

Oracle® Health Sciences Information Manager

Cross Community Access User's Guide

Release 3.0

E61377-01

March 2015

This guide provides information on Oracle Health Sciences Information Manager (OHIM) Cross-Community Access (XCA) Gateway. It describes features and functionalities of Gateway, Integrating the Healthcare Enterprise (IHE) standards, and Web Services with their configuration options.

This document is intended for Oracle Health Information XCA Gateway users.

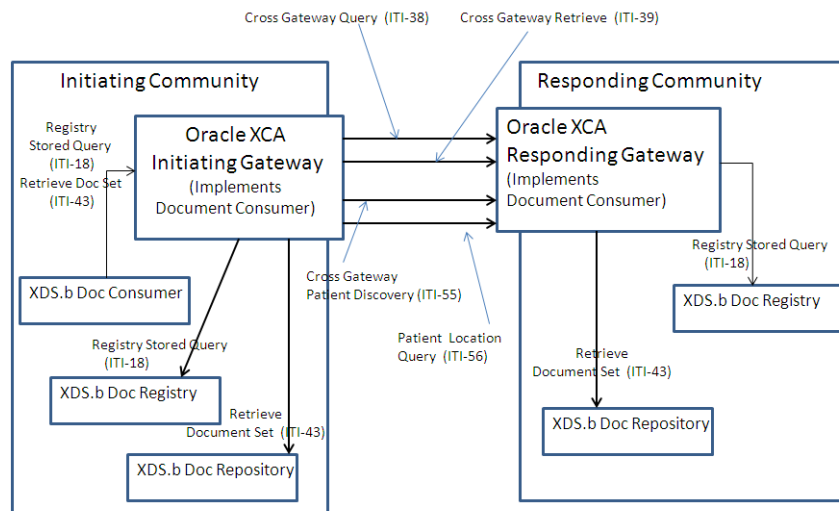
Overview

The XCA Profile supports the means to query and retrieve patient relevant medical data held by other communities. The Cross-Community Patient Discovery (XCPD) Profile supports the means to locate communities that hold patient relevant health data and the translation of patient identifiers across communities holding the same patient's data.

Cross-Enterprise Document Sharing Actors and Transactions

Figure 1 shows the XDS actors and transactions among them.

Figure 1 XDS Actors and Transactions



Actors and Transactions Supported by Gateway

XCA supports the following IHE profiles and transactions:

Table 1 Actors and Transactions Supported by XCA

Actors	Transactions
Initiating Gateway (IG)	Cross Gateway Query (ITI-38)
Initiating Gateway	Cross Gateway Retrieve (ITI-39)
Initiating Gateway	Registry Stored Query (ITI-18)
Initiating Gateway	Retrieve Document Set (ITI-43)
Responding Gateway (RG)	Cross Gateway Query (ITI-38)
Responding Gateway	Cross Gateway Retrieve (ITI-39)

Table 2 Actors and Transactions Supported by XCPD

Actors	Transactions
Initiating Gateway	Cross Gateway Patient Discovery (ITI-55)
Responding Gateway	Patient Location Query (ITI-56)
Responding Gateway	Cross Gateway Patient Discovery (ITI-55)
Responding Gateway	Patient Location Query (ITI-56)

Services Provided

All of the IHE ITI transactions supported by XCA and XCPD are supported through SOAP 1.2 based Web Services. The following are the SOAP 1.2 Web Services supported by XCA and XCPD:

- Initiating Gateway Service (Registry Stored Query, Retrieve Document set, Patient Discovery, Cross Gateway Query, Cross Gateway Retrieve)
- Responding Gateway Service (Patient Discovery, Cross Gateway Query, Cross Gateway Retrieve)

Web Services

Web Services are implemented using JAX-WS Web Services API and stack on Oracle WebLogic server. For more information on Web Service definitions and related IHE XDS, XCA, and XCPD transactions, see IHE IT Infrastructure XDS, XCA, and XCPD Profile specifications.

Core Gateway Service

The following Web Services operations and IHE transactions are supported for Core Gateway Services:

- ITI-18 Registry Stored Query
The Registry Stored Query is classified into the following types:
 - FindDocuments
 - FindSubmissionSets

- FindFolders
- GetAll
- GetDocuments
- GetFolders
- GetAssociations
- GetDocumentsAndAssociations
- GetSubmissionSets
- GetSubmissionSetAndContents
- GetFolderAndContents
- GetFoldersForDocument
- GetRelatedDocuments
- ITI-43 Retrieve Document Set
- ITI-38 Cross Gateway Query
- ITI-39 Cross Gateway Retrieve
- ITI-55 XCPD Patient Discovery
- ITI-56 XCPD Patient Location Query

For details on these Web Services operations and IHE transactions, see http://www.ihe.net/Technical_Frameworks.

