Oracle® Communications Unified Inventory Management

Installation Guide

Release 7.6
F95171-02
January 2025

Oracle Communications Unified Inventory Management Installation Guide, Release 7.6

F95171-02

Copyright © 2012, 2025, Oracle and/or its affiliates.

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, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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.

Contents

Preface

Audience x
Documentation Accessibility x
Diversity and Inclusion x

1 Unified Inventory Management Installation Overview

Overview of the UIM Installation Procedure 1-1
Installation Options 1-1
    Interactive Install and Silent Install 1-1
Ensuring a Successful UIM Installation 1-2
Directory Placeholders Used in This Guide 1-2
Unified Inventory and Topology 1-2

2 Unified Inventory Management System Requirements

Software Requirements 2-1
Hardware Sizing Guidelines 2-1
Unified Topology for Inventory and Automation Hardware Sizing Guidelines 2-2
Information Requirements 2-6

3 Installing and Configuring the Oracle Database

Installing Oracle Database 3-1
    About Spatial, Graph, and Locator in Database 3-1
Configuring Oracle Database 3-2
    Database Connection Information 3-2
    Setting the Database Parameters 3-2
    Setting the Database Time Zone 3-3
    Creating and Configuring Your Tablespaces 3-3
    Creating the Database (MetaData) Schema for UIM 3-4
        Schema User Name Information 3-4
    Installing and Configuring Oracle Database Real Application Clusters 3-7
        Database Connection Information for Real Application Clusters Database 3-7

Tuning the Database 3-7
Enabling and Configuring Server Affinity 3-8

4 Installing and Configuring Oracle WebLogic Server

About Java Requirements 4-1
Installing IBM Java 4-1
Installing the Oracle JDK 4-1
Downloading and Installing Oracle WebLogic Server 4-1
Installing Patches 4-2
Installing Oracle Application Development Runtime 4-2
Installing Optional Software Supported by UIM 4-3
Creating a WebLogic Domain for a Single Server Installation 4-3
WebLogic Server Connection Information 4-3
Creating a Standalone WebLogic Domain 4-4
Starting the WebLogic Server 4-7
Setting Memory Requirements for UIM 4-8
Setting Memory Requirements for UIM in UNIX Environments 4-8
Setting Memory Requirements for UIM in AIX Environments 4-9
Setting Memory Requirements for UIM in Solaris Environments 4-9
Creating a WebLogic Domain for a Server Cluster Installation with a Shared Disk Storage 4-9
Installation Scenario 4-9
Server Cluster Example 4-10
Server Cluster Prerequisites 4-11
Overview of Steps for Setting Up a Server Cluster 4-12
Installing Oracle WebLogic Server in a Clustered Environment 4-12
Creating a Domain 4-12
Starting the WebLogic Server 4-19
Starting the Cluster Servers 4-19
Configuring the WebLogic Server StuckThreadMaxTime Value 4-20
Configuring the WebLogic Server Proxy Timeout Value 4-21
Creating a WebLogic Domain for a Server Cluster Installation without a Shared Disk Storage 4-21
About Setting Up UIM in a Server Cluster 4-21
Installation Scenario 4-22
Server Cluster Example 4-22
Server Cluster Prerequisites 4-22
Setting Up a Server Cluster without a Shared Storage 4-23
Installing Oracle WebLogic and UIM on an Administration Server Machine 4-23
Creating a WebLogic Domain for a Dynamic Server Cluster Installation 4-23
Installation Scenario 4-24
Server Cluster Example 4-24
Server Cluster Prerequisites 4-25

Setting Up a Dynamic Server Cluster 4-25
Configuring the WebLogic Server to Not Use KSS Demo Identity and Trust Keystores 4-25
Enabling WebLogic SSL Port 4-26
Installing and Configuring Additional Software 4-26
Installing and Configuring an Authentication Provider 4-26
Configuring WebLogic Server for the Authentication Provider 4-27
Configuring Custom Authentication Providers 4-28

5 Installing Unified Inventory Management

About the UIM Installer 5-1
Installing UIM by Using Interactive Install 5-1
Installing UIM by Using Silent Install 5-9
About the Response File 5-9
Populating the Response File 5-10
Starting Silent Install 5-10

6 Unified Inventory Management Post-Installation Tasks

Configuring a Trusted Certificate for UIM 6-1
Deploying UIM Cartridges 6-1
Connecting the UIM Web Service Interface to a Remote Application 6-2
Routing Traffic Between Proxy and Cluster 6-3
Configuring Mail Sessions 6-4
Defining the Map Data Source 6-4

7 Verifying the Unified Inventory Management Installation

Checking the Installation Logs 7-1
Checking the State of Installed Components 7-1
Logging In to Unified Inventory Management 7-2

8 Troubleshooting the Unified Inventory Management Installation

Reporting Problems 8-1
Problem: RCU Creation Fails Due to Invalid Common User or Role Name 8-1
Problem: Database Server and Application Server Have Different Dates 8-2
Problem: Unable to Create the UIM Administrator User Except During Installation 8-2
Problem: Unable to Run SQL Script 8-3
Problem: Timers are Not Started 8-5
Problem: Deploying Enterprise Manager Error on Managed Servers 8-5
Problem: Errors Observed in Managed Server Logs When Redeploying Cartridges During UIM Upgrade 8-6

Problem: Errors Observed After Domain Upgrade 8-6
Problem: Errors Observed During UIM Installation 8-7
Problem: Error Occurred While Expanding oracle.communications.inventory in the Console 8-7

9 Upgrading Unified Inventory Management

About Upgrading UIM 9-1
Supported Upgrade Paths 9-1
Planning Your Upgrade 9-1
Testing the Upgrade in a Test Environment 9-2
Upgrade Impacts 9-2
Database Software Changes 9-3
Database Schema Changes 9-3
Fusion Middleware Changes 9-3
Java Development Kit Changes 9-3
Application Component Changes 9-3
API Changes 9-3
Design Studio Changes 9-4
Cartridge Changes 9-4
Upgrading UIM 9-4
Pre-Upgrade Tasks for Release 7.3.x 9-4
Pre-Upgrade Tasks from Release 7.4.0 to Release 7.5.1 9-12
Pre-Upgrade Tasks from Release 7.4.1, 7.4.2, or 7.5.0 to Release 7.5.1 9-16
POMS Cache Coordination MDB 9-19
Upgrading UIM 9-19
Post-Upgrade Tasks 9-23
About Rolling Back UIM 9-25

10 Setting Up Unified Inventory Management for Single Sign-On Authentication

Installing Required Software 10-1
Configuring UIM to Enable SSO Authentication 10-3
Prerequisites 10-3
Installing and Deploying UIM Specifying the External LDAP Provider 10-3
Configuring the Frontend URL in Administration Console 10-3
Creating and Configuring Providers for OAM SSO 10-4
Configuring web.xml for the OAM Identity Asserter 10-5
Configuring the mod_wl_ohs Plug-In for Oracle HTTP Server 10-7
Configuring the WebLogic Proxy Plug-In 10-7
Editing the mod_wl_ohs.conf File 10-7
Protecting Resources For SSO Authentication 10-9

Excluding Resources From SSO Authentication 10-10
Configuring SSO using SAML 2.0 Protocol from IDCS Identity Provider 10-11
Configuring SAML for SSO 10-11
Creating SAML Assertion Provider and SAML Authenticator 10-11
Specifying General Information 10-12
Configuring the SAML Service Provider 10-12
Publishing the Service Provider Metadata 10-13
Registering Identity Provider in WebLogic 10-13
Updating the Deployment Plan of Unified Inventory Management 10-14
Verifying SAML Configuration 10-15
Registering UIM in IDCS Identity Provider 10-16
Manually Configuring UIM Details in IDCS Identity Provider 10-16
Creating SAML2.0 Client in Identity Provider by Importing UIM Metadata (xml) 10-17
Configuring WebLogic for Using Identity Provider for Authorization 10-18
Updating the SSL.hostnameVerifier Property 10-18
Configuring Oracle Identity Cloud Integrator Provider 10-18
Setting Up Trust between IDCS and WebLogic 10-21
Creating an Administrator User in IDCS Administration Console for WebLogic 10-21
Managing Group Memberships, Roles, and Accounts 10-22

11 Installing UIM Patches

About Patching UIM 11-1
Planning Your Patch Installation 11-2
Installing a Patch 11-2

12 Configuring Oracle Maps

Choosing a Map Option 12-1
Pointing to the Oracle Map Service (Default) 12-1
Using Existing Map Data 12-1
Using a Sample Map 12-1
Configuring MapViewer 12-2
Defining the Map Data Source 12-2
Copying the JNDI URL of Map Data Source 12-3
Defining Base Maps 12-3
Modifying the Map Profile Defaults 12-4
Linking UIM Map Profile to MapViewer 12-5
Enabling Map View 12-6
Installing Map Builder 12-6
Viewing MapViewer Documentation 12-6

13 Uninstalling Unified Inventory Management

About Uninstalling UIM 13-1
Uninstalling UIM or UIM Components 13-1

14 Enabling Geographic Redundancy and Disaster Recovery

About Geographic Redundancy and Disaster Recovery in UIM 14-1
- About Switchover and Failover 14-3
- Geographically Redundant Traditional UIM Deployment 14-3
- Geographically Redundant UIM Cloud Native Deployment 14-5

Prerequisites for Geographic Redundancy 14-7
- Synchronize File Systems 14-7
- Synchronize UIM Domain 14-8
- Oracle Data Guard 14-8
- Network Configuration 14-9
  - Network Bandwidth Estimation 14-10
- Host Configuration 14-11

UIM Geo-Redundancy Lab Architecture 14-12
- UIM Application Architecture 14-13
- Installation and Configuration 14-13
- Installing Oracle Data Guard 14-14
- UIM GR Lab Data Guard Configuration 14-14

Switchover and Failover Test Procedures 14-15
- Switchover Procedure (Graceful Shutdown) 14-15
- Failover Procedure 14-16
- Test Cases 14-16

A Configuring KeyCloak as Identity Provider for UIM, UTIA, and Message Bus

Prerequisites for Configuring KeyCloak A-1
Creating a New Realm A-1
Downloading the Identity Provider Metadata File A-1
Creating a UIM Cloud Native Instance A-1
Creating a SAML Client for UIM A-2
- Creating a SAML Client Role A-2
- Adding Role Mapper in SAML Client Scope A-2

Adding Users and Mapping the Users to the SAML Client Role A-2
Creating OAUTH Client for UTIA and Message Bus A-3
Configuring the Client Scope and Audience A-3
Adding Scope to the Client A-4

Getting OpenID Endpoint Configurations A-4
Configuring Message Bus and UTIA with OAUTH Client A-4
Integrating UIM with UTIA and Message bus A-5

Preface

This guide provides instructions for installing Oracle Communications Unified Inventory Management (UIM).

Audience

This document is for system administrators, database administrators, and developers who install and configure UIM. The person installing the software should be familiar with the following topics:

- Operating system commands
- Database configuration
- Oracle WebLogic Server
- Network management

Before reading this guide, you should have familiarity with UIM. See *UIM Concepts*.

UIM requires Oracle Database and Oracle WebLogic Server. See the documentation for these products for installation and configuration instructions.

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 that have purchased support 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.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1

Unified Inventory Management Installation Overview

This chapter provides an overview of the installation process of Oracle Communications Unified Inventory Management (UIM).

Overview of the UIM Installation Procedure

Installing UIM involves a number of steps that you or others must complete:

1. Review system requirements. See "Unified Inventory Management System Requirements".
2. Install Oracle Database and configure it for UIM. See "Installing and Configuring the Oracle Database".
3. Install Oracle WebLogic Server and configure it for UIM. See "Installing and Configuring Oracle WebLogic Server ".
4. Install UIM. See "Installing Unified Inventory Management".
5. Perform post-installation configuration tasks. See "Unified Inventory Management Post-Installation Tasks".
6. Verify the installation. See "Verifying the Unified Inventory Management Installation".
7. Upgrade UIM. See "Upgrading Unified Inventory Management".
8. (Optional) Troubleshooting UIM. See "Troubleshooting the Unified Inventory Management Installation".
9. Install UIM patches. See "Installing UIM Patches ".
10. (Optional) Configure Oracle Maps. See "Configuring Oracle Maps".
11. (Optional) Configure Unified Inventory and Topology microservices. See "Unified Inventory and Topology"
12. (Optional) Uninstall UIM. See "Uninstalling Unified Inventory Management ".

Installation Options

There are many options you can choose during installation. This section describes the options that have the largest impact on the installation process.

Interactive Install and Silent Install

"Installing Unified Inventory Management" describes the following ways you can install UIM:

- **Interactive install**: A typical installation or custom interactive installation where you interact with the Oracle Universal Installer UI.
- **Silent install**: A script-based installation.

Both installations provide the same options. Oracle recommends that you use interactive install for your first installation.

Ensuring a Successful UIM Installation

UIM installation should be performed only by qualified personnel. You must be familiar with the following before you begin the installation:

- UNIX operating system
- Oracle WebLogic Server administration
- Oracle Database administration

Additionally, you should have experience installing Java-related packages.

Follow these guidelines:

- Pay close attention to the system requirements. Before you begin installing the application, ensure your system has the required base software. In addition, ensure that you know all of the required configuration values, such as host names and port numbers.
- Make a note of any new configuration values as you create them. You will be required to enter configuration values later in the procedure.
- As you install each component, verify that it installed successfully before continuing the installation process.
- Monitor the installation log files, to verify the installation events. See "Checking the Installation Logs" for information on the installation log files.

Directory Placeholders Used in This Guide

Table 1-1 lists the placeholders that are used in this guide to refer to directories related to the UIM application.

Table 1-1 Directory Placeholders

Placeholder	Directory Description
UIM_Home	The directory in which the UIM software is installed. This directory contains various installation-related files.
MW_Home	The directory in which the Oracle Fusion Middleware products are installed. This directory contains the base directory for the WebLogic Server, a utilities directory, and other files and directories.
WL_Home	The directory in which the WebLogic Server is installed. It is located in the *MW_Home* directory.
Domain_Home	The directory containing the configuration for the domain into which UIM is installed. The default location is *MW_Home***/user_projects/domains/***domain_name*, where *domain_name* is the name of the WebLogic server domain for UIM.

Unified Inventory and Topology

UIM 7.5.1 supports the following microservices that are collectively called as Unified Inventory and Topology:

- Unified Topology for Inventory and Automation (UTIA)
- Oracle Communications Unified Operations Message Bus
- Common Authentication

You can configure these microservices to avail the corresponding services offered.

See *Unified Inventory and Topology Deployment Guide*, for deploying and configuring the microservices.

2

Unified Inventory Management System Requirements

This chapter describes the hardware, operating system, software, server, and database requirements for installing Oracle Communications Unified Inventory Management (UIM).

Software Requirements

For details about the software required to support the UIM components for traditional deployment, see "UIM Traditional Deployment Software Compatibility" in *UIM Compatibility Matrix*.

Hardware Sizing Guidelines

Table 2-1 provides hardware sizing guidelines for UIM.

> **Note:**
>
> - The information in this section is meant as a guideline only. The values in this section are approximate. Accurate sizing for a production system requires a detailed analysis of the proposed business requirements. Sizing guidelines are based on an average CPU utilization rate of 60% - 70%. The guidelines do not account for High Availability and Disaster Recovery environments.
> - For information on hardware sizing requirements for HP-UX Itanium, contact Oracle Support.
> - The UIM installer supports Internet Protocol version 6 (IPv6) addresses. You can install and deploy UIM on servers that support IPv6 addresses.

