric collection error.

Error message: CertPathValidatorException: Signature Check Failed

Cause – The TrustStore file may not be appropriate.

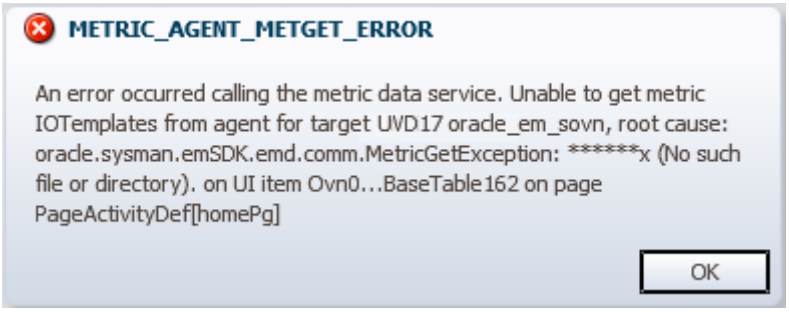
Figure 3 UI Error Message, CertPathValidatorException: Signature Check Failed



Error message: MetricGetException: No Such File or Directory

Cause – The TrustStore path may be incorrect.

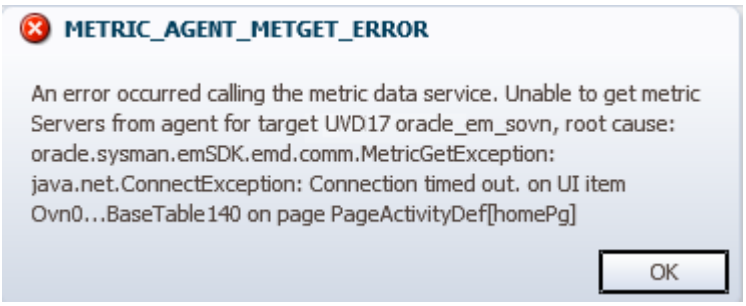
Figure 4 UI Error Message, MetricGetException: No Such File or Directory



Error message: ConnectException: Connection Timed Out

Cause – Incorrect host name or IP address or no access to Oracle Virtual Networking host.

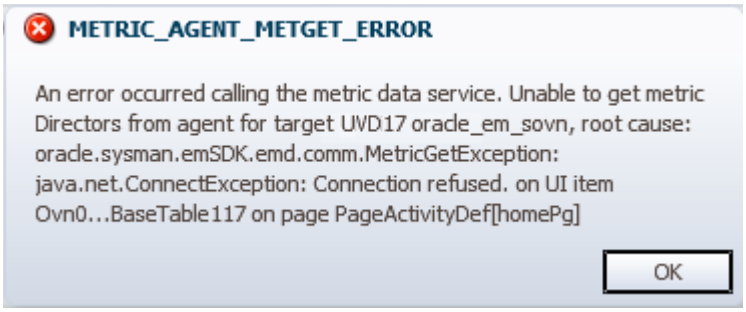
Figure 5 UI Error Message, ConnectException: Connection Timed Out.



Error message: ConnectException: Connection Refused

Cause – Oracle Fabric Manager is not running, the server is down.

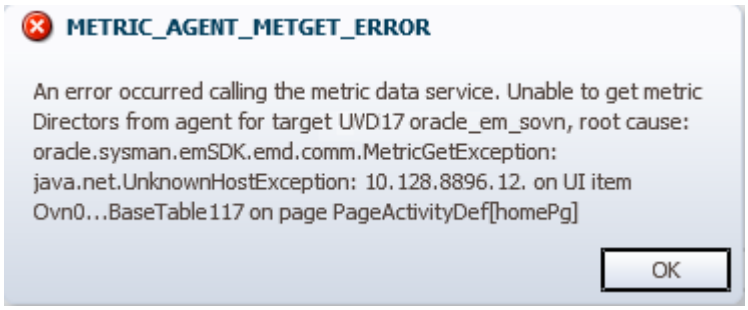
Figure 6 UI Error Message, ConnectException: Connection Refused



Error message: MetricGetException: UnknownHostException

Cause – Incorrect host name or IP address.

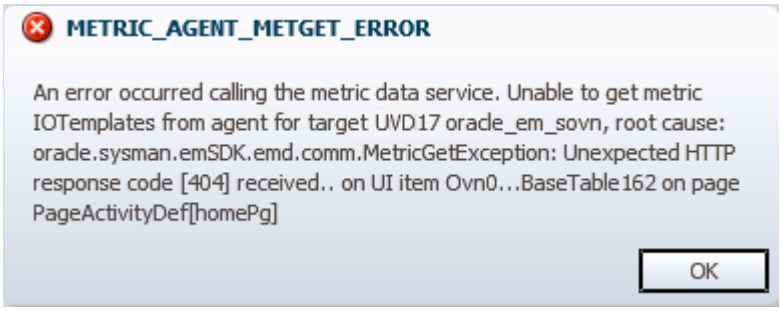
Figure 7 UI Error Message, MetricGetException: UnknownHostException



Error message: MetricGetException: Unexpected HTTP Response Code [404]

Cause – The Enterprise Manager plug-in is not installed on Oracle Fabric Manager or Xsigo Fabric Manager. For more information, refer to the readme file included in the Enterprise Manager plug-in.