Deployment Environment

Core Gateway Services are implemented as Java Enterprise Edition (EE) components.

Hardware Requirement

The following are the minimum hardware requirements for installing XCA:

- 4 GB (4096 MB) of RAM for WebLogic
- 12 GB of disk space
- 16 GB of disk space for 64-bit

Software Requirement

The following are the software requirements for installing XCA:

- Java 1.7 executable in path (for installer)
- Oracle JDK 1.7.0_45+ and WebLogic Server 11g Release 1 (10.3.6.0) or WebLogic Server 12c Release 2 (12.1.2)
- Oracle Database 11g Release 2 (11.2.0.4.0) or Oracle Database 12c Release 1 (12.1.0.2.0)
- Oracle Enterprise Linux 5.5 or higher

Supported IHE Profiles

Table 3 lists the IHE profiles supported by XCA.

Table 3 Supported IHE Profiles

Profile Name	Version	Location
Cross-Community Access	Revision 11.0 Sept 23, 2014	http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf
		http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf
		http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf
		http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf
Cross-Community Patient Discovery (XCPD) Health Data Locator and Revoke Option	Trial Implementation October 13, 2014	http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCPD_HDL_Revoke_Option.pdf

Configuration

The configuration file is located under `config/xca/config` directory of the Application Server domain directory.

WebLogic: `<Weblogic Middleware Home>/user_projects/domains/<domain name>/config/xca/IG.properties`

`<Weblogic Middleware Home>/user_projects/domains/<domain name>/config/xca/RG.properties`

Configuring Initiating Gateway

Providing Local Home Community ID of the Initiating Gateway

Enter the following community IDs for configuring Initiating Gateway:

- `localHomeCommunityId_IG=`
- `localHomeCommunityId_XCPD=`

Configuring the Repository for Initiating Gateway

Prerequisite: Get the repository unique ID and repository URL for retrieving document transactions.

Update the configuration file as follows:

Syntax: `RepositoryUniqueId=RepositoryURL`

For example,

`#1.3.6.1.4.1.21367.13.40.39=https://<hostname>:<port>/hd/services/xdsrepositoryb`

Enabling the Grouping Option with Local Document Consumer

Prerequisite to enable grouping: Get the local community registry URL for Stored Query and Repository URL for retrieving document.

Set the following **INGWGroupedWithDocumentConsumer** property to **yes** to enable the grouping with local document consumer:

- `INGWLocalRegistry` - Takes the value of registry URL.
- `INGWLocalRepository` - Takes the value of repository URL.
- `INGWGroupedWithDocumentConsumer=no`

For example,

- `INGWLocalRegistry=`
- `INGWLocalRepository=`

Configuring Responding Gateway Using Home Community ID

Prerequisite: Responding Gateway Query and retrieve endpoints.

The following is the syntax for configuring the initiating gateway for a specific home community ID. You can configure multiple responding gateways.

Configuration for query transaction:

- Syntax: `CrossGatewayQuery_homecommunityid=RespondingGatewayQueryURL`
- Syntax: `CrossGatewayRetrieve_homecommunityid=RespondingGatewayRetrieveURL`

Configuring Multiple Responding Gateways for Broadcasting Mode

Prerequisite: All the responding gateways query URLs and home community IDs that need to be configured.

You can configure multiple responding gateways for the Cross Gateway Query queries by patient ID.

- `XCARespondingGateway_<count>` - This parameter takes the value of the Responding Gateway query URL.
`<count>` is the variable which ranges from one to the maximum number of Responding gateways that you want to configure.
- `XCARespondingGateway_<count>_HomeCommunityId` - Takes the value of the Home community ID of the responding gateway.

For example, *when <count> value is 1,*

`XCARespondingGateway_1=`

`XCARespondingGateway_1_HomeCommunityId=`

When <count> value is 2,

`XCARespondingGateway_1=`

`XCARespondingGateway_1_HomeCommunityId=`

`XCARespondingGateway_2=`

`XCARespondingGateway_2_HomeCommunityId=`

As mentioned, <count> is the number of responding gateways that you want to configure.

Configuring Local MPI to Initiating Gateway

Prerequisite: Local MPI PDQ Supplier endpoint.

XCA_Local_PDQSupplier takes the value of the PDQ supplier endpoint URL.