Table 2-1 Hardware Sizing Guidelines

Deployment Size	Small	Medium	Large	Extra-Large
Services/day	<= 300,000	<= 600,000	<= 1,500,000	<= 3,000,000
Services/hour	<= 33,500	<= 66,500	<= 166,500	<= 333,000
# of Subscribers Base (in Millions)	10	20	50	100
x86-64/Linux Platform - Application Server	CPU: 1 x 4 core - 2.55 GHz AMD EPYC™ 77J3- 8 threads RAM: 1 x 60 GB HDD: 1 X 300 GB	CPU: 2 x 4 core - 2.55 GHz AMD EPYC™ 77J3 - 16 threads RAM: 2 x 60 GB HDD: 2 X 300 GB	CPU: 8 x 4 core - 2.55 GHz AMD EPYC™ 77J3-64 threads RAM: 8 x 60 GB HDD: 8 X 300 GB	CPU: 14 x 4 core - 2.55 GHz AMD EPYC™ 77J3-112 threads RAM: 14 x 60 GB HDD: 14 X 300 GB

Table 2-1 (Cont.) Hardware Sizing Guidelines

Deployment Size	Small	Medium	Large	Extra-Large
Oracle Cloud Infrastructure Equivalent for Application Server	1 x VM.Standard.E4. Flex (4 OCPUs)	2 x VM.Standard.E4.Flex (8 OCPUs)	8 x VM.Standard.E4.Flex (32 OCPUs)	14 x VM.Standard.E4.Flex (56 OCPUs)
x86-64/Linux Platform - Database Server	CPU: 1 x 8 core - 2.55 GHz AMD EPYC™ 77J3- 16 threads RAM: 1 x 120 GB Initial storage: 400 GB Storage growth (annual): 1.2 TB	CPU: 2 x 16 core - 2.55 GHz AMD EPYC™ 77J3- 64 threads RAM: 2 x 240 GB Initial storage: 2 TB Storage growth (annual): 4 TB	CPU: 21 x 24 core - 2.55 GHz AMD EPYC™ 77J3- 96 threads RAM: 2 x 320 GB Initial storage: 4 TB Storage growth (annual): 6 TB	CPU: 2 x 24 core - 2.55 GHz AMD EPYC™ 77J3- 96 threads RAM: 2 x 320 GB Initial storage: 6 TB Storage growth (annual): 12 TB
Oracle Cloud Infrastructure Equivalent for Database Server	1 x VM.Standard.E4.Flex (8 OCPUs)	2 x VM.Standard.E4.Flex (32 OCPUs)	2 x VM.Standard.E4.Flex (48 OCPUs)	2 x VM.Standard.E4.Flex (48 OCPUs)

Note:

Based on the 5G Mobile cartridge pack, one service invokes five Web service operations against UIM. Each service is composed of 1 CFS and 2 RFS.

DB Storage is listed without retention calculations. Storage requirements will increase with number of subscriber population and retention period requirements.

UIM 7.5 and later cloud native deployments require an additional 5% compute resources for Kubernetes and container management.

UIM 7.5 and later versions have native application monitoring capabilities which require a minimum 2 GB additional allocation in the heap if the monitoring feature is enabled.

Unified Topology for Inventory and Automation Hardware Sizing Guidelines

Unified Topology for Inventory and Automation (UTIA) is made up of several components that run in Kubernetes environment. The sizing for each of these components is listed in the following tables and the total value represents the hardware footprint that is required to run Kubernetes and the UTIA components. The sizing is divided between application components and database components.

> **Note:**
>
> The information in this section is meant as a guideline only. The values in this section are approximate. Accurate sizing for a production system requires a detailed analysis of the proposed business requirements. The guidelines do not account for High Availability, Disaster Recovery environments, or lower testing and development environments. The database storage is listed without retention calculations.

The following tables provide hardware sizing guidelines for UTIA.

Table 2-2 Hardware Sizing Guidelines for Application Components

Deployment Size	Small	Medium	Large
UTIA Data Characteristics			
Vertices and Edges	10 Million	25 Million	50 Million
No. of Network Nodes	0.5 Million	1 Million	2.5 Million
No. of Equipments	0.5 Million	2 Million	7.5 Million
No. of Locations and Network Entity Codes	0.5 Million	1 Million	2.5 Million
No. of Connectivities	1 Million	2 Million	4 Million
UTIA Service			
UTIA API	No. of pods: 2 Compute per pod (OCPUs): 1 RAM per pod (GB): 3 Total Compute (OCPUs): 2 Total RAM (GB): 6	No. of pods: 3 Compute per pod (OCPUs): 1 RAM per pod (GB): 3 Total Compute (OCPUs): 3 Total RAM (GB): 9	No. of pods: 3 Compute per pod (OCPUs): 1 RAM per pod (GB): 3 Total Compute (OCPUs): 3 Total RAM (GB): 9
UTIA UI	No. of pods: 1 Compute per pod (OCPUs): 4 RAM per pod (GB): 6 Total Compute (OCPUs): 4 Total RAM (GB): 6	No. of pods: 1 Compute per pod (OCPUs): 4 RAM per pod (GB): 6 Total Compute (OCPUs): 4 Total RAM (GB): 6	No. of pods: 1 Compute per pod (OCPUs): 6 RAM per pod (GB): 9 Total Compute (OCPUs): 6 Total RAM (GB): 9
Sub-total	Compute (OCPUs): 6 RAM (GB): 12	Compute (OCPUs): 7 RAM (GB): 15	Compute (OCPUs): 9 RAM (GB): 18
Unified Operations Message Bus			

Table 2-2 (Cont.) Hardware Sizing Guidelines for Application Components

Deployment Size	Small	Medium	Large
Kafka Broker	No. of pods: 2 Compute per pod (OCPUs): 0.5 RAM per pod (GB): 2 Total Compute (OCPUs): 1 Total RAM (GB): 4	No. of pods: 3 Compute per pod (OCPUs): 0.5 RAM per pod (GB): 2 Total Compute (OCPUs): 1.5 Total RAM (GB): 6	No. of pods: 3 Compute per pod (OCPUs): 0.5 RAM per pod (GB): 2 Total Compute (OCPUs): 1.5 Total RAM (GB): 6
Kafka Consumer	No. of pods: 2 Compute per pod (OCPUs): 0.25 RAM per pod (GB): 1 Total Compute (OCPUs): 0.5 Total RAM (GB): 2 **Note**: The capacity of this system allows a seamless processing of upto 20 TPS	No. of pods: 3 Compute per pod (OCPUs): 0.25 RAM per pod (GB): 1 Total Compute (OCPUs): 0.75 Total RAM (GB): 3 **Note**: The capacity of this system allows a seamless processing of upto 30 TPS	No. of pods: 5 Compute per pod (OCPUs): 0.25 RAM per pod (GB): 1 Total Compute (OCPUs): 1.25 Total RAM (GB): 5 **Note**: The capacity of this system allows a seamless processing of upto 50 TPS
Kafka Zookeeper	No. of pods: 1 Compute per pod (OCPUs): 0.5 RAM per pod (GB): 1 Total Compute (OCPUs): 0.5 Total RAM (GB): 1	No. of pods: 1 Compute per pod (OCPUs): 0.5 RAM per pod (GB): 1 Total Compute (OCPUs): 0.5 Total RAM (GB): 1	No. of pods: 1 Compute per pod (OCPUs): 0.5 RAM per pod (GB): 1 Total Compute (OCPUs): 0.5 Total RAM (GB): 1
Sub-total	Compute (OCPUs): 2.0 RAM (GB): 7	Compute (OCPUs): 2.75 RAM (GB): 10	Compute (OCPUs): 3.25 RAM (GB): 12
In-memory Database			
PGX	No. of pods: 2 Compute per pod (OCPUs): 2 RAM per pod (GB): 10	No. of pods: 2 Compute per pod (OCPUs): 2 RAM per pod (GB): 15	No. of pods: 2 Compute per pod (OCPUs): 2 RAM per pod (GB): 25
Sub-total	Compute (OCPUs): 4 RAM (GB): 20	Compute (OCPUs): 4 RAM (GB): 30	Compute (OCPUs): 4 RAM (GB): 50
Common Authentication			

Table 2-2 (Cont.) Hardware Sizing Guidelines for Application Components

Deployment Size	Small	Medium	Large
OAM	No. of pods: 1 Compute per pod (OCPUs): 0.5 RAM per pod (GB): 8 Total Compute (OCPUs): 0.5 Total RAM (GB): 8	No. of pods: 1 Compute per pod (OCPUs): 1 RAM per pod (GB): 8 Total Compute (OCPUs): 1 Total RAM (GB): 8	No. of pods: 1 Compute per pod (OCPUs): 1 RAM per pod (GB): 8 Total Compute (OCPUs): 1 Total RAM (GB): 8
OHS	No. of pods: 1 Compute per pod (OCPUs): 0.5 RAM per pod (GB): 4 Total Compute (OCPUs): 0.5 Total RAM (GB): 4	No. of pods: 1 Compute per pod (OCPUs): 0.5 RAM per pod (GB): 4 Total Compute (OCPUs): 1 Total RAM (GB): 4	No. of pods: 1 Compute per pod (OCPUs): 0.5 RAM per pod (GB): 4 Total Compute (OCPUs): 1 Total RAM (GB): 4
Sub-total	Compute (OCPUs): 1 RAM (GB): 12	Compute (OCPUs): 2 RAM (GB): 12	Compute (OCPUs): 2 RAM (GB): 12
Total Application Components			
AMD EPYC™ 77J3	Compute OCPUs: 13.5 RAM (GB): 53	Compute OCPUs: 16 RAM (GB): 66	Compute OCPUs: 18.5 RAM (GB): 90
Oracle Cloud Infrastructure equivalent	Shape VM.Standard.E4.Flex (14 OCPU)	Shape VM.Standard.E4.Flex (16 OCPU)	Shape VM.Standard.E4.Flex (19 OCPU)

The following table provides the hardware sizing guidelines for the database components:

Table 2-3 Hardware Sizing Guidelines for Database Components

Deployment Size		Medium	Large
UTIA Data Characteristics			
Vertices and Edges	10 Million	25 Million	50 Million
No. of Network Nodes	0.5 Million	1 Million	2.5 Million
No. of Equipments	0.5 Million	2 Million	7.5 Million
No. of Locations and Network Entity Codes	0.5 Million	1 Million	2.5 Million
No. of Connectivities	1 Million	2 Million	4 Million
Database Components			

Table 2-3 (Cont.) Hardware Sizing Guidelines for Database Components

Deployment Size		Medium	Large
UTIA Database	No. of RAC nodes: 2 Compute per node (OCPUs): 4 RAM per node (GB): 60 Total Compute (OCPUs): 8 Total RAM (GB): 120 Total Storage (TB): 0.3	No. of RAC nodes: 2 Compute per node (OCPUs): 8 RAM per node (GB): 120 Total Compute (OCPUs): 16 Total RAM (GB): 240 Total Storage (TB): 0.5	No. of RAC nodes: 2 Compute per node (OCPUs): 12 RAM per node (GB): 160 Total Compute (OCPUs): 24 Total RAM (GB): 320 Total Storage (TB): 1
OAM	No. of RAC nodes: 1 Compute per node (OCPUs): 2 RAM per node (GB): 30 Total Compute (OCPUs): 2 Total RAM (GB): 30 Total Storage (TB): 0.1	No. of RAC nodes: 1 Compute per node (OCPUs): 2 RAM per node (GB): 30 Total Compute (OCPUs): 2 Total RAM (GB): 30 Total Storage (TB): 0.1	No. of RAC nodes: 1 Compute per node (OCPUs): 4 RAM per node (GB): 60 Total Compute (OCPUs): 4 Total RAM (GB): 60 Total Storage (TB): 0.2
Total Database Components			
AMD EPYC™ 77J3	Compute OCPUs: 10 RAM (GB): 150 Storage (TB): 0.4	Compute OCPUs: 18 RAM (GB): 270 Storage (TB): 0.6	Compute OCPUs: 28 RAM (GB): 380 Storage (TB): 1.2
Oracle Cloud Infrastructure equivalent	2 x Shape VM.Standard.E4.Flex 1 x Shape VM.Standard.E4.Flex (2 OCPU)	2 x Shape VM.Standard.E4.Flex (8 OCPU) 1 x Shape VM.Standard.E4.Flex (2 OCPU)	2 x Shape VM.Standard.E4.Flex (12 OCPU) 1 x Shape VM.Standard.E4.Flex (4 OCPU)

Information Requirements

During UIM installation, you are required to enter configuration values such as host names and port numbers. You define some of these configuration values when you install and configure the Oracle database and WebLogic Server.

If you have already installed Oracle Communications products, the installer reads the values from the existing Oracle Communications products and uses them as default values. If no

Oracle Communications products are installed, the installer uses the default values shown in the following tables.

Each chapter contains tables for the configuration values.

3

Installing and Configuring the Oracle Database

This chapter describes the process of installing the Oracle Database and configuring the Oracle database for Oracle Communications Unified Inventory Management (UIM).

Installing Oracle Database

The Oracle Universal Installer checks for a database to connect to during the installation process. Ensure that a database is running before you start installing UIM. If you already have a database running, you must create a tablespace for UIM.

Download and install Oracle Database for this version of UIM. See *UIM Compatibility Matrix* for the appropriate version of Oracle Database to install.

For information on installing Oracle Database, see the Oracle Database installation documentation.

> **Note:**
>
> UIM uses Oracle Locator, which must be installed prior to the UIM installation. When you install Oracle Database, Oracle MultiMedia is installed; and when Oracle MultiMedia is installed, Oracle Locator is installed.
>
> You can also install Oracle MultiMedia manually if necessary. For more information, see *Oracle MultiMedia User's Guide* at:
>
> http://docs.oracle.com/database/122/IMURG/toc.htm

About Spatial, Graph, and Locator in Database

By default, the Spatial and Graph are installed with the Enterprise edition database. UIM uses only the Oracle Locator that comes with the database and it does not use the Spatial and Graph. You can remove the installed Spatial and Graph from the database.

To remove the Spatial and Graph from the database:

1. Ensure that the Oracle Multimedia is installed.
2. Connect to the database as the **SYS** user with **SYSDBA** privileges.

   Enter the **SYS** as **SYSDBA** and enter the SYS account password when prompted.
3. Start the **SQL*Plus**.
4. Enter the following statements:

   Linux:

   ```
   @$ORACLE_HOME/md/admin/mddins.sql
   ```

   Windows:

```
@%ORACLE_HOME%\md\admin\mddins.sql
```

Configuring Oracle Database

The Oracle database must be configured for UIM. Specifically, this section covers the following:

- Database Connection Information
- Setting the Database Parameters
- Setting the Database Time Zone
- Creating and Configuring Your Tablespaces
- Creating the Database (MetaData) Schema for UIM
- Installing and Configuring Oracle Database Real Application Clusters
- Tuning the Database
- Enabling and Configuring Server Affinity

Database Connection Information

Table 3-1 lists database connection details that you are required to provide during the Oracle Database installation.

Table 3-1 Database Connection Information

Information Type	Description	Default Value
Hostname	Host name of the server where you install the Oracle database.	This option has no default value.
Port number	The number assigned to this specific port. Port numbers are usually predefined and you can accept the provided default value.	**1521**
User name	Your database user name. You define the user name when you install the database.	**sys**
Password	The password to connect to the database as the user for which you provided the user name. You define this password along with the user name during database installation. **Note**: The password should comply to Oracle Database Password Policy. It should contain one lower case alphabet, one upper alphabet, one number, and one special character.	This option has no default value.
Service Name	The name of the database service or instance to remotely connect to the database.	**orcl**

Setting the Database Parameters

If you are installing Oracle Database on a UNIX system, set the following parameters:

- 8-bit ASCII character set
- NLS_LANG=AMERICAN_AMERICA.WE8ISO8859P1 (for English)

  or

  NLS_LANG=AL32UTF8 (for any other language)

Setting the Database Time Zone

The Oracle database must have the correct time zone setting because UIM uses the datatype TIMESTAMP WITH LOCAL TIME ZONE in its database schema.

See *Oracle Database Globalization Support Guide* for information and instructions on setting the time zone.

> **Note:**
>
> - After UIM is installed, the database time zone cannot be changed. Ensure the time zone is correctly set before installing UIM.
> - The Database server and the Application server must be in the same time zone.

Creating and Configuring Your Tablespaces

You must set up your tablespaces before installing UIM. For a minimum installation, there are at least two tablespaces, one permanent and one temporary.

The permanent tablespace stores UIM data, and the temporary tablespace is used by Oracle as a workspace while processing UIM commands. For a minimum installation, place the UIM data in one permanent tablespace. Tablespaces should be created by an experienced Oracle DBA. For assistance, contact Oracle.

In a high-throughput system, create each tablespace or set of data files on a different physical disk. Place the Oracle redo log files on a separate physical disk. You should not have any other load on this disk.

In a production system, use a RAID device for physical storage.

This example shows how to create your permanent tablespace:

```
create tablespace large_data
datafile '/u01/oradata/UIM/data_001M01_01.dbf' size 2200M
extent management local
uniform size 1M;
```

This example shows how to create your temporary tablespace:

```
create temporary tablespace large_temp
tempfile '/u01/oradata/UIM/temp_001M01_01.dbf' size 1600M
extent management local
uniform size 1M;
```

> **Note:**
>
> If you are using Chinese UTF8 characters, the block size for the tablespaces must be configured larger than 2 KB.

Creating the Database (MetaData) Schema for UIM

The MetaData schema is an Oracle Fusion Middleware component that is required by UIM. You create the schema using the Oracle Fusion Middleware Repository Creation Utility (RCU). RCU enables you to create and drop database schemas that are required for Fusion Middleware products.

> **Note:**
>
> A new schema must be created for all new UIM installations. Upgrade installations will use the schema created during the installation of that UIM instance.
>
> The RCU can run on the Linux (32 bit) and Microsoft Windows platforms. A Linux or Windows system can be used to remotely access and configure the database.