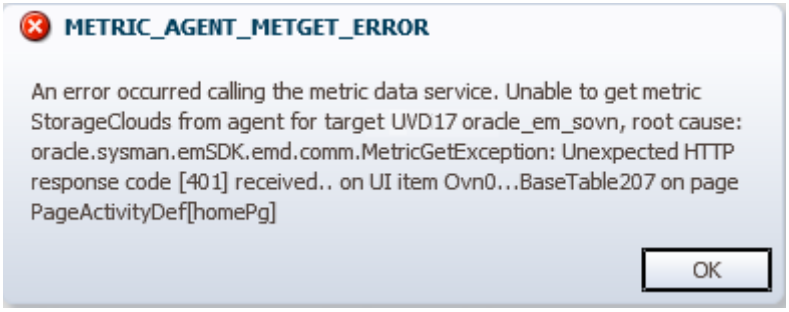
Figure 8 UI Error Message, MetricGetException: Unexpected HTTP Response Code [404]



Error message: MetricGetException: Unexpected HTTP Response Code [401] Received.

Cause – User name or password not match.

Figure 9 UI Error Message, MetricGetException: Unexpected HTTP Response Code [401] received



Solving Metric Collection Issues

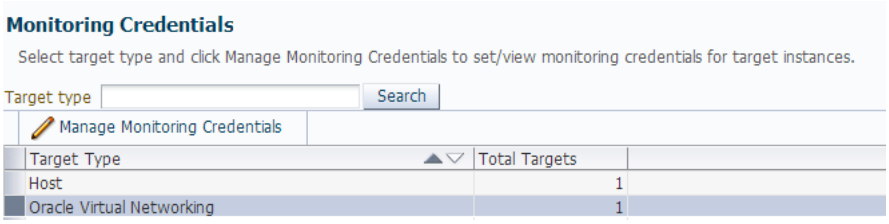
To solve some metrics collection issues, you should manage the credentials sets or the host name properties.

Manage TrustStore and UserCredential Sets

To manage TrustStore and UserCredential sets, do the following:

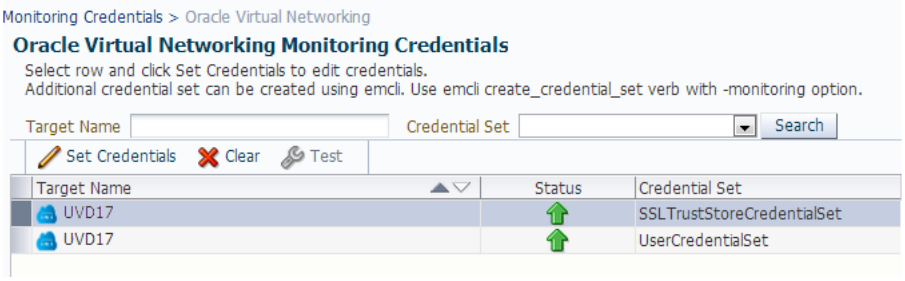
1. Click **Setup**, then **Security** and finally **Monitoring Credentials**.

Figure 10 Select Monitoring Credentials



2. Select Oracle Virtual Networking target and click **Manage Monitoring Credentials**.

Figure 11 Select SSLTrustStoreCredentialsSet/ UserCredentialSet



****

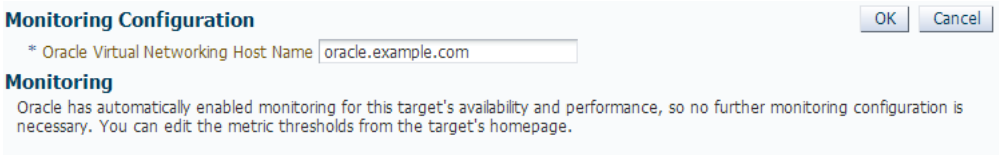
3. Select SSLTrustStoreCredentialsSet and UserCredentialSet and click **Set Credentials**.

Manage Host Name Property

To manage the host name or IP address properties, do the following:

1. Click **Oracle Virtual Networking**, then **Target Setup** and finally **Monitoring Configuration**.

Figure 12 Monitoring Configuration



Documentation Accessibility

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

Access to Oracle Support

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

Oracle Enterprise Manager System Monitoring Plug-in Installation Guide for Oracle Virtual Networking, Release 12.1.0.2.0
E40873-02

Copyright © 2007, 2013, 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 is software or related documentation that 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 END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware 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 that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware 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.