For example,

```
XCA_Local_PDQSupplier=
```

ATNA Audit Configuration

Prerequisites: Audit repository host name or IP and audit repository UDP or TLS port.

- ATNAsyslogProtocol - Set this value to UDP or TLS.
- auditMessageType - Represents the audit message type (DICOM XML schema compliant or RFC3881 XML schema compliant) that system generates. Set this value to either RFC3881 or DICOM.

Ensure to configure the following properties when you use TLS for ATNAsyslogProtocol:

- keyStore: Enter the file path of the keystore. For example, /home/common/cert/keystore.jks.
- keyStoreType: Specify the type of the keystore. By default, the value is set to JKS.
- trustStore: Enter the file path of the truststore. For example, /home/common/cert/keystore.jks.
- trustStoreType: Specify the type of the truststore. By default, the value is set to JKS.
- credentialStore: Enter the directory where Oracle wallet is created. For example, /home/common.

To enable auditing, set **Audit** to Yes.

For example, Audit Configuration:

```
auditRepositoryServer=
```

```
auditRepositoryPort=
```

```
ATNAsyslogProtocol=
```

```
auditMessageType=
```

```
keyStore=
```

```
keyStoreType=JKS
```

```
trustStore=
```

```
trustStoreType=JKS
```

```
credentialStore=
```

```
Audit=no
```

Enabling MTOM Option

You can configure this property to enable or disable the MTOM option on the Cross Gateway Document Retrieve Web Service Client Request.

`enableMTOM` - Set this value to true or false.

Configuring Number of Threads and Timeout for Initiating Gateway

You can configure one initiating gateway for multiple responding gateways. Multiple threads ensure better performance.

- `maximumThreadCount` - Takes the value of max number of threads that you want to create.

For example, number of threads required to send the Cross Gateway requests:

`maximumThreadCount=`

Time out configurations for the requests:

- `default_timeout_sync` - Takes the value of the time out for synchronous transactions.
- `default_timeout_async` - Takes the value of the time out for asynchronous transactions.

For example,

- `default_timeout_sync=`
- `default_timeout_async=`

Configuring XCPD Initiating Gateway

Configuring XCPD Responding Gateway

Prerequisite: XCPD URL and Homecommunity ID of the responding gateway.

- `XCPD_RespondingGW_<TargetHomeCommunityID>` - Takes the value of the responding gateway XCPD URL.
`<TargetHomeCommunityID>` must be replaced with the homecommunity ID of the responding gateway.

`XCPD_RespondingGW_TargetHomeCommunityID=XCPD Responding Gateway URL`

For example, `XCPD_RespondingGW_1.0=http://localhost:8080/RespondingGateway_Service/XCPDRespondingGateway`

Configuring Sender and Receiver OIDs

The following properties take sender and receiver OID values appropriately:

- `XCPD_IG_SenderOID=`
- `XCPD_IG_RecieverOID=`

Patient ID Mapping Workflow

The property `PatientID_Mapping_Workflow` takes the following values:

- `xca` - When the value is `xca`, initiating gateway does not send any XCPD request to find patient ID in remote community. IG uses the same patient ID that is sent by the document consumer.
- `xcpd`: When the value is `xcpd`, the initiating gateway sends XCPD request to each configured responding gateway, fetch the patient ID, and uses that patient ID for the respective Cross Gateway Query Transactions.

For example,

```
PatientID_Mapping_Workflow=
```

Configuring Responding Gateway

Configuring Responding Gateway Local Home Community

Enter the following IDs for configuring responding gateway local home community:

- `localHomeCommunityId_RG=`
- `localHomeCommunityId_XCPD=`

Configuring Responding Gateway's Local Registry Repository

Prerequisite: Responding Gateway's local registry, repository URLs with repository unique ID.

- `RespondingGatewayRegistryURL=`
- `RespondingGatewayRepositoryID=`

Prerequisite: Get repository unique and repository URL for retrieving document transactions.

Update the configuration file as follows:

```
Syntax: RepositoryUniqueId=RepositoryURL
```

For example,

```
1.3.6.1.4.1.21367.13.40.39=http://<hostname>:<port>/services/xdsrepository  
b
```

ATNA Audit Configuration

Prerequisites: Audit repository host name or IP and audit repository UDP or TLS port.

- `ATNAsyslogProtocol` - Set this value to UDP or TLS.
- `auditMessageType` - Represents the audit message type (DICOM XML schema compliant or RFC3881 XML schema compliant) that system generates. Set this value to either RFC3881 or DICOM.