RCU for Linux or Microsoft Windows is available with the Oracle Fusion Middleware Infrastructure distribution.

> **Note:**
>
> For information about how to install this software and obtain RCU, see *Oracle Fusion Middleware Installing and Configuring the Oracle Fusion Middleware Infrastructure* at:
>
> `http://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/infin/toc.htm`

For information on creating the MetaData schema, see the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

Schema User Name Information

Table 3-2 lists schema user details that you are required to provide during schema installation.

Table 3-2 Schema User Information

Information Type	Description	Default Value
Schema User Name	Your schema user name that you will use to access the UIM schema.	This option has no default value.
Schema User Password	The password to access the UIM schema for the schema user you defined.	This option has no default value.

> **Caution:**
>
> If you attempt to create a common user or role, and the following Oracle Database error message is returned:
>
> ```
> ORA-65096: invalid common user or role name
> ```
>
> refer to "Problem: RCU Creation Fails Due to Invalid Common User or Role Name".

To create the schema for UIM using RCU:

1. Export the environment variables by running one of the following commands:

   ```
   export JAVA_HOME=$JDK_HOME
   ```

   or

   ```
   export ORACLE_HOME=$mw_home
   ```

2. Run the following command:

   ```
   . /MW_Home/oracle_common/bin/rcu
   ```

   The Welcome screen of the Repository Creation Utility appears.

3. Click **Next**.

   The Create Repository screen appears.

4. Select **Create Repository**, **System Load and Product Load**, and click **Next**.

   The Database Connection Details screen appears.

5. Do the following:

   a. From the **Database Type** list, select **Oracle Database**.

   b. In the **Host Name** field, enter the database system host name or IP address.

   c. In the **Port** field, enter the port number for the system hosting the database.

   d. In the **Service Name** field, enter the service name.

   e. In the **Username** field, enter the user name for the database user.

   > **Note:**
   >
   > This user account must have the following privileges: CATALOG, CONNECT, Create User, Create Session, Grant Any Privilege, Grant Any Role, Select Any Table, Select any Dictionary.

   > **Caution:**
   >
   > You must use the same user name and password when providing database user information during UIM installation.

   f. In the **Password** field, enter the password for the database user.

g. From the **Role** list, select **SYSDBA**.

h. Click **Next**.

The Checking Global Prerequisites screen appears, displaying the progress of establishing the connection with the specified database.

i. Click **OK**.

The Select Components screen appears.

6. On the Select Components screen, do the following:

a. Select **Create new prefix** and enter the prefix value.

The prefix is any appropriate name for your schema. RCU adds a suffix to this name.

b. Expand **Oracle AS Repository Components**.

c. Expand **AS Common Schemas** and select **Metadata Services**, **Audit Services**, **Audit Services Append**, **Audit Services Viewer**, and **Oracle Platform Security Services**.

> **Note:**
>
> The Service Table (*prefix*_**STB** and *prefix*_**WLS**) schemas are default selections and you cannot change them. You defined the prefix in step 6.a.

d. Click **Next**.

The Checking Component Prerequisites screen appears, displaying the progress of the component prerequisites check before the schemas are created.

e. Click **OK**.

The Schema Passwords screen appears.

7. Select **Use same password for all schemas**.

> **Caution:**
>
> You must use the same user name and password when providing UIM schema user information during UIM installation.

8. In the **Password** field, enter the password for the schema.

9. In the **Confirm Password** field, enter the password for the schema again and click **Next**.

The Map Tablespaces screen appears.

10. Review the entries on the Map Tablespaces screen and click **Next**.

(Optional) To create new tablespaces or modify existing tablespaces, click **Manage Tablespaces**.

The RCU Confirmation screen appears.

11. Click **OK**.

The Creating Tablespaces progress screen appears, displaying details of the creation and validation of the tablespaces.

12. Click **OK**.

The Summary screen appears. Review and verify the information you have provided.

13. Click **Create**.

    The Completion Summary screen appears, displaying details of the newly created repository.

14. Click **Close**.

15. Tune the authorization properties on the OPSS schema. Set the **-Djps.subject.cache.key** Java system property to **5**.

    See *Oracle Fusion Middleware Performance and Tuning Guide* for more information.

Installing and Configuring Oracle Database Real Application Clusters

If your network data requires multiple databases for storage purposes, Oracle recommends Oracle Real Application Clusters for high availability and scalability. Refer to the Oracle Real Application Clusters documentation on the Oracle Help Center.

Database Connection Information for Real Application Clusters Database

Table 3-3 lists database connection details for an Oracle Real Application Clusters (Oracle RAC) database that you are required to provide during the Oracle RAC installation.

Table 3-3 Database Connection Information for Oracle RAC Database

Information Type	Description	Default Value
RAC Database Connection String	The information string that is used to connect to the Oracle RAC database.	This option has no default value.
User name	Your database user name. You define the user name when you install the database.	**sys**
Password	The password to connect to the database as the user for which you provided the user name. You define this password along with the user name during database installation.	This option has no default value.

Tuning the Database

Table 3-4 and Table 3-5 provide recommended database parameters for tuning your database for the UIM installation. These are the minimum requirements for UIM.

Table 3-4 Database Creation Parameters

Parameter	Recommended Value
SGA+PGA	At least 4 GB in total. Oracle recommends that you use as much memory as you have available in the system, and also use Automatic Memory Management.
Processes	You can calculate the minimum number of processes required to handle the connection requests of all UIM application servers using the following formula: *Cumulative Maximum Capacity of all Data Sources * Number of UIM Application Servers*

Table 3-4 (Cont.) Database Creation Parameters

Parameter	Recommended Value
Connection mode	Dedicated server
Redo log file size	1024 MB minimum

Table 3-5 Database Initialization Parameters

Parameter	Recommended Value
db_file_multiblock_read_count	16
distributed_lock_timeout	1800
dml_locks	9700
job_queue_processes	10
log_buffer	31457280
open_cursors	5000
parallel_max_servers	640
plsql_code_type	NATIVE

Enabling and Configuring Server Affinity

Server affinity is a performance feature that ensures all database operations performed on data on an Oracle RAC cluster are directed to the same Oracle RAC instance. When server affinity is enabled and configured, the target Oracle RAC instance is determined by data. For example, a business interaction ID; in this scenario, server affinity ensures all operations that operate on a business interaction ID are routed to the same Oracle RAC node, reducing global cache transfers.

Server affinity is also known as data affinity.

> **Note:**
>
> By default, UIM uses extended architecture (XA) affinity. Server affinity differs from XA affinity in that XA affinity ensures all database operations performed on an Oracle RAC cluster within the context of a transaction are directed to the same Oracle RAC instance. In XA affinity, the affinity context is established based on the global transaction id, where as in server affinity the affinity context is established based on the data.

In UIM, server affinity is based on EclipseLink partitioning. See the EclipseLink documentation for more information on EclipseLink partitioning:

`http://wiki.eclipse.org/EclipseLink/Examples/JPA/Partitioning`

To enable and configure server affinity:

1. Update the following property value in the *UIM_Home*/**config/affinity-config.properties** file to **true**:

```
uim.affinity.configuration.enabled=true
```

2. In the WebLogic Server Administration Console, create JDBC Multi Data Sources pointing to each node in the Oracle RAC cluster. For example, if there are two nodes in the Oracle RAC cluster, define two Multi Data Sources by doing the following:

   a. Create two generic data sources pointing to both nodes in the Oracle RAC.

      For example:

      - InventoryTxAffinityNode1

        with JNDI name jdbc/InventoryTxAffinityNode1

      - InventoryTxAffinityNode2

        with JNDI name jdbc/InventoryTxAffinityNode2

   b. Create a Multi Data Source with JNDI name jdbc/InventoryTxNode1DataSource.

   c. Add InventoryTxAffinityNode1 to the Multi Data Source, and select the Algorithm Type of **Failover**.

      This defines InventoryTxAffinityNode1 as a data source pointing to Node1 while Node1 is up, and which fails over to Node2 if Node1 is down.

   d. Add InventoryTxAffinityNode2 to the Multi Data Source, and select the Algorithm Type of **Failover**.

      This defines InventoryTxAffinityNode2 as a data source pointing to Node2 while Node2 is up, and which fails over to Node1 if Node2 is down.

   e. Create a Multi Data Source with JNDI name jdbc/InventoryTxNode2DataSource.

   f. Add InventoryTxAffinityNode2 to the Multi Data Source, and select the Algorithm Type of **Failover**.

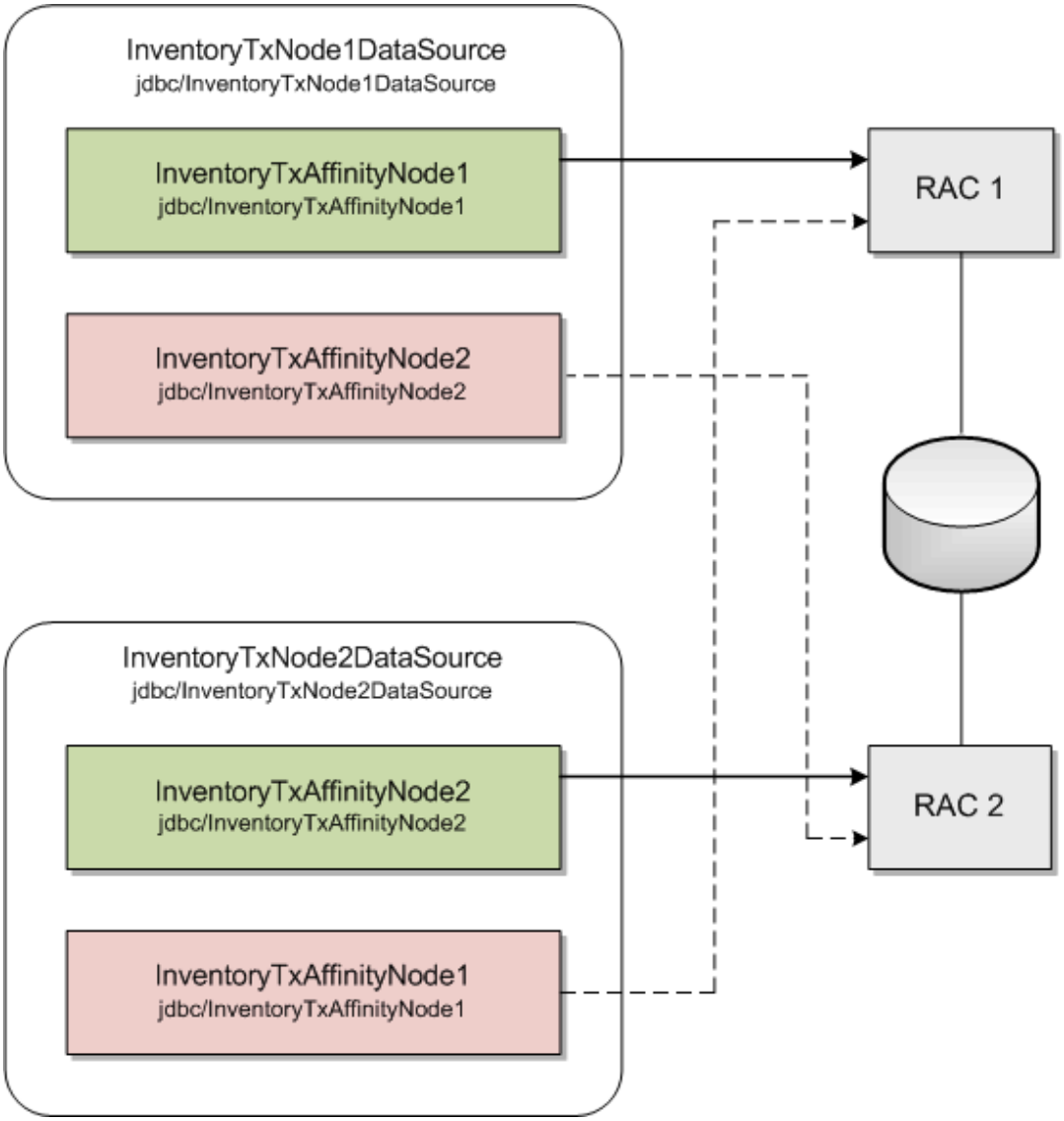
      This defines InventoryTxAffinityNode2 as a data source pointing to Node2 while Node2 is up, and which fails over to Node1 if Node2 is down.

   g. Add InventoryTxAffinityNode1 to the Multi Data Source, and select the Algorithm Type of **Failover**.

      This defines InventoryTxAffinityNode1 as a data source pointing to Node1 while Node1 is up, and which fails over to Node2 if Node1 is down.

Figure 3-1 shows the server affinity example that step 2 describes. In the figure, the solid arrows indicate the primary path, and the dotted arrows indicate the secondary path.

Figure 3-1 Service Affinity Example



3. Repeat step 2 for each node that is available. Ensure that every node in the Oracle RAC has a Multi Data Source that is primary.
4. In the *UIM_Home*/**config/affinity-config.properties** file, configure the data sources that you created by specifying the following (provide name and JNDI name):

```
uim.affinity.connectionpool.name.1           = node1
uim.affinity.connectionpool.node1.datasource = jdbc/InventoryTxNode1DataSource
uim.affinity.connectionpool.name.2           = node2
uim.affinity.connectionpool.node2.datasource = jdbc/InventoryTxNode2DataSource
```

> **Note:**
>
> If a new node is added, this list must be updated to include the new node, and the WebLogic Server must be restarted.

5. The affinity policy that is provided with the UIM installation is based on ID. If this does not meet your requirements, you can define an affinity policy that does meet your requirements in the *UIM_Home*/**config/affinity-config.properties** file.

   Table 3-6 lists and describes the properties that define an affinity policy.

Table 3-6 Affinity Policy Property Names and Descriptions

Property Name	Property Description
uim.affinity.policy.name	Name of the affinity policy. The name of your affinity policy, *policyName*, is then used in the remaining property names.
uim.affinity.*policyName*.algorithm	Determines the Java class that implements this algorithm. The default value should be **oracle.communications.inventory.api.framework.persistence.affinity.ExtendedHashPartitioningPolicy**.
uim.affinity.*policyName*.key	The context ID, which determines the Oracle RAC node.
uim.affinity.*policyName*.connectionpools	List of connection pools the affinity policy uses.
uim.affinity.*policyName*.entity.list	List of entities to which the affinity policy is applied.

4

Installing and Configuring Oracle WebLogic Server

Oracle Communications Unified Inventory Management (UIM) is installed and run on Oracle WebLogic Server. This chapter describes procedures relating to installing the WebLogic Administration Server and configuring it for UIM.

About Java Requirements

WebLogic Server is a Java application and needs a Java environment in which to run.

When WebLogic Server is installed on IBM AIX, Oracle recommends installing IBM Java.

When WebLogic Server is installed on Linux x86 or Solaris, Oracle recommends that you use the Oracle Java Development Kit (JDK).

Installing IBM Java

Download the Java SDK from the IBM website.

For information on installing IBM Java, see the IBM Java installation documentation.

Installing the Oracle JDK

Use a 64-bit Java Runtime Environment (JRE) on a 64-bit operating system (OS) for a successful UIM installation. The JRE is contained in the JDK.

Download JDK for the required platform from the Oracle Technology Network website:

http://www.oracle.com/technology

For information on installing the JDK, see the JDK installation documentation.

Downloading and Installing Oracle WebLogic Server

Oracle WebLogic Server is available as a component of the Oracle Communications Unified Inventory Management software. Oracle Communications Unified Inventory Management includes WebLogic Server, JDeveloper, and other software. See *UIM Compatibility Matrix* for the appropriate versions.

Download Oracle WebLogic Server from the Oracle software delivery website.

https://edelivery.oracle.com/

> **Note:**
>
> The Oracle WebLogic Server software is available in a 32-bit version, for each supported platform, and in a generic 64-bit version, supported across all the platforms.

For information about installing Oracle WebLogic Server, see the Oracle WebLogic Server documentation.

> **Tip:**
>
> You can launch the Oracle WebLogic Server installation from a command line by entering the following:
>
> ```
> JAVA_HOME/bin/java -jar fmw_fmwVersion_wls.jar
> ```
>
> where *fmwVersion* is the Fusion Middleware release version number.

Installing Patches

After you install Oracle WebLogic Server, you must install any applicable patches.

Download the patches from the My Oracle Support website:

`https://support.oracle.com`

You apply patches using the OPatch tool. For information about downloading and applying patches, see *Oracle Fusion Middleware Install, Patch and Upgrade* at this website:

`https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/upgrade-tasks.html`

For additional information about using the OPatch tool, refer to this document:

`https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/opatc/patching-your-environment-using-opatch.html`

Installing Oracle Application Development Runtime

Download Oracle Application Development Runtime from the UIM software on the Oracle software delivery website:

`https://edelivery.oracle.com`

This software is used to create and manage applications used by UIM.

For installing Oracle Application Development Runtime, see the Oracle Fusion Middleware documentation on the Oracle Help Center.

> **Note:**
>
> The Oracle Fusion Middleware Application Developer Installer installs both Oracle Application Development Runtime and Oracle Enterprise Manager.
>
> Install Application Developer with the same credentials used to install WebLogic Server.

See *UIM Compatibility Matrix* for Oracle Application Development Runtime patch information.

For more information on the Application Development Framework, see *Oracle Fusion Middleware Understanding Oracle Application Development Framework*.

Installing Optional Software Supported by UIM

Download and install the supported software items as needed for your requirements. See *UIM Compatibility Matrix* for the full list of optional software items that are supported by UIM and their required software versions.

Oracle Analytics Server

Use Oracle Analytics Server for data visualization and augmented AI analytics. Optionally, download the Oracle Analytics Server software from one of the following websites:

- https://www.oracle.com/solutions/business-analytics/analytics-server/analytics-server.html
- http://edelivery.oracle.com/

Install and configure Oracle Analytics Server using the information on the Installing and Configuring Oracle Analytics Server website:

https://docs.oracle.com/en/middleware/bi/analytics-server/install-config-oas/index.html

MapViewer

Use MapViewer to view a network geographically in the UIM Map View page. Optionally download the MapViewer software from the Oracle software delivery website:

https://edelivery.oracle.com

Creating a WebLogic Domain for a Single Server Installation

This section provides instructions on installing UIM on a single server. A single server arrangement is used for a small UIM deployment.

WebLogic Server Connection Information

Table 4-1 lists WebLogic Server connection details that you are required to provide during the WebLogic Server installation.

Table 4-1 Application Server Connection Information

Information Type	Description	Default Value
Host Name	The host name for this WebLogic Server instance.	*current_hostname*
Port Number	The number assigned to this specific port. Port numbers are usually predefined and you can accept the provided default value.	**7001**
User Name	Your WebLogic Server user name. You define this name when you install WebLogic Server.	weblogic
Password	The password to connect to WebLogic Server as the user for which you provided the user name. You define this password along with the user name during the WebLogic Server installation.	This option has no default value.

Creating a Standalone WebLogic Domain

To create a standalone WebLogic domain:

1. Navigate to the following directory:

   MW_Home`/wlserver/common/bin`

2. Enter the following command:

   ```
   ./config.sh
   ```

   The Configuration Type screen of the Fusion Middleware Configuration Wizard appears.

3. Select the **Create a new domain** option and in the **Domain Location** field, enter the full path for the domain or click **Browse** to navigate to the directory in which your domains are located, and then click **Next**.

   The Templates screen appears.

4. Select the **Create Domain Using Product Templates** option and from the provided list, select the following products:

   - **Basic WebLogic Server Domain** (This product is selected by default and you cannot deselect it.)
   - **Oracle Enterprise Manager - 12.2.1.4.0 [em]**
   - **Oracle JRF - 12.2.1.4.0 [oracle_common]**
   - **WebLogic Coherence Cluster Extension - 12.2.1.4.0 [wlserver]**
   - **Oracle MapViewer - 12.2.1.4.0 [oracle_common]** (This product is only available if you chose to install MapViewer.)

   > **Note:**
   >
   > The selection of the **WebLogic Coherence Cluster Extension** template for this step does not imply or require the use of the Oracle Coherence product.

5. Click **Next**.

   The Application Location screen appears.

6. In the **Domain name** field, enter a domain name.
7. In the **Domain location** field, enter the path and directory for the domain files. For example, enter the value:

   MW_Home/user_projects/domains/*base_domains*
8. In the **Application location** field, enter the path and directory for the application files. For example, enter the value:

   MW_Home/user_projects/applications/*application_name*
9. Click **Next**.

   The Administrator Account screen appears.
10. In the **Name** field, enter the administrator user name.
11. In the **Password** field, enter the administrator user password. The password must be a minimum of 8 alphanumeric characters, and must contain at least one number or special character.

    In the **Confirm Password** field, reenter your password.
12. Click **Next**.

    The Domain Mode and JDK screen appears.
13. In the Domain Mode section, select the **Production** option.

    In the JDK section, select the required JDK (Oracle JDK 1.8.0_*patch* where *patch* is the latest critical update) by doing the following:

    - Select **Available JDKs** and select a JDK from the list provided. or
    - Select **Other JDK** and browse to the location of another JDK. Ensure that this JDK is supported. See *UIM Compatibility Matrix* for details.
14. Click **Next**.

    The Database Configuration Type screen appears.
15. Select the **RCU Data** option and enter the connection information that you specified for the Service Table (STB) schema component in the Repository Creation Utility (RCU):
    a. In the **Vendor** field, select the vendor name for the component schema.
    b. In the **DBMS/Service** field, enter the database management system or service name for the component schema.
    c. In the **Driver** field, select the driver used by the component schema.
    d. In the **Host Name** field, enter the host name/IP address for the component schema.
    e. In the **Port** field, enter the port number used by the schema component.
    f. In the **Schema Owner** field, enter the owner name for the schema component.

    > **Note:**
    >
    > The default schema owner name is *prefix*_**STB**, where *prefix* is the prefix that you defined in RCU for the Service Table schema.

    g. In the **Schema Password** field, enter the password for the schema component.
    h. Click **Get RCU Configuration**, which retrieves the schema information.

i. After the schema information is retrieved successfully, click **Next**.

   The Component Datasources screen appears.

16. Do one of the following:

- For single-instance database: Verify the values in the fields and click **Next**, the JDBC Test screen appears. Continue with step 17.
- For Oracle Real Application Clusters (RAC) database: Select the **Convert to RAC multi data source** check box and click **Next**.

  The Oracle RAC Multi Data Source Component Schema screen appears.

  a. From the **Driver** list, select **Oracle's Driver (Thin) for RAC Service-Instance connections; Versions:10 and later**.

  b. In the **Service Name** field, enter the service name for the RAC database.

  c. In the **Username** field, enter the owner name of the schema component.

  d. In the **Password** field, enter the password for the schema component.

  e. In the **Host Name** field, enter the host name/IP address of the machine configured for RAC database.

  f. In the **Instance Name** field, enter the SID of the host.

  g. In the **Port** field, enter the configured port of the host.

  h. Add additional hosts by clicking **Add Host** and repeat steps 16.e through 16.g for each new host added.

  i. Click **Next**.

     The JDBC Test screen appears, which enables you to test the configurations for the schemas.

17. Select the check boxes beside the schemas you want to test and click **Test Selected Connections**.
18. Verify that all the JDBC component connections pass the validation test and click **Next**.

    The Advanced Configuration screen appears.

19. Select the following:

- **Administration Server**

20. Click **Next**.

    The Administration Server screen appears.

21. Do the following:

    a. In the **Server Name** field, enter the Administration Server name.

       This single server serves as the UIM domain Administration Server.

    b. In the **Listen Address** field, select a DNS or an IP address.

> **Note:**
>
> Use listener addresses that are equal to a resolvable DNS host or IP address. Do *not* use **localhost** or **127.0.0.1**. Those addresses interfere with clustered servers.

c. In the **Listen Port** field, accept the default.

d. Select the **Enable SSL** check box to enable SSL.

It is not a requirement to either enable or disable SSL.

If you decide to enable SSL, ensure that you configure SSL for WebLogic Server using correct cipher suites.

For more information, see “Configuring SSL in Oracle Fusion Middleware" in *Oracle Fusion Middleware Administering Oracle Fusion Middleware* at:

`https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/asadm/configuring-ssl1.html`

e. In the **SSL Listen Port** field, enter a port that is not used by another domain.

This field is enabled only if you selected the **Enable SSL** check box.

f. In the **Server Groups** list, select the **MAPVIEWER-MAN-SVR** and **JRF-MAN-SVR** groups.

The **Server Groups** list may not display both the groups if you did not install MapViewer.

g. Click **Next**.

The Configuration Summary screen appears.

22. Review the summary to verify the contents of your domain.

(Optional) Click **Previous** to return to prior screens to modify their content.

23. Click **Create** to create the domain.

24. To finish the domain creation process, click **Done**, after the domain is created successfully.

See Oracle Fusion Middleware documentation for more information.

25. To set memory requirements, see "Setting Memory Requirements for UIM".

26. Start the WebLogic Server. See "Starting the WebLogic Server".

For more information on WebLogic domains, see *Oracle WebCenter Content* documentation.

You can now manually start the Administration Server, and log in to the WebLogic Server Administration Console.

Starting the WebLogic Server

To start the WebLogic Server:

1. Open a command window.

2. Navigate to the *Domain_Home* directory, and enter the following command:

```
./startWebLogic.sh
```

The script starts the WebLogic Server.

3. Verify that the server started:

a. In a Web browser, enter:

`http://ServerName:Port/console`

where *ServerName* is the name of the Administration Server machine and *Port* is the Administration Server port number.

b. Enter the WebLogic Server administration user name and password.

c. In the Domain Structure tree, expand **Environment**, and click **Servers**.

   The Summary of Servers screen appears.

d. View the **State** of the AdminServer and see RUNNING.

   If the State is not RUNNING, you may need to wait a short period and refresh the page.

4. Look at the bottom of the Administration server command window.

   The command window should contain the following lines:

```
Server state changed to RUNNINGServer started in RUNNING mode
```

Setting Memory Requirements for UIM

In UNIX, AIX, and Solaris environments, you must set appropriate memory requirement values in the WebLogic Server to be able to install UIM. Not allotting enough memory space for the WebLogic domain can cause errors during installation.

Setting Memory Requirements for UIM in UNIX Environments

The example shows the entries in the **setDomainEnv.sh** file for setting the memory requirement values for UIM:

> **Note:**
>
> These values can be adjusted based on the available system memory. The configuration values shown are examples of the memory sizes that can be entered. If your system has sufficient memory resources, you can increase the size of the memory allocation.

1. In the *Domain_Home*/**bin** directory, open the **setDomainEnv.sh** file.
2. Set the memory arguments for your JVM as follows:

```
WLS_MEM_ARGS_64BIT="-Xms4g -Xmx4g"
```

> **Note:**
>
> Oracle recommends that you set the heap size for the Young Generation (-Xmn) to a value between 25% and 33%. Start with a value of 33%, and then gradually decrease it to 25% if the heap size of the Old Generation continues to run out of space.

3. Change the following entries from this:

```
MEM_ARGS_64BIT="${CUSTOM_MEM_ARGS_64BIT}"
MEM_ARGS_32BIT="${CUSTOM_MEM_ARGS_32BIT}"
```

   to this:

```
MEM_ARGS_64BIT="${WLS_MEM_ARGS_64BIT}"
MEM_ARGS_32BIT="${WLS_MEM_ARGS_32BIT}"
```

Setting Memory Requirements for UIM in AIX Environments

The example shows the entries in the **startWebLogic.sh** file for setting the User memory argument values for UIM:

1. In the *Domain_Home*/**bin** directory, open the **startWebLogic.sh** file.
2. Set the user memory arguments as follows:

```
USER_MEM_ARGS="-Xms1024m -Xmx3000m -Xmn850m"
export USER_MEM_ARGS
```

Setting Memory Requirements for UIM in Solaris Environments

The example shows the entries in the **setUIMEnv.sh** file for setting the User memory argument values for UIM:

1. In the *Domain_Home*/**bin** directory, open the **setUIMEnv.sh** file.
2. Set the user memory arguments as follows:

```
USER_MEM_ARGS="-Xms1024m -Xmx2560m -Xmn850m -Xrs -XX:+HeapDumpOnOutOfMemoryError -
XX:+UseConcMarkSweepGC -XX:+CMSClassUnloadingEnabled
export USER_MEM_ARGS
```

Creating a WebLogic Domain for a Server Cluster Installation with a Shared Disk Storage

A server cluster arrangement is used for load balancing, scalability, and failover. A clustered server installation (also called an Administration Server with cluster-managed servers installation) is one in which one or more WebLogic Server instances are managed by a separate Administration Server. In this arrangement, clustering the Managed Servers in WebLogic allows the servers to work together as one unit, rather than as several independent processing units. This is the configuration Oracle recommends because it provides protection if a server fails.

When working with a cluster, deploy the Cartridge Management Web Services (CMWS) and UIM adapters on the machine where the Administration server is running.

Installation Scenario

This installation scenario includes two clustered Managed Servers (uim01 and uim02) that are separate from the Administration Server, an Administration server, and a hardware load balancer, used for load balancing. Managed Servers are instances of WebLogic Servers used to host enterprise applications; in this case, UIM.

> **Note:**
>
> For more information on configuring the load balancer, see *UIM System Administrator's Guide*.

This example uses a shared disk storage environment.

For cluster deployments, it is mandatory that the **UIM_Home** directory and the **DOMAIN_Home/bin** folder be placed in a shared disk location. The advantages of using shared disk storage include easier UIM installation, maintenance, and cartridge deployment. In addition, using shared disk storage allows the Administration Server and all of the managed servers in the cluster to use the same instance of WebLogic Server. The machines on which the servers reside must have access to the shared storage.

UIM does not support session replication, but it does support server failover.

Server Cluster Example

See Table 4-2 and Table 4-3 for information on setting up the cluster arrangement.

Table 4-2 Server Cluster Example Values

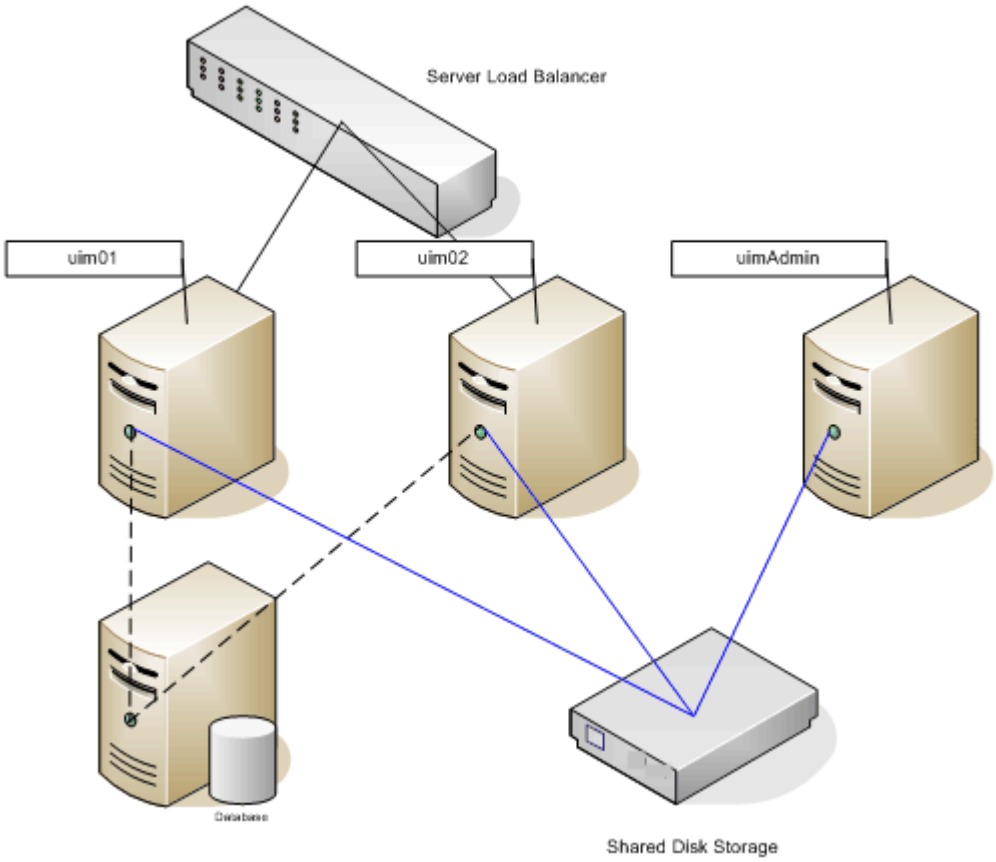
Information Type	Values
WL_Home	Home/
Domain_Home directory	*WL_Home*/user_projects/domains/cluster01
Domain login	weblogic
Domain password	*password*
Cluster DNS	UIMClusterDNS (includes the uim01 and uim02 listening IP addresses.)

Table 4-3 Servers in a Sample Cluster

Information Type	Administration Server	Cluster-Managed Server #1	Cluster-Managed Server #2
WebLogic Server	uimAdmin	uim01	uim02
Listening port	XX.XX.XX.XX:8063	XX.XX.XX.XX:8065	XX.XX.XX.XX:8066
Machine	UIM1	UIM2	UIM3

Figure 4-1 shows the servers in a sample server cluster.