Ensure to configure the following properties when you use TLS for `ATNAsyslogProtocol`.

- `KeyStore`: Enter the file path of the keystore. For example, `/home/common/cert/keystore.jks`.
- `KeyStoreType`: Specify the type of the keystore. By default, the value is set to `JKS`.
- `TrustStore`: Enter the file path of the truststore. For example, `/home/common/cert/keystore.jks`.

- **TrustStoreType:** Specify the type of the truststore. By default, the value is set to JKS.
- **CredentialStore:** Enter the directory where Oracle wallet is created. For example, /home/common.

To enable auditing, set **Audit** to Yes.

For example, Audit Configuration:

```
auditRepositoryServer=
auditRepositoryPort=
ATNASyslogProtocol=
auditMessageType=
keyStore=
keyStoreType=JKS
trustStore=
trustStoreType=JKS
credentialStore=
Audit=no
```

Configuring Local MPI to Responding Gateway

Prerequisite: Local MPI PDQ Supplier endpoint.

- XCPD_RG_PDQSupplier<count> - Takes the value of the PDQ endpoint of the MPI.
- XCPD_RG_PDQSupplier<count>_domainID - Takes the value of the domain ID.

For example, IHERED, IHEBLUE, and so on.

XCPD Responding Gateway settings:

You can have multiple PDQ suppliers to talk with.

- XCPD_RG_PDQSupplier<count>=
- XCPD_RG_PDQSupplier<count>_domainID=

<count> can be replaced with any number of PDQ suppliers that are planned to configure. Responding gateway can look through multiple MPI systems to search for a patient.

For example, when <count> is 1,

```
XCPD_RG_PDQSupplier1=
XCPD_RG_PDQSupplier1_domainID=
```

When <count> is 2,

```
XCPD_RG_PDQSupplier1=
XCPD_RG_PDQSupplier1_domainID=
XCPD_RG_PDQSupplier2=
XCPD_RG_PDQSupplier2_domainID=
```

Configuring Health Data Locator

To enable Health Data Locator, set the value of `SupportsHealthDataLocator` property in the `RG.properties` file to `yes`.

If the value is set to `yes`, RG responds to the XCPD request indicating that it supports patient location query.

If the value is set to `no`, RG does not support Health Data Locator.

Transactions and Web Service Uniform Resource Locator

Table 4 lists the Web Services supported by XCA. You can find the Web Service WSDL by suffixing endpoint Uniform Resource Locator (URL) with `?wsdl`.

Table 4 Transactions and Web Service URL

Transaction	Synch	Asynch	Endpoint URL
Cross Patient Discovery (ITI-55)	Yes	Yes	<code>http(s)://<XCA_HOST>:<PORT>/RespondingGateway_Service/XCPDRespondingGateway</code>
Registry Stored Query (ITI-18)	Yes	No	<code>http(s)://<XCA_HOST>:<PORT>/InitiatingGatewayQuery_Service/XCAInitiatingGatewayQuery</code>
Retrieve Document Set (ITI-43)	Yes	No	<code>http(s)://<XCA_HOST>:<PORT>/InitiatingGatewayRetrieve_Service/XCAInitiatingGatewayRetrieve</code>
Cross Document Query (ITI-38)	Yes	Yes	<code>http(s)://<XCA_HOST>:<PORT>/RespondingGatewayQuery_Service/XCARespondingGatewayQuery</code>
Cross Document Retrieve (ITI-39)	Yes	Yes	<code>http(s)://<XCA_HOST>:<PORT>/RespondingGatewayRetrieve_Service/XCARespondingGatewayRetrieve</code>
Patient Location Query (ITI-56)	Yes	Yes	<code>http(s)://<XCA_HOST>:<PORT>/RespondingGateway_Service/XCPDRespondingGateway</code>
Asynchronous Registry Stored Query	No	Yes	<code>http(s)://<XCA_HOST>:<PORT>/IGAsyncServices/XCAInitiatingGatewayQuery</code>
Asynchronous Retrieve Document Set	No	Yes	<code>http(s)://<XCA_HOST>:<PORT>/IGAsyncServices/XCAInitiatingGatewayRetrieve</code>

Oracle Extensions

As per the IHE specification, XCA and XCPD are two different profiles. The Oracle implementation is merged together. The Initiating Gateway first sends the XCPD request, finds out the patient identifiers in the remote community, and then uses this patient identifier for the next cross gateway query call to the responding gateway.

Security Configuration Issues

This section describes security configuration issues you must consider when implementing XCA.