Figure 4-1 Servers in a Sample Cluster



Server Cluster Prerequisites

The prerequisites for setting up a server cluster are:

- Oracle WebLogic administration experience.
- A hardware load balancer. Refer to the server load balancer configuration for details.
- A DNS entry containing all of the cluster-managed servers' listening addresses, serves as the UIM cluster address.
- A machine hosting multiple cluster-managed servers. The machine must be multi-homed.

> **Note:**
>
> UIM recommends using Multicast for Cluster messaging mode. For more information, see "Communications In a Cluster" in *Oracle Fusion Middleware Administering Clusters for Oracle WebLogic Server*.

Overview of Steps for Setting Up a Server Cluster

> **Note:**
>
> The figures shown in this section are for reference only. The actual server names that you will use may be different from those shown in the figures.

Installing an Oracle WebLogic Server cluster arrangement involves:

- Installing Oracle WebLogic Server in a Clustered Environment
- Creating a Domain
- Starting the WebLogic Server
- Starting the Cluster Servers
- Configuring the WebLogic Server StuckThreadMaxTime Value
- Configuring the WebLogic Server Proxy Timeout Value

Installing Oracle WebLogic Server in a Clustered Environment

Install WebLogic Server on the shared disk storage by following the procedures in "Downloading and Installing Oracle WebLogic Server".

Creating a Domain

To create a domain:

1. Navigate to the *WL_Home*/**common**/**bin** directory and run the following command:

   ```
   ./config.sh
   ```

   The Configuration Type screen of the Fusion Middleware Configuration Wizard appears.
2. Select the **Create a new domain** option and in the **Domain Location** field, enter the full path for the domain or click **Browse** to navigate to the directory in which your domains are located, and then click **Next**.

   The Templates screen appears.
3. Select the **Create Domain Using Product Templates** option and from the provided list, select the following products:
   - **Basic WebLogic Server Domain**

     > **Note:**
     >
     > This product is selected by default and you cannot deselect it.
   - **Oracle Enterprise Manager - 12.2.1.4.0 [em]**
   - **Oracle JRF - 12.2.1.4.0 [oracle_common]**
   - **WebLogic Coherence Cluster Extension - 12.2.1.4.0 [wlserver]**

- **Oracle MapViewer - 12.2.1.4.0 [oracle_common]**

> **Note:**
>
> – This product is only available if you chose to install MapViewer.
>
> – The selection of the **WebLogic Coherence Cluster Extension** template for this step does not imply or require the use of the Oracle Coherence product.

4. Click **Next**.

   The Application Location screen appears.

5. Do the following:

   a. In the **Domain Name** field, enter an appropriate domain name as per your requirements or standards.

   b. In the **Domain Location** field, enter the path and directory where the domain files will be created. For example, enter the value: *WLServer_Home*/**user_projects**/**domains**/*base_domains*.

   c. In the **Application Location** field, enter the path and directory for the application files. For example, enter the value:

      WLServer_Home/**user_projects**/**domains**/*application_name*

   d. Click **Next**.

      The Administrator Account screen appears.

6. In the **Name** field, enter the administrator user name.

7. In the **Password** field, enter the administrator user password. The password must be a minimum of 8 alphanumeric characters, and must contain at least one number or special character.

   In the **Confirm Password** field, re-enter your password.

8. Click **Next**.

   The Domain Mode and JDK screen appears.

9. In the Domain Mode section, select the **Production** option.

   In the JDK section, select the required JDK (Oracle JDK 1.8.0_*patch* where *patch* is the latest critical update) by doing the following:

   - Select **Available JDKs** and select a JDK from the list provided. or
   - Select **Other JDK** and browse to the location of another JDK. Ensure that this JDK is supported. See *UIM Compatibility Matrix* for details.

10. Click **Next**.

    The Database Configuration Type screen appears.

11. Select the **RCU Data** option and enter the connection information that you specified for the Service Table (STB) schema component in the Repository Creation Utility (RCU):

    a. In the **Vendor** field, select the vendor name for the component schema.

    b. In the **DBMS/Service** field, enter the database management system or service name for the component schema.

c. In the **Driver** field, select the driver used by the component schema.

d. In the **Host Name** field, enter the host name/IP address for the component schema.

e. In the **Port** field, enter the port number used by the schema component.

f. In the **Schema Owner** field, enter the owner name for the schema component.

> **Note:**
>
> The default schema owner name is *prefix*_**STB**, where *prefix* is the prefix that you defined in RCU for the Service Table schema.

g. In the **Schema Password** field, enter the password for the schema component.

h. Click **Get RCU Configuration**, which retrieves the schema information.

i. After the schema information is retrieved successfully, click **Next**.

The Component Datasources screen appears.

12. Do one of the following:

- For single-instance database: Verify the values in the fields and click **Next**, the JDBC Test screen appears. Continue with step 13.
- For Oracle Real Application Clusters (RAC) database: Select the **Convert to RAC multi data source** check box and click **Next**.

  The Oracle RAC Multi Data Source Component Schema screen appears.

  a. From the **Driver** list, select **Oracle's Driver (Thin) for RAC Service-Instance connections; Versions:10 and later**.

  b. In the **Service Name** field, enter the service name for the RAC database.

  c. In the **Username** field, enter the owner name of the schema component.

  d. In the **Password** field, enter the password for the schema component.

  e. In the **Host Name** field, enter the host name/IP address of the machine configured for RAC database.

  f. In the **Instance Name** field, enter the SID of the host.

  g. In the **Port** field, enter the configured port of the host.

  h. Add additional hosts by clicking **Add Host** and repeat steps 12.e through 12.g for each new host added.

  i. Click **Next**.

  The JDBC Test screen appears, which enables you to test the configurations for the schemas.

13. Select the check boxes beside the schemas you want to test and click **Test Selected Connections**.

14. Verify that all the JDBC component connections pass the validation test and click **Next**.

The Advanced Configuration screen appears.

15. Select the following:

- **Administration Server**
- **Topology**

- **Deployments and Services**

> **Note:**
>
> Oracle recommends that production environments for UIM use a minimum of an Administration Server and one or more Managed Servers or Clusters. Lab environments can be installed on an Administration Server only, if desired.
>
> If you select only **Administration Server**, the Domain Creation wizard does not display some dialog boxes pertaining to managed servers or clusters.

16. Click **Next**.

    The Administration Server screen appears.

17. Do the following:

    a. In the **Server Name** field, enter your Administration Server name.

    b. In the **Listen Address** field, select a DNS or an IP address.

> **Note:**
>
> Use listener addresses that are equal to a resolvable DNS host or IP address. Do not use **localhost** or **127.0.0.1**. Those addresses interfere with clustered servers.

    c. In the **Listen Port** field, accept the default.

    d. Select **Enable SSL** if you are enabling SSL.

    It is not a requirement to either enable or disable SSL.

    If you decide to enable SSL, ensure that you configure SSL for WebLogic Server using correct cipher suites.

    For more information, see “Cipher Suites" in *Fusion Middleware Securing Oracle WebLogic Server* at:

    `https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/asadm/configuring-ssl1.html`

    e. In the **SSL Listen Port** field, enter a port that is not used by another domain.

    This field is enabled only if you selected the **Enable SSL** check box.

    f. In the **Server Groups** list, accept the provided default value.

    g. Click **Next**.

    The Managed Servers screen appears.

18. Do the following:

    a. Click **Add** to add a managed server to the cluster.

    b. In the **Server Name** field, enter a name for the managed server.

    c. In the **Listen Address** field, enter the host, or IP address of the machine where the managed server is running.

> **Note:**
>
> Use listener addresses that are equal to a resolvable DNS host or IP address. Do not use **localhost** or **127.0.0.1**. Those addresses interfere with clustered servers.

d. In the **Listen Port** field, enter the number of the port where the managed server will listen for incoming messages.

e. Select **Enable SSL** as required.

f. In the **SSL Listen Port** field, enter the appropriate value only if SSL is selected.

g. In the **Server Groups** list, select the **MAPVIEWER-MAN-SVR** and **JRF-MAN-SVR** groups.

   The **Server Groups** list may not display both the groups if you did not install MapViewer.

h. (Optional) Click **Add** to add more managed servers as required on your UIM deployment.

i. Click **Next**.

   The Clusters screen appears.

> **Note:**
>
> If you are creating the domain without using a shared storage:
>
> - Ensure that the servers (MS1 and MS2) are on different machines.
> - Ensure that MS1 and Administration Server are on the same machine.
> - Ensure to apply hotfixes (if any) on all Managed Servers.

19. Do the following:

    a. Click **Add** to start configuring the cluster.

    b. In the **Cluster Name** field, enter the name for the cluster.

    c. In the **Cluster Address** field, provide the cluster address information.

       The cluster address contains each managed server along with the managed server's port separated by a comma. Separate the managed server and the port number by a colon.

    d. Click **Next**.

       The Server Template screen appears.

20. Click **Next**.

    The Dynamic Servers screen appears.

21. Click **Next**.

    The Assign Servers to Clusters screen appears.

22. Assign the servers to the cluster by moving the managed servers in the left pane to the required cluster in the right pane.

23. Click **Next**.

The HTTP Proxy Applications screen appears.

24. (Optional) Select **Create HTTP Proxy** for any proxy servers in the list.

    Click **Next**.

    The Coherence Clusters screen appears, displaying the Coherence cluster that is automatically added to the domain.

    This screen appears only if you included Coherence in the WebLogic Server installation.

25. Do the following:

    a. In the **Name** field, accept the default cluster name or type a new name for the Coherence cluster.

    b. In the **Coherence Listen Port** field, enter the port number to use as the Coherence cluster listen port.

26. Click **Next**.

    The Machines screen appears. Use this screen to change the configuration information for the machines. A machine is the logical expression of the system that hosts one or more WebLogic Server instances. The Administration Server and the Node Manager application use the machine definition to start remote servers.

27. (Optional for shared storage) Add the machines by doing one of the following:

> **Note:**
>
> This step is mandatory if you are creating the domain without using a shared storage.

- Select the **Machine** tab, and do the following:

  a. Click **Add** to create the first machine.

  b. In the **Name** field, enter a name for the machine.

  c. In the **Node Manager Listen Address** field, enter the host, or IP address of the node manager.

  d. In the **Node Manager Listen Port**, enter the port number for the node manager.

  e. (Optional) Create further machines as required on your UIM deployment.

  f. Click **Next**.

     The Deployments Targeting screen appears.

- Select the **Unix Machine** tab, and do the following:

  a. Click **Add** to create the first UNIX machine.

  b. If required, select **Enable Post Bind GID**. The default state is unselected.

  c. In the **Post Bind GID** field, enter a value or select the default.

  d. If required, select **Enable Post Bind UID**. The default state is unselected.

  e. In the **Post Bind UID** field, enter a value or select the default.

  f. In the **Node Manager Listen Address** field, enter the host, or IP address of the node manager.

  g. In the **Node Manager Listen Port** field, enter the port number of the node manager.

h. (Optional) Create further machines or UNIX machines as required on your UIM deployment.

i. Click **Next**.

   The Assign Servers to Machines screen appears.

28. Assign the servers to the machines by moving the servers in the left pane to the required machine in the right pane.

29. Click **Next**.

    The Virtual Targets screen appears.

30. Click **Next**.

    The Partition screen appears.

31. Click **Next**.

    The Deployments Targeting screen appears.

32. Under **Targets** (on the right-hand side), select the Administration Server; under **AppDeployment** (on the left-hand side), select **em**; and then click the right arrow, which moves **em** to the Administration Server for deployment.

> **Caution:**
>
> Do not deploy Enterprise Manager to the managed servers in the WebLogic domain for a server cluster installation. Only deploy Enterprise Manager on the Administration Server.
>
> Refer to "Problem: Deploying Enterprise Manager Error on Managed Servers" for more information on the error you encounter if this occurs.

33. Under **Targets** (on the right-hand side), select **Cluster**; under **AppDeployment** (on the left-hand side), select **mapviewer**; and then click the right arrow, which moves mapviewer to the Cluster for deployment.

34. Under **Targets** (on the right-hand side), select **Cluster**; select the library (on the left-hand side); and then click the right arrow, which moves all libraries to the Cluster for deployment.

35. Click **Next**.

    The Services Targeting screen appears.

36. Under **Targets**, select the Administration Server, under **Services**, select all the services; and then click the right arrow, which moves the services to the Administration Server.

37. Repeat step 36 to target services (libraries) to the cluster.

38. Click **Next**.

    The Configuration Summary screen appears.

39. Review the summary to verify the contents of your domain and click **Create** to create the domain.

    The Configuration Progress screen appears, which displays the progress of the domain creation process.

    After the domain is created successfully, the Configuration Success screen appears.

40. Click **Finish**.

    See Oracle Fusion Middleware documentation for more information.

41. To set memory requirements, see "Setting Memory Requirements for UIM".
42. To deploy cartridges over SSL ports, update `setUIMEnv.cmd` with the following Java options and restart the managed server using SSL port:

```
export JAVA_OPTIONS=-Dweblogic.DefaultProtocol=t3s
./startManagedWebLogic.sh ms1 t3s://10.177.127.61:9002
```

43. Start the WebLogic Server. See "Starting the WebLogic Server".

    You can now log in to the WebLogic Server Administration Console and start the Administration Server manually.

> **Note:**
>
> Create domains for remote machine in the same manner, in the respective machines.

Starting the WebLogic Server

You start the WebLogic Server in a clustered environment in the same way that you start the WebLogic Server in a single server environment. See "Starting the WebLogic Server".

Starting the Cluster Servers

Depending on whether you have configured the node manager, you can start the UIM cluster servers one of two ways:

- If you have not configured the node manager, you must start the cluster servers through a command prompt on the first cluster server.

  See "Starting the Cluster Servers from the First Cluster Server".
- If you have configured the node manager, you can start the cluster servers through the WebLogic Server Administration Console.

  See "Starting the Cluster Servers from the WebLogic Server".

Starting the Cluster Servers from the First Cluster Server

To start the cluster servers from the first cluster server:

1. Log in to the first cluster server machine.
2. Navigate to the *Domain_Home*/**bin** directory.
3. Start the cluster server by running the following command from the machine where the managed server is defined:

   `./startManagedWebLogic.sh` *`cluster_server_name admin_server_URL`*
4. Repeat steps 1 through 3 for each cluster server.
5. Verify that the server started:
   a. Log in to the WebLogic Server Administration Console.
   b. In the Domain Structure tree, expand **Environment**, and click **Servers**.

      The Summary of Servers page appears.
   c. View the **State** of the cluster servers and see RUNNING.

If the State is not RUNNING, you may need to wait a short period and refresh the page.

Starting the Cluster Servers from the WebLogic Server

To start the cluster servers from the WebLogic Server:

1. Log in to the WebLogic Server Administration Console.
2. In the Domain Structure tree, expand **Environment**, and click **Servers**.

   The Summary of Servers page appears.
3. Click the link for the managed server.

   The Settings for the selected server page appears.
4. Click the **Server Start** tab.
5. In **Class Path**, enter the following. (These are the classpaths defined in the **setUIMEnv.sh** and **startUIM.sh** files, which you must also define for the node manager.)

   ```
   UIM_Home/lib/aspectjrt.jar:
   UIM_Home/lib/aspectjtools.jar
   ```

   where *UIM_Home* is the UIM directory under domain. For example, **/opt/Weblogic/user_projects/domains/UIM_Rel/UIM**.

   And where *MODULES_HOME* is the modules directory under Middleware. For example, **/opt/Weblogic/modules**.
6. In **Arguments**, enter the following. (These are the arguments defined in the **setUIMEnv.sh** and **startUIM.sh** files, which you must also define for the node manager.)

   ```
   -Duim.home=UIM_Home
   -Dweblogic.log.Log4jLoggingEnabled_uim=true
   -Dlog4j.configuration_uim=loggingconfig.xml
   -Duim.logging.watchdog.timer=5000
   -Djava.io.tmpdir=UIM_Home/tmp
   -Dweblogic.management.discover.retries=6
   -javaagent:UIM_Home/lib/aspectjweaver.jar -Daj.weaving.verbose=false
   -Dsun.lang.ClassLoader.allowArraySyntax=true
   -XX:-UseSSE42Intrinsics
   -DUSE_JAAS=false -Djps.policystore.hybrid.mode=false
   -Djps.combiner.optimize.lazyeval=true -Djps.combiner.optimize=true
   -Djps.authz=ACC
   -DUIMMaster=ManagedServer
   ```

   where *UIM_Home* is the UIM directory under domain. For example, **/opt/Weblogic/user_projects/domains/UIM_Rel/UIM**.

   And where *ManagedServer* is the managed server name. For example, ManagedServer1.
7. Click **Save**.

Configuring the WebLogic Server StuckThreadMaxTime Value

During the installation of Oracle WebLogic Server and UIM in a clustered environment, if the execute thread takes more time than the *Stuck Thread Max Time:* declared in WebLogic, a *Stuck Thread Max Time:* error is displayed.

Stuck Thread Max Time: is a configurable property in WebLogic for performance tuning. It is defined as “The number of seconds that a thread must be continually working before this

server considers the thread stuck". The minimum value is 0 seconds; the default value is 600 seconds.

Consider setting *Stuck Thread Max Time:* from its default 600 seconds to a larger value such as 3600 seconds.

Use the WebLogic Server Administration Console to change this value:

1. Log in to the WebLogic Server Administration Console.
2. In the left section, under Domain Structure, expand **Environment**.
3. Click **Servers**, and then click the link for each managed server.
4. For each managed server, click the **Configuration** tab and then click the **Tuning** tab.
5. Increase the value of **Stuck Thread Max Time** to 3600.
6. Restart your domain. Your changes will take effect only after a restart.

Configuring the WebLogic Server Proxy Timeout Value

When you install UIM in a clustered environment using WebLogic HttpClusterServlet, long-running transactions time out from the proxy, which logs you out of UIM. To avoid this situation, configure the WebLogic Server proxy timeout value.

To configure the WebLogic Server proxy timeout value:

1. Navigate to and open the *Domain_Home*/**apps/OracleProxy4_cluster1_uim_proxy/WEB-INF/web.xml** file.
2. Add the following parameter to the **web.xml** file:

```
<init-param>
    <param-name>WLIOTimeoutSecs</param-name>
    <param-value>1800</param-value>
</init-param>
```

3. Save and close the **web.xml** file.
4. Restart the WebLogic Server.

Creating a WebLogic Domain for a Server Cluster Installation without a Shared Disk Storage

You can install UIM on a WebLogic Server cluster across the UIM domain. Oracle recommends that you set up a server cluster with shared disk storage. The advantages of using shared disk storage include easier UIM installation, maintenance, and cartridge deployment. However, you can set up UIM on a server cluster without a shared disk storage.

About Setting Up UIM in a Server Cluster

A server cluster arrangement is used for load balancing in most of the UIM production environments. A clustered server installation (also called an administration server with cluster-managed servers installation) is one in which one or more WebLogic Server instances are managed by a separate Administration Server. In this arrangement, clustering the managed servers in WebLogic allows the servers to work together as one unit, rather than several independent processing units. This is the configuration Oracle recommends because it provides protection when a server fails.

Installation Scenario

This section describes an installation scenario that includes two clustered managed servers (MS1 and MS2), an administration server and a proxy. After the installation, the pack or unpack mechanism of the domains is considered in this section.

> **Note:**
>
> Ensure that at least one managed server (for example, MS1) is present and running on the same machine as the administration server is running, and MS1 is up and running during cartridge deployment.

Server Cluster Example

In this example, the WebLogic directory and the UIM domain directory are not shared.

See Table 4-4 and Table 4-5 for more information on setting up the cluster arrangement.

Table 4-4 Server Cluster Example Values

Information Type	Values
ORACLE_Home	HOME/Oracle_12.2.1.4
Domain_Home directory	*HOME/Oracle_12.2.1.4*/user_projects/domains/UIMCLUSTER1
Domain login	weblogic
Domain password	*password*
Cluster DNS	CLUSTER1 (includes the MS1 and MS2 listening IP addresses.)
JMS Store	JMS DB store (not the file store)

Table 4-5 Servers in a Sample Cluster

Information Type	Administration Server	Cluster-Managed Server #1	Cluster-Managed Server #2	Proxy
WebLogic Server	AdminServer	MS1	MS2	Proxy
Listening port	XX.XX.XX.XX:9111	XX.XX.XX.XX:9113	XX.XX.XX.XX:9115	XX.XX.XX.XX:9117
Machine	blr00boe.*example*.com	blr00boe.*example*.com	blr00aif.*example*.com	blr00boe.*example*.com

Server Cluster Prerequisites

The prerequisites for setting up a server cluster without a shared storage are:

- You need Oracle WebLogic administration experience.
- You must have the same directory structure in both the machines (admin server and cluster-managed server).

- Follow the same directory structure as the WebLogic installed directory.
- The machine that hosts multiple cluster-managed servers must be multi-homed.
- Web services on JMS must be configured to have persistent stores on the database instead of the file stores.
- All cluster-managed servers must reside in the same subnet for multicast traffic.
- Use multicast for the following:
  - WebLogic cluster heart beating and JNDI update.
- Ensure that multicasts do not collide.

Setting Up a Server Cluster without a Shared Storage

To set up an Oracle WebLogic Server cluster arrangement without a shared storage:

1. Install WebLogic on an Administration Server. See "Installing Oracle WebLogic and UIM on an Administration Server Machine" for instructions.
2. Create a domain with two managed servers (MS1 and MS2) and a proxy. See "Creating a Domain" for instructions.

   The End Of Configuration page appears after the domain is created successfully on node1.

   > **Note:**
   >
   > See Table 4-5 for the server, port, and machine values of MS1, MS2, and Proxy.

3. Zip the domain to the **UIMCLUSTER1.zip** file.
4. Go to node2 and unzip the domain file.
5. Start the WebLogic Server. See "Starting the WebLogic Server" for instructions.
6. Start the server cluster. See "Starting the Cluster Servers" for instructions.
7. (Optional) If the execute thread takes more time than the value of **Stuck Thread Max Time**, increase the property value. See "Configuring the WebLogic Server StuckThreadMaxTime Value " for instructions.
8. Configure the WebLogic proxy timeout value to avoid auto-logout from UIM while doing long-running transactions during UIM installation. See "Configuring the WebLogic Server Proxy Timeout Value" for instructions.
9. Install UIM. See "Installing Unified Inventory Management" for more information.

Installing Oracle WebLogic and UIM on an Administration Server Machine

Install the WebLogic and UIM software on the administration server by following the procedures in "Downloading and Installing Oracle WebLogic Server" and *UIM System Administrator's Guide*.

Creating a WebLogic Domain for a Dynamic Server Cluster Installation

Dynamic clusters consist of server instances that can be dynamically scaled up to meet the resource needs of your application. A dynamic cluster uses a single server template to define

configuration for a specified number of generated (dynamic) server instances. See "Dynamic Clusters" from *Oracle Fusion Middleware Administering Clusters for Oracle WebLogic Server* for more information.

> **Note:**
>
> You can install UIM on WebLogic Server dynamic cluster across the UIM Domain from UIM 7.5.1 release.

Installation Scenario

This installation scenario includes dynamically managed servers (MS1,MS2,..,MSn) in dynamic cluster and an administration server. The configuration is same as the installation scenario of "Installation Scenario", with difference in the cluster as dynamic with dynamic servers.

Server Cluster Example

The server cluster example values are as follows:

Table 4-6 Server Cluster Examples for Dynamic Clusters

Information Type	Values
WL_Home	home/
Domain_Home directory	*WL_Home*/user_projects/domains/dynaclustdomain1
Domain login	weblogic
Domain password	*password*

The server template values are as follows:

Table 4-7 Server Template Values for Dynamic Clusters

Information Type	Values
Name	dyna-server-template
Listen Port	9100
SSL Listen Port	9500

The dynamic server values are as follows:

Table 4-8 Dynamic Server Values

Information Type	Values
Cluster name	dynaCluster
Server Name Prefix	ms
Server Template	dyna-server-template
Dynamic Cluster Size	6

Table 4-8 (Cont.) Dynamic Server Values

Information Type	Values
Machine Name Match Expression	<default value>
Calculated Machine Names	<default value>
Calculated Listen Ports	true
Dynamic Server Group	<default value>

Server Cluster Prerequisites

See "Server Cluster Prerequisites" for the server cluster prerequisites.

Setting Up a Dynamic Server Cluster

To set up a dynamic server cluster:

1. Install WebLogic Server. See "Installing Oracle WebLogic and UIM on an Administration Server Machine" for instructions.
2. Create a domain with dynamic managed servers and dynamic cluster. See "Creating a Domain" for instructions.
    a. In **Managed Servers**, do not configure any managed server and click **Next**.
    b. In **Server Template**, enter values for **Name** and **Listen Port**. See "Server Cluster Example" for the values.
    c. (Optional) Enter the values for **SSL Listen Port** and **Enable SSL**.
    d. In **Dynamic Servers**, enter the values for **Cluster Name**, **Server Name Prefix**, **Dynamic Cluster Size**, and **Calculated Listen Ports**. See "Server Cluster Example" for the values.
3. Start the WebLogic Server. See "Starting the WebLogic Server" for instructions.
4. Start the server cluster. See "Starting the Cluster Servers" for instructions.
5. (Optional) If the execute thread takes more time than the value of **Stuck Thread Max Time**, increase the property value. See "Configuring the WebLogic Server StuckThreadMaxTime Value " for instructions.
6. Install UIM. See "Installing Unified Inventory Management" for more information.

Configuring the WebLogic Server to Not Use KSS Demo Identity and Trust Keystores

By default, the Administration server is configured to use the demonstration identity and trust keystores. Oracle recommends that you not use the demonstration keystores in a production environment.

To configure the WebLogic Server to not use the KSS demonstration identity and trust keystores:

1. Log in to the WebLogic Server Administration Console using the Administrator credentials.

    The WebLogic Server Administration Console is displayed.

2. Click **Lock & Edit**.
3. In the left pane, click the name of the domain where you want to install UIM.
4. Select **Security**, and then **Advanced**.
5. Deselect the **Use KSS For Demo** check box.
6. Click **Save**.
7. Restart the Administration server.

Enabling WebLogic SSL Port

You must enable the WebLogic SSL port in the WebLogic Server Console to avoid the rerouting of URL from SSL to non-SSL.

To enable the WebLogic SSL port:

1. Log in to the WebLogic Server Console using your credentials.

   The WebLogic Console is displayed.
2. Open the **Environments** tab.
3. Click **Servers** and then click **SSL_Managed_Server**.
4. Under **General**, select **Advanced**.
5. Select the **WebLogic Plug-In Enabled** checkbox.
6. Under **Client Cert Proxy Enabled** field, select **Yes**.
7. Click **Save** and restart the WebLogic Server.

> **Note:**
>
> Your changes will take effect only after a restart.

Installing and Configuring Additional Software

You can perform the following steps to enhance UIM performance:

- Installing and Configuring an Authentication Provider
- Configuring WebLogic Server for the Authentication Provider
- Configuring Custom Authentication Providers

Installing and Configuring an Authentication Provider

The WebLogic Server includes an embedded LDAP store that acts as the default security provider data store for the Default Authentication, Authorization, Credential Mapping, and Role Mapping providers. You manage the embedded LDAP store using the WebLogic Server Administration Console. The Oracle Universal Installer uses this embedded LDAP server by default as the security provider. During installation, you can change the setting to use third-party security providers with WebLogic Server. See *Oracle Fusion Middleware Securing Oracle WebLogic Server* for information on the embedded LDAP server.

You can use an external LDAP store or security provider if your requirements are greater and you need more security options than are provided by the embedded LDAP server.

Oracle recommends Oracle Internet Directory as an external LDAP store.

> **Note:**
>
> The use of Oracle Internet Directory requires a separate license. Contact your Oracle representative for information on acquiring a license.

You require the following information to configure the Oracle Internet Directory:

- A static IP address

  You require a static IP address in order to install the Oracle Identity Management suite.
- Oracle Database
- WebLogic Server
- Application Development Runtime
- Identity Management
- Fusion Middleware

For information on installing and configuring Oracle Internet Directory, see *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

Configuring WebLogic Server for the Authentication Provider

To enable the WebLogic Server to work with an external LDAP store, or Oracle Internet Directory:

1. Log in to the WebLogic Server Administration Console.
2. Under Your Application's Security Settings, click **Security Realms**.

   The Summary of Security Realms screen appears.
3. Select the realm *YourRealmName*, for which you need to set the Oracle Internet Directory as the external LDAP store.

   The Settings For *YourRealmName* screen appears.
4. Click the **Providers** tab, and then click the **Authentication** tab.
5. Click **New**.

   The Create a New Authentication Provider screen appears.
6. In the **Name** field, enter the name of the authenticator.
7. From the **Type** list, select **OracleInternetDirectoryAuthenticator**.
8. Click **OK**.

   The Settings For *YourRealmName* screen appears, showing the newly created authentication name in the **Authentication** tab.
9. Click the link for the authentication name.

   The Settings for *AuthenticatorName* screen appears.
10. In the **Control Flag** list, select **SUFFICIENT**.
11. Click **Save**.

12. Click the **Provider Specific** tab.
13. Under the Connection section, in the following fields, enter the relevant values:
    - Host
    - Port
    - Principal
    - Credentials
    - Confirm Credentials
14. Under the Users section, in the following fields, enter the relevant values:
    - User Base DN

      Ensure that you provide the following value:

      ```
      cn=Users,dc=idc,dc=oracle,dc=com
      ```
    - All User Filter
    - User From Name Filter
    - User Search Scope
    - User Name Attribute
    - User Object Class
15. Under the Groups section, in the following fields, enter the relevant values:
    - Group Base DN

      Ensure that you provide the following value:

      ```
      cn=Groups,dc=idc,dc=oracle,dc=com
      ```
    - All Groups Filter
    - Group From Name Filter
    - Group Search Scope
    - Group Membership Searching
    - Max Group Membership Search Level
16. Click **Save**.
17. Restart the WebLogic Server.
18. Log in to the WebLogic Server Administration Console.
19. Navigate to the **Settings For** *YourRealmName* screen, and click **Reorder**.

    The Reorder Authentication Providers screen appears.
20. Use the Up and Down arrows to reorder the listed Authentication Providers, and click **OK**.

Configuring Custom Authentication Providers

You can configure custom authentication providers for your external security provider. In which case, you are required to manually create users and groups before starting UIM installation.

Create the following groups and the corresponding users in the new authentication provider store:

- Group: **uim-users**

User: **uimuser**

(**uimuser** is a member of the **uim-users** group.)

- Group: **uim-metrics-users**

  User: **uimmetricsuser**

  (**uimmetricsuser** is a member of the **uim-metrics-users** group.)

> **Note:**
>
> Ensure that you create the groups and users in the default security realm.

5

Installing Unified Inventory Management

This chapter describes how to install Oracle Communications Unified Inventory Management (UIM).

About the UIM Installer

You install UIM using the Oracle Universal Installer. This UI-based installer installs the core application and configures connections with the components, based on the connection details you provide. You can install UIM by using interactive install or silent install.

- **Interactive install:** Use interactive install when you want to interact with the installer UI during installation, such as installing a UIM production environment. See "Installing UIM by Using Interactive Install".
- **Silent install:** Use silent install when you are installing UIM using the same configuration repeatedly, such as installing multiple UIM test environments. Silent install does not use the installer UI. Rather, it is a scripted installation that runs in the background. See "Installing UIM by Using Silent Install".

Installing UIM by Using Interactive Install

This section describes the procedure for installing UIM using interactive install.

Prerequisite

- Configure the WebLogic Server to not use the demonstration identity and trust keystores. See "Configuring the WebLogic Server to Not Use KSS Demo Identity and Trust Keystores" for more information.

To install UIM by using interactive install:

> **Note:**
>
> In the event that the installation fails for some reason, you are required to create a new WebLogic domain and a new database user before you begin installation again.
>
> For upgrade scenarios, retry the installation and if the installation fails again contact My Oracle Support.
>
> See "Installing and Configuring Oracle WebLogic Server ".

> **Note:**
>
> The installer must be launched from a host which has access to *Domain_Home* on the UIM AdminServer. If UIM is installed using a shared file system, then this is not an issue.

1. Download the latest version of the JRE, which is contained in the JDK. See "Installing the Oracle JDK" for more information.
2. Create a temporary directory *(temp_dir)*.
3. Download the software pack for your operating system from the Oracle software delivery website and save it to *temp_dir*:
4. Unzip the software pack in a folder of your choice using the following command:

   ```
   unzip UnifiedInventoryManagement-Release-OS.zip
   ```

   where *Release* is the version of UIM, and *OS* is your operating system.

   The **uim/Disk1/install/** folder structure is created.

   > **Note:**
   >
   > For Solaris and Linux x86 installations, the UIM installation will fail due to an Out of Memory error. To fix this issue perform the following:
   >
   > a. Navigate to the **oraparam.ini** file, located in the **uim/Disk1/install/**folder.
   > b. Open the file and locate the **JRE_MEMORY_OPTIONS** parameter.
   > c. Change the default value for the **JRE_MEMORY_OPTIONS** parameter to the following:
   >
   > ```
   > JRE_MEMORY_OPTIONS="-d64 -mx256m -XX:MaxPermSize=512m"
   > ```

5. Run the Oracle Universal Installer executable file **runInstaller** using the following command:

   ```
   ./runInstaller -jreloc jre_Path
   ```

   Where *jre_Path* is the JRE location.