General Security Principles

The following are fundamental principles for using any application securely:

Keep software up-to-date

Keep all software versions and patches up-to-date.

Keep up-to-date on latest security information critical patch

Oracle continually improves its software and documentation. Critical patch updates are the primary means of releasing security fixes for Oracle products to customers with valid support contracts. Oracle recommends you to apply these patches as soon as they are released.

Configure strong passwords on the database

Repeat the following basic rule of security management.

Ensure all passwords are strong. You can strengthen passwords by creating and using password policies for your organization. For guidelines on securing passwords and for additional ways to protect passwords, refer to the *Oracle® Database Security Guide* specific to the database release you are using.

You should modify the following passwords to use your policy-compliant strings:

- Passwords for the database default accounts, such as SYS and SYSTEM.
- Passwords for the database application-specific schema accounts, such as Gateway.
- Password for the database listener.

Oracle recommends that you do not configure a password for the database listener as it will enable remote administration. For more information, refer to the section *Removing the Listener Password* of *Oracle® Database Net Services Reference 11g Release 2 (11.2)*.

Follow the principle of least privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Overly ambitious granting of responsibilities, roles, grants - especially early on in an organization's life cycle when people are few and work needs to be done quickly - often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

To restrict access, it is recommended to have the following default file permissions in Unix environment.

- 740 for executable
- 640 for regular files

Managing default user accounts

Lock and expire default user accounts.

Closing all open ports when not in use

Keep only the minimum number of ports open. You should close all ports when not in use.

Disabling the Telnet service

Oracle XCA standard configuration does not use the Telnet service. By default, Telnet listens on port 23. Telnet, which sends clear-text passwords and user names through a log in, is a security risk to your servers. If the Telnet service is available on any system, it is recommended to disable Telnet in favor of Secure Shell (SSH). Disabling Telnet protects your system security.

Disabling Other Unused Services

In addition to not using Telnet, the Oracle XCA Gateway standard configuration does not use the following services or information for any functionality:

- Simple Mail Transfer Protocol (SMTP) - This protocol is an Internet standard for e-mail transmission across Internet Protocol (IP) networks.
- Identification Protocol (identd) - This protocol is generally used to identify the owner of a TCP connection on UNIX.
- Simple Network Management Protocol (SNMP) - This protocol is a method for managing and reporting information about different systems.

Restricting these services or information does not affect the use of Oracle XCA standard configuration. If you are not using these services for other applications, it is recommended to disable these services to minimize your security exposure. If you need SMTP, identd, or SNMP for other applications, ensure to upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

Designing multiple layers of protection

When designing a secure deployment, design multiple layers of protection. If a hacker gains access to one layer, such as Application server, that should not automatically give them easy access to other layers, such as the database server.

Providing multiple layers of protection may include:

- Enabling only those ports required for communication between different tiers. For example, only allow communication to the database tier on the port used for SQL*NET communications (by default, 1521).
- Placing firewalls between servers so that only expected traffic can move between servers.

Utilizing SSL

Consider utilizing Application Server SSL service for the XCA application. The XCA application is a standard Java EE application and can utilize an industry standard security infrastructure and framework. There is no configuration required on the XCA application. The application Server (WebLogic) provides SSL service. For more information about configuring SSL to achieve SSL security for XCA, see the Application Server's documentation.

When SSL or TLS is configured, it is recommended to use TLS_RSA_WITH_AES_128_CBC_SHA cipher instead of SSL_RSA_WITH_3DES_EDE_CBC_SHA for TLS authentication.

Related Documents

Refer to the following links for standard definitions of:

- Integrating the Healthcare Enterprise (IHE) Actors: <http://wiki.ihe.net/index.php?title=Actors>
- IHE Profiles and Standards: <http://www.ihe.net/profiles/index.cfm>

- IT Infrastructure Domain: http://wiki.ihe.net/index.php?title=IT_Infrastructure
- Cross-Enterprise Document Sharing (XDS): http://wiki.ihe.net/index.php?title=Cross-Enterprise_Document_Sharing
- Cross-Community Access (XCA): http://wiki.ihe.net/index.php?title=Cross-Community_Access

Appendix A: Acronyms

This section provides a list of commonly used acronyms.

- IG - Initiating Gateway
- IHE - Integrating the Healthcare Enterprise
- RG - Responding Gateway
- XCA - Cross-Community Access
- XCPD - Cross-Community Patient Discovery
- XDS - Cross-Enterprise Document Sharing

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® Health Sciences Information Manager Cross Community Access User's Guide, Release 3.0
E61377-01

Copyright © 2012, 2015, 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 about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