   > **Note:**
   >
   > The installer can also be run by specifying the install user group and Oracle Inventory directory location.
   >
   > ```
   > ./runInstaller.sh -invPtrLoc ~/orainst.loc
   > ```
   >
   > where **orainst.loc** contains:
   >
   > ```
   > inst_group=uimcluster
   > ```
   >
   > ```
   > inventory_loc=/share/uimcluster/oraInventory
   > ```

The Welcome screen of the installation wizard appears.

6. Click **Next**.

   The Select Installation Type screen appears.

> **Note:**
>
> The installer creates an Inventory directory if it does not detect any installed Oracle products on the system. The Inventory directory manages all Oracle products installed on your system.

7. Select the type of UIM installation you require, and click **Next**.
   - If you select **Complete**, this option installs all the components. The Specify Home Details screen appears.

     Skip to step 9.
   - If you select **Custom**, this option allows you to specify which components to install. This option is used for UIM upgrades. The Available Product Components screen appears.

     Continue with step 8.
8. In the Available Product Components screen, select the components you want to install, and click **Next**.
9. In the Specify Home Details screen, do the following:
   a. In the **Name** field, enter an appropriate name for the folder that will contain all of the installation files.
   b. In the **Path** field, enter the path to the folder where you want to install UIM.

> **Note:**
>
> You can also select the name for the installation from the list of names the installer provides.
>
> You can also browse for the path where UIM will be installed from the provided list using the explorer UI.

   c. Click **Next**.

   The WebLogic Administration Server Connection Information screen appears.
10. Do the following:
    a. In the **Host Name** field, enter the Listen address of the Administration server (IP address or the host name of the host machine).
    b. In the **Port Number** field, enter the Administration server port number.
    c. In the **User Name** field, enter user name with which you connected to the Administration server.

> **Note:**
>
> This user should belong to the WebLogic Server Administrator's group.

d. In the **Password** field, enter the password for the user name that you provided in the **User Name** field.

e. Select or deselect the **Use SSL** check box based on your business need.

f. In the **KeyStore Location** field, enter the keystore location if the **Use SSL** check box is selected.

g. Click **Next**.

The WebLogic Server/Cluster Selection screen appears.

11. Select the option for the server, or cluster, where you want to deploy UIM, and click **Next**.

The Database Type Selection screen appears.

> **Note:**
>
> If you select a managed server, ensure that the managed server and the node manager are running.

12. Select the option for the database type to be used and click **Next**.

- If you select Standard Oracle 19c Enterprise Database, the MDS Schema information screen appears. Proceed to step 15.
- If you select Oracle 19c Real Application Clusters Database, the RAC DB for MDS screen appears. Proceed to step 13.

13. Enter the Oracle RAC DB for MDS Schema information, by doing the following:

a. In the **RAC Database Connection String** field, enter the MDS schema information to connect to the Oracle RAC database.

For example:

HOST_NAME1:PORT1:SERVICE_NAME; HOST_NAME2:PORT2:SERVICE_NAME

> **Caution:**
>
> You must use the same user name and password provided when the UIM MDS schema was created.

b. In the **User Name** field, enter the *prefix*_**MDS** schema user name.

c. In the **Password** field, enter the password for the user name that you provided in the **User Name** field.

d. Click **Next**.

The Oracle RAC Database Nodes Connection Information screen appears.

14. Enter the Oracle RAC Database Nodes Connection information, by doing the following:

a. In the **RAC Database Connection String** field, enter the connection details to connect to the Oracle RAC database.

   For example:

   HOST_NAME1:PORT1:SERVICE_NAME; HOST_NAME2:PORT2:SERVICE_NAME

b. In the **User Name** field, enter the user name for the Oracle RAC database server.

> **Note:**
>
> The user must have the following privileges: CATALOG, CONNECT, Create User, Create Session, Grant Any Privilege, Grant Any Role, Select Any Table, Select any Dictionary, CREATE MATERIALIZED VIEW, QUERY REWRITE, RESOURCE, UNLIMITED TABLESPACE.

c. In the **Password** field, enter the password for the user name that you provided in the **User Name** field.

d. Click **Next**.

   The UIM Administrator user creation (Optional) screen appears.

   Proceed to step 22.

15. Enter the MDS Schema information by doing the following:

    a. In the **Host Name** field, enter the IP address or host name of the machine where the database server is installed.

    b. In the **Port Number** field, enter the port number with which the installer will connect to the database server.

    c. In the **User Name** field, enter the user name for the MDS schema.

    d. In the **Password** field, enter the password for the user name that you provided in the **User Name** field.

    e. In the **Service Name** field, enter the service name for that uniquely identifies your database on the system.

    f. Click **Next**.

    The Database Connection Information screen appears.

16. Enter the Database Connection information by doing the following:

    a. In the **Host Name** field, enter the IP address or host name of the machine where the database server is installed.

    b. In the **Port Number** field, enter the port number with which the installer will connect to the database server.

    c. In the **User Name** field, enter the user name for the database server.

> **Caution:**
>
> You must use the same user name and password that you provided when you set up the database schema using the Repository Creation Utility (RCU).
>
> The user must have the following privileges: CATALOG, CONNECT, Create User, Create Session, Grant Any Privilege, Grant Any Role, Select Any Table, Select any Dictionary, CREATE MATERIALIZED VIEW, QUERY REWRITE, RESOURCE, UNLIMITED TABLESPACE.
>
> See "Creating the Database (MetaData) Schema for UIM" for more information.

d. In the **Password** field, enter the password for the user name that you provided in the **User Name** field.

e. In the **Service Name** field, enter the service name for that uniquely identifies your database on the system.

f. Click **Next**.

The UIM database schema creation screen appears.

17. Select whether or not to create the UIM database schema and click **Next**.

> **Caution:**
>
> Ensure the user has the database privileges mentioned in the step 14.b

> **Note:**
>
> If you select to create the UIM database schema, the schema will be empty.
>
> If you select not to create the UIM database schema, then you are using an existing schema (from a previous install or a manually created UIM schema).

The Unified Inventory Management Schema Information screen appears.

18. Enter the UIM database schema information, by doing the following:

a. In the **User Name** field, enter the user name for the Unified Inventory Management schema.

b. In the **Password** field, enter the password for the user name that you provided in the **User Name** field.

c. In the **System Tablespace** field, enter the name for the permanent tablespace.

d. In the **Temp Tablespace** field, enter the name for the temporary tablespace.

e. Click **Next**.

The Security Provider Selection screen appears.

19. Select the security provider you want to use and click **Next**.

- If you select the default WebLogic security provider (**Embedded_LDAP**) option, the CMWS User Information screen appears. Continue with step 21.

- If you select the external security provider option (**External_LDAP**), the External Security Provider Connection Information screen appears. Continue with step 20.

20. Enter the External Security Provider information, by doing the following:
    a. In the **LDAP Server Host Name** field, enter the host name for the external LDAP server.
    b. In the **LDAP Server Port Number** field, enter the port number for the external LDAP server.
    c. In the **LDAP Server User Name** field, enter the user name for the external LDAP server.
    d. In the **LDAP Server Password** field, enter the password for the external LDAP server.
    e. In the **User Base DN** field, enter the user base DN.
    f. In the **Group Base DN** field, enter the group base DN.
    g. In the **Use SSL?** field, clear the check box if you do not want to use SSL.

       This option is checked by default. If you accept the default, ensure that your server is SSL-enabled. The SSL port would have been configured when creating the domain.
    h. In the **KeyStore Location** field, enter the location for the keystore.
    i. Click **Next**.

       The CMWS User Information screen appears.
21. Enter the CMWS User information, by doing the following:
    a. In the **User Name** field, enter the user name for the CMWS user.
    b. In the **Password** field, enter the password for the user name that you provided in the **User Name** field.
    c. In the **Confirm Password** field, enter the password again.
    d. Click **Next**.

       The UIM Administrator user creation (Optional) screen appears.
22. Do the following:
    a. In the **User Name** field, enter the user name for the UIM user.

       This user accesses and uses Unified Inventory Management.
    b. In the **Password** field, define a password for the UIM user.

       > **Note:**
       >
       > The UIM user password can be a maximum of 12 letters long, and should contain at least one numeric value and one capital letter. For example, Weblogic123.
       >
       > Also, the user name must not be part of the password.

       In the **Confirm Password** field, enter the password again, to confirm it.
    c. Click **Next**.

       The Do you want to create the UIM file store or JDBC store? screen appears.
23. Select the type of store to create, and click **Next**.

> **Note:**
>
> If File Store is selected, a file store (**inv_jms_store**) is created at the *Domain_Home*/**UIM** location.

The SSL enable Information screen appears.

24. Select whether or not to enable SSL, and click **Next**.

> **Note:**
>
> If you select **Yes**, enter the **Port** number and click **Next**.

The MapViewer information screen appears if MapViewer was installed.

25. (Optional if MapViewer is running in a different domain) In the **URL** field, enter the URL for MapViewer.
26. Click **Next**.

    The Summary screen appears.
27. Review the selections you have made in the preceding screens, and click **Install**.

    The Install screen appears.
28. You can view the installation progress.

    On successful installation of Unified Inventory Management, the End of Installation screen appears.

> **Note:**
>
> Record the URL that is displayed in the End of Installation screen, to access UIM.

29. (For installing UIM without using a shared storage) Zip the **<Domain_Home>/bin** and **<Domain_Home>/UIM** directories on node 1 and unzip them on node 2.

> **Note:**
>
> You need to zip the **<Domain_Home>/bin** and **<Domain_Home>/UIM** directories on node 1 and unzip them on node 2 for all UIM upgrade or patch installations.

30. Perform the UIM post-installation tasks. See "Unified Inventory Management Post-Installation Tasks" for more information.
31. Restart the Administration server by using the following command from within the *Domain_Home*/**bin** directory:

```
./startWebLogic.sh
```

> **Note:**
>
> For clustered deployments, you need to edit the **setDomainEnv.sh** file and set the **WLS_JDBC_REMOTE_ENABLED** parameter to true. The **setDomainEnv.sh** file is located in the *Domain_Home*/**bin** directory.
>
> The following is an example of the parameter:
>
> ```
> WLS_JDBC_REMOTE_ENABLED="-Dweblogic.jdbc.remoteEnabled=true"
> ```

32. Start the managed server by using the following command:

    ```
    ./startUIM.sh Managed_Server_Name Admin_URL
    ```

For information on verifying the successful installation of UIM, see "Verifying the Unified Inventory Management Installation".

Installing UIM by Using Silent Install

Use silent install when you are installing UIM using the same configuration repeatedly. Silent install does not use the installer UI, instead it uses a response file that must be setup with the configuration values required for your specific installation. Silent install runs in the background and is not visible to the user.

About the Response File

The installer uses a response file, which contains a pre-defined set of values, such as server connection details.

The following two response file templates come as part of the UIM installation package:

- **oracle.communications.uim.Complete.rsp**

  Use this file template if you are doing a complete installation.

- **oracle.communications.uim.Custom.rsp**

  Use this file template if you are doing a custom installation.

The response file templates contain all the fields that the installer requires values for to connect to various servers during the silent, unattended installation.

When you untar the UIM package, the response file templates are saved in the **Response** folder at the following location:

uim/Disk1/stage/Response

Populate the response file with the required server and connection values for the installer to use during installation, before you begin the silent installation. The provided response file is a template with pre-defined places where you fill in the required values of the required type. Shown here is sample section of a response file:

```
#Name       : DATABASE_TYPE
#Datatype   : String
#Description: Enter the database type whether Clustered or Non-Clustered DB. The value
should be string containing database type.
#Example: DATABASE_TYPE="&Standard Oracle 19c Enterprise Database" (for Non-RAC
database) or DATABASE_TYPE="Oracle 19c &Real Application Clusters Database" (for RAC
database)
#------------------------------------------------------------------
```

```
DATABASE_TYPE=
#---------------------------------------------------------------------
#Name       : MANAGED_SERVER_NAME
#Datatype   : String
#Description: Name of the managed server.
#Example: MANAGED_SERVER_NAME="Managed_Server_1"
#---------------------------------------------------------------------
MANAGED_SERVER_NAME=
#---------------------------------------------------------------------
#Name       : RAC_DB_COUNT
#Datatype   : String
#Description: Number of hosts in the Oracle RAC database.
#Example: RAC_DB_COUNT="2"
#---------------------------------------------------------------------
RAC_DB_COUNT=
#---------------------------------------------------------------------
#Name       : MDS_RAC_DB_COUNT
#Datatype   : String
#Description: Number of hosts in the Oracle RAC database.
#Example: MDS_RAC_DB_COUNT="2"
#---------------------------------------------------------------------
MDS_RAC_DB_COUNT=
```

In this section of the response file sample, you would provide values for the following:

```
DATABASE_TYPE=
MANAGED_SERVER_NAME=
RAC_DB_COUNT=
MDS_RAC_DB_COUNT=
#---------------------------------------------------------------------
```

Similarly, provide values for all variables described in the response file.

Populating the Response File

To populate the response file manually:

1. Navigate to the following directory:

   uim/Disk1/stage/Response
2. Open the appropriate **.rsp** template and make a copy for your current requirement.
3. Enter the required input values in the provided locations.

Starting Silent Install

Before you begin installing UIM by using silent install, ensure that you have provided all required input values in the response file template.

To install UIM by using silent install:

1. Use the following command, where *path* is the response file location, to start the installation:

   ```
   ./runInstaller -responseFile path -silent -jreloc jre_Path -waitforcompletion
   ```

   Where *path* is the response file location and *jre_Path* is the JRE location. You optionally add the **waitforcompletion** option if you want the installer to stay in the foreground.

   The installation will run silently in the background.
2. When the installation completes, manually shut down all of the servers.

3. Perform the UIM post-installation tasks. See "Unified Inventory Management Post-Installation Tasks" for more information.
4. Restart the Administration server by using the following command from within the *Domain_Home*/**bin** directory:

   ```
   ./startWebLogic.sh
   ```

5. Restart the managed servers by using the following command:

   ```
   ./startUIM.sh Managed_Server_Name Admin_URL
   ```

6. After the installation is complete, open the following file to get the URL to access UIM:

   Oracle_Home/**install/readme.txt**

   For example: **/opt/uim/OracleCommunications/install/readme.txt**

7. Copy and paste the URL in a Web browser and press **Enter** to access UIM.

   You can now access the UIM application.

For information on verifying the successful installation of UIM, see "Verifying the Unified Inventory Management Installation".

6

Unified Inventory Management Post-Installation Tasks

This chapter provides instructions for Oracle Communications Unified Inventory Management (UIM) post-installation tasks.

Configuring a Trusted Certificate for UIM

Oracle WebLogic Server provides a default certificate that automatically configures the Secure Sockets Layer (SSL) settings in your Web browser. To use another certificate, you must manually reconfigure SSL.

> **Note:**
>
> UIM uses a default certificate provided by Oracle WebLogic Server. As a result, when you connect to the UIM UI for the first time, the Web browser displays a warning page with a message indicating that the security certificate presented is not issued by a trusted certificate authority.
>
> This is expected behavior. Accept this untrusted certificate to continue to connect to the UIM UI.

For information about configuring SSL for UIM, see *UIM System Administrator's Guide*.

Deploying UIM Cartridges

Oracle recommends that you deploy all of the base cartridges into UIM. Base cartridges are located in the *UIM_Home*/**cartridges**/**base** directory. For information on base cartridges, see *UIM Cartridge Guide*.

> **Note:**
>
> The **ora_uim_mds_cartproj.zip** and **ora_uim_model_cartproj.zip** cartridges are located in this same directory, but these two cartridges should not be deployed into UIM.

You can deploy cartridges interactively from Oracle Communications Service Catalog and Design - Design Studio. You can automate cartridge deployment by using the Design Studio Cartridge Management Tool. Or, you can deploy cartridges using the UIM Cartridge Deployer Tool.

> **Note:**
>
> If you are creating the Weblogic domain without using a shared storage:
>
> - If there are any changes in the configuration/resources files after the cartridge deployment, pack and unpack **DOMAIN_HOME/UIM** contents to all nodes.
> - Ensure that MS1 is up and running during the cartridge deployment.

See the *UIM Cartridge Guide* for information about deploying cartridges and cartridge packs.

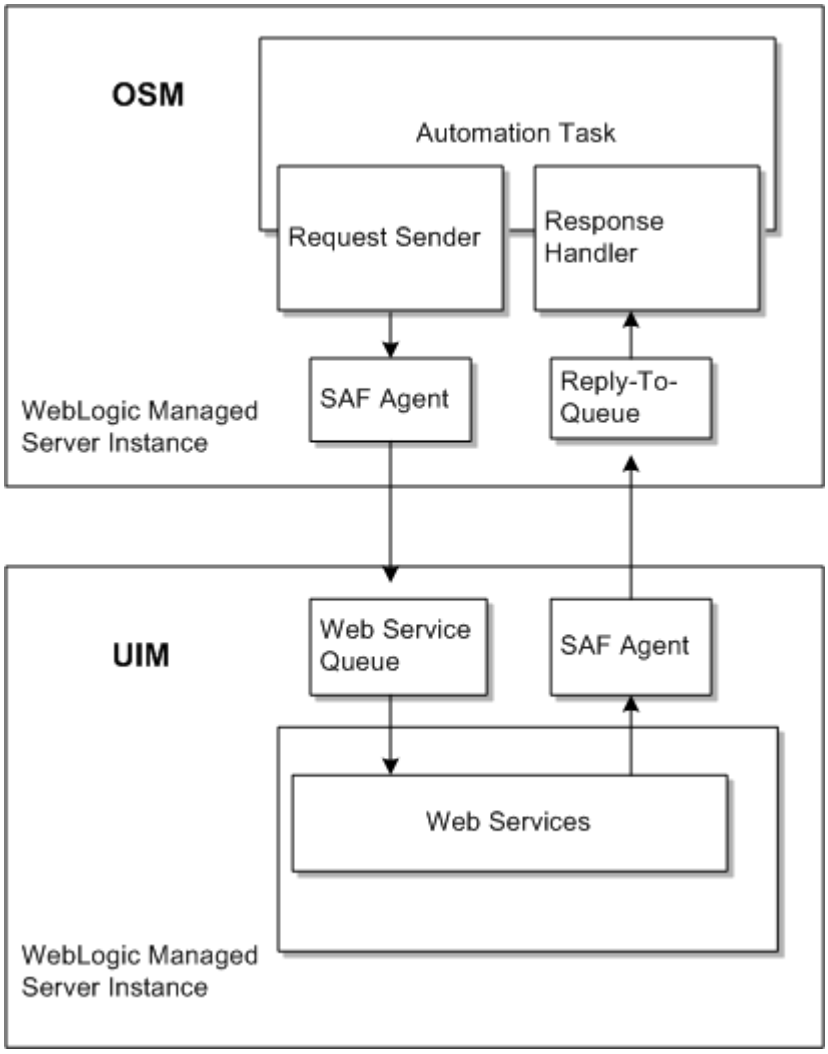
> **Note:**
>
> When working in a Development Environment, with several cartridge deployments, you might see *NullPointerException* and *ORA-01653* errors. See Knowledge Article 1506444.1 - *NullPointerException and 'ORA-01653: unable to extend table DEV_MDS.MDS_COMPONENTS' Errors When Deploying UIM Cartridges* to resolve the errors.

Connecting the UIM Web Service Interface to a Remote Application

Oracle recommends that you create a SAF agent between the UIM WebLogic Server and a remote application server. Oracle recommends this SAF agent for the Web Service interfaces to ensure reliable communication.

Figure 6-1 illustrates an example SAF configuration between the Web Service interface on UIM and a Web Service client on a remote application, in this case, the Oracle Order Service and Management (OSM) application.

Figure 6-1 SAF Agent Configuration Between UIM and a Remote Application (OSM)



In this example, an OSM SAF agent sends requests to the UIM request queue, and UIM returns responses through the UIM SAF agent to the OSM reply-to queue.

For detailed instructions for creating SAF queues and topics between UIM and OSM, see Knowledge Article 1431235.1 - *Configuring WebLogic Resources for OSM Integration With ASAP And UIM On Different Domains* on the My Oracle Support website:

https://support.oracle.com

This article is applicable to any remote application that uses a WebLogic JMS server to send and receive Web Service messages.

Routing Traffic Between Proxy and Cluster

For more information, see *Fusion Middleware Administering Clusters for Oracle WebLogic Server* at:

https://docs.oracle.com/en/middleware/fusion-middleware/weblogic-server/12.2.1.4/clust/index.html

Configuring Mail Sessions

To enable the notification functionality in UIM, you must configure JavaMail for the UIM WebLogic Server. For more information about notifications, see *UIM Developer's Guide*. Refer to *Oracle Fusion Middleware Documentation for Administration Console Online Help* for configuring the mail session at the website:

https://docs.oracle.com/en/middleware/fusion-middleware/weblogic-server/12.2.1.4/wlach/pagehelp/Mailmailmailsessionconfigtitle.html

Table 6-1 describes the important configuration properties in the mail session.

Table 6-1 Mail Session Properties

Property	Value description
JNDI Name	This is the unique JNDI name that modules use to access this mail session. For example, you can set the JNDI name to “mail/InventoryMailSession."
JavaMail SSL enable	Indicate if SSL is enabled. For example, you can set “mail.smtp.sll.enable=true."
JavaMail port	Indicates the port for a specific protocol for the mail session. For example, you can set “mail.smtp.port=465."
JavaMail host	Indicates the mail host for a specific protocol. For example, you can set “mail.smtp.host=mail.*example*.com."

Defining the Map Data Source

To configure MapViewer for UIM, you must define a map data source. See "Defining the Map Data Source" for more information.

7

Verifying the Unified Inventory Management Installation

This chapter describes how to verify that Oracle Communications Unified Inventory Management (UIM) is installed correctly.

Checking the Installation Logs

You can verify the UIM installation by viewing the installation logs. The installation logs can be found at **CentralInventorylocation/logs**. You can use the following log files to monitor installation and post-installation events:

- **installActions***TimeStamp***.log**
- **oraInstall***TimeStamp***.err**
- **dbScripts***TimeStamp***.log**
- **silentInstall***TimeStamp***.log** (for Silent Mode installation)

Checking the State of Installed Components

You can verify that UIM is installed by checking the state of all installed components.

To check the state of all installed components:

1. Log in to the WebLogic Administration Server Console.
2. In the left section, under Domain Structure, click **Deployments**.

   The Summary of Deployments page appears.
3. Ensure that all of the managed servers are running.
4. If UIM is installed successfully, the following deployments appear in the **Active** state:
   - cartridge_management_ws
   - DMS Application
   - em
   - FMW Welcome Page Application
   - oracle.communications.inventory
   - oracle.communications.inventory.cartridgeadapter
   - oracle.communications.inventory.javadoc
   - oracle.communications.inventory.mapviewer
   - wsil-wls

Logging In to Unified Inventory Management

You can verify that UIM is installed by logging in to the UIM application.

To log in to UIM:

1. Open a Web browser. See *UIM Compatibility Matrix* for supported Web browsers.
2. Enter the URL as provided by the installer at the end of the installation.
3. Press the **Enter** key.

   The Unified Inventory Management login page appears.
4. Do the following:
   a. In the **User Name** field, enter the UIM user name.
   b. In the **Password** field, enter the password for the UIM user name.

> **Note:**
>
> Use the same UIM user name and password that you provided when you installed UIM.

The Unified Inventory Management home page appears, verifying that UIM is installed successfully.

8

Troubleshooting the Unified Inventory Management Installation

This chapter describes how to troubleshoot the Oracle Communications Unified Inventory Management (UIM) installation.

Reporting Problems

Before calling Oracle Support, perform the following:

- Problems can often be fixed by shutting down UIM and restarting the computer that it runs on. See *UIM System Administrator's Guide* for more information.
- If that does not solve the problem, the first troubleshooting step is to look at the error log for the application or process that reported the problem.
- Prepare and gather the following pertinent information:
  - A clear and concise description of the problem, including when it began to occur.
  - Relevant portions of the relevant log files.
  - Relevant configuration files.
  - Recent changes in your system, even if you do not think they are relevant.
  - List of all UIM components and patches installed on your system.

When you are ready, report the problem to Oracle Support.

Problem: RCU Creation Fails Due to Invalid Common User or Role Name

If MDS schema creation through RCU fails and the following error message appears:

```
ORA-65096: invalid common user or role name.
```

The error is due to the use of a database name that is not valid for common users or roles. In addition to the usual rules for user and role names, common user and role names must start with C## or c## and consist only of ASCII characters.

Solution

When using the RCU installer (see "Creating the Database (MetaData) Schema for UIM"), you need to provide the Oracle 19*c* pluggable database (pdb) details.

To create a valid user name:

1. Ensure that the pdb is up.
2. Open a command prompt and log in to SQL*Plus.
3. Run the following command to change the open mode of the PDB SID from mounted to opened:

```
alter pluggable database $PDB_SID open;
```

4. Run the following command to switch to the PDB SID:

```
alter session set container=$PDB_SID
```

For more information about how to configure the pdb, see *Oracle Database Administrator's Guide, 19c Release 3 (19.3).*

Problem: Database Server and Application Server Have Different Dates

If the DB server and the Application server have different dates, then the two servers will not be able to communicate with each other.

Solution

Ensure that the Database server and Application server dates are set close to each other. They can have different dates due to time zone differences, but they should not be in different weeks.

See *Oracle Database Globalization Support Guide* for information and instructions on setting the date.

Problem: Unable to Create the UIM Administrator User Except During Installation

If the UIM Administrator user is not created during installation, then the user will not be able to log in to the UIM user interface or the UIM Web services.

Solution

To create the UIM Administrator user, after the UIM installation has been completed, perform the following:

1. Log in to the WebLogic Administration Server Console.
2. In the left section, under Change Center, click **Lock & Edit**.
3. In the left section, under Domain Structure, click **SecurityRealms**.

   The Summary of Security Realms page appears.
4. Click **myrealm**.

   The Settings for myrealm page appears.
5. Click the **Users and Groups** tab.
6. Click the **Groups** tab, click **New** and enter the following group properties:
   - Group name
   - Group description
   - Provider (select from the list)
7. Create the new group, click **OK**.
8. Click the **Users** tab, click **New** and enter the following user properties:
   - User name

- User description
- Provider (select from the dropdown list)
- User password

9. Create the new user, click **OK**.
10. Click **Release Configuration**.
11. Log in to the Enterprise Manager console.
12. In the left section, expand **WebLogic Domain** and select the domain name.
13. Right-click the domain name, select **Security**, and then select **Application Roles**.

    The Application Roles page appears.
14. In the **Application Stripe** field, select **oracle.communications.inventory** from the dropdown list, and then click the search icon.

    A list of role names will appear.
15. Select the **uimuser** role and click **Edit**.

    The Edit Application Role: uimuser page appears.
16. In the Members section, click **Add**.

    The Add Principal dialog box appears.
17. In the **Type** field, select **Group** from the dropdown list and then click the search icon.
18. Select the group created in steps 6 and 7, then click **OK**.
19. Click **OK** to save and close the Edit Application Role: uimuser page.

Problem: Unable to Run SQL Script

If the number of processes is not set high enough to accommodate your installation, the installer is interrupted and the following error message appears:

```
Unable to run SQL Script.
```

If you click **Retry**, the same error message appears.

If you click **Continue**, errors regarding JMS connections and JDBC connections not being found are encountered.

After the installation completes, you may notice that several database resources in the WebLogic domain were not created. In this situation, the UIM installer log reflects the following:

```
Exception Name: oui.j2ee.core.exception.JOUIUnabletoConnectException
Exception String: Error: Unable to run SQL Script.
SQL Exception: Error Code = 17002, SQL State = null,
Oracle DB Message = Io exception: Connection refused
(DESCRIPTION=(TMP=)(VSNNUM=186647296)(ERR=12516)(ERROR_STACK=
(ERROR=(CODE=12516)(EMFI=4)))).
Exception signaled in a connect operation.
Please check installer log files for more details.
Exception Severity: 1
```

And the UIM installer error log reflects the following:

```
INFO: Creating SQL script execution log file at [ /scratch/share/domains/
clusterUim723b240/UIM/scripts/llr_log.txt]
Sep 4, 2016 2:29:12 PM oui.j2ee.core.common.JDBCComponent getEncryptedConnectionImpl
SEVERE: SQL Exception: Error Code = 17002, SQL State = null, Oracle DB Message = Io
exception: Connection refused(DESCRIPTION=(TMP=)(VSNNUM=186647296)(ERR=12516)
(ERROR_STACK=
(ERROR=(CODE=12516)(EMFI=4))))
Sep 4, 2016 2:29:12 PM oui.j2ee.actions.database.AI_RunSQLScriptSP installAction
SEVERE: Error: Unable to run SQL Script. SQL Exception: Error Code = 17002, SQL State =
null , Oracle DB Message = Io exception: Connection refused(DESCRIPTION=(TMP=)
(VSNNUM=186647296)(ERR=12516)(ERROR_STACK=(ERROR=(CODE=12516)(EMFI=4)))). Exception
signaled in a connect operation. Please check installer log files for more details.
```

This problem is encountered when your total number of processes exceeds the specified number of processes. The problem can occur when running multiple managed servers, which multiplies the number of database connections used. For example, if you have 3 persistent stores per managed server, and you have 20 managed servers, 60 processes are consumed just for the persistent stores.

Solution

Change the number of processes to a higher number. The default number of processes is 150 and Oracle recommends that this value be set to 2000 when installing the database, as described in "Tuning the Database".

To change the number of processes:

1. Open a command prompt and log in to SQL*Plus.
2. Run the following command to determine the current number of processes:

   ```
   show parameter process;
   ```

   The output shows the following:

   ```
   NAME                         TYPE        VALUE
   ---------------------------- ----------  ----------
   aq_tm_processes              integer     1
   cell_offload_processing      boolean     true
   db_writer_processes          integer     1
   gcs_server_processes         integer     0
   global_txn_processes         integer     1
   job_queue_processes          integer     1000
   log_archive_max_processes    integer     4
   processes                    integer     150
   processor_group_name         string
   ```

3. Run the following command to change the number of processes:

   ```
   alter system set processes=2000 scope=spfile;
   ```

4. Run the following command to validate the current number of processes:

   ```
   show parameter process;
   ```

   The output should show the following:

   ```
   NAME                         TYPE        VALUE
   ---------------------------- ----------  ----------
   ```

```
aq_tm_processes              integer     1
cell_offload_processing      boolean     true
db_writer_processes          integer     1
gcs_server_processes         integer     0
global_txn_processes         integer     1
job_queue_processes          integer     1000
log_archive_max_processes    integer     4
processes                    integer     2000
processor_group_name         string
```

Problem: Timers are Not Started

If the timers are not started for any reason, you need to manually restart them.

Solution

To restart the timers:

1. Log in to the WebLogic Server Administration Console.
2. On the Home page, under Domain Structure, click the **Deployments** link.

   The Summary of Deployments page appears.
3. Expand **oracle.communications.inventory**.
4. Expand **EJBs**.
5. Click the **TimerBean** link.

   The Settings for TimerBean page appears.
6. Click the **Control** tab.
7. Select a timer and click **Activate Timers**.

   This restarts the selected timer.

Problem: Deploying Enterprise Manager Error on Managed Servers

This problem occurs if you create a WebLogic domain for a server cluster installation and deploy the Enterprise Manager to the managed servers. In this scenario the following NullPointerException error can occur:

```
<ManagedServer01> <[STANDBY] ExecuteThread: '2' for queue:
'weblogic.kernel.Default (self-tuning)'> <<WLS Kernel>> <>
<9ce3222e-dd29-4da5-b4a8-73602be2e080-00000003> <1482848744159> <BEA-101165>
<Could not load user defined filter in web.xml:
oracle.sysman.eml.app.EMTargetAuthFilter.
java.lang.NullPointerException
at oracle.sysman.eml.app.EMTargetAuthFilter.init(EMTargetAuthFilter.java:119)
at weblogic.servlet.internal.FilterManager$FilterInitAction.run
 (FilterManager.java:374)
```

Solution

Do not deploy Enterprise Manager to the managed servers in a WebLogic domain. Only deploy Enterprise Manager on the Admin Server.

Problem: Errors Observed in Managed Server Logs When Redeploying Cartridges During UIM Upgrade

When redeploying cartridges during UIM upgrade, you observe the following errors in the managed server logs:

```
[EL Severe]: ejb: 2017-10-20 14:00:54.023--ServerSession(810796743)--Exception
[EclipseLink-22106] (Eclipse Persistence Services - 2.6.5.v20170607-b3d05bd):
org.eclipse.persistence.exceptions.RemoteCommandManagerException
Exception Description: Could not create external JMS connection with Topic UIMCacheTopic
and Topic Factory UIMPomsTopicConnectionFactory. Also, check your context properties are
set correctly.
Internal Exception: Exception [EclipseLink-22101] (Eclipse Persistence Services -
2.6.5.v20170607-b3d05bd):
org.eclipse.persistence.exceptions.RemoteCommandManagerException
Exception Description: Could not obtain JNDI context, check your properties are set
correctly.
Internal Exception: javax.naming.AuthenticationException:
[Security:090938]Authentication failure: The specified user failed to log in.
javax.security.auth.login.FailedLoginException: [Security:090302]Authentication
Failed: User specified user denied [Root exception is
javax.security.auth.login.FailedLoginException: [Security:090938]Authentication failure:
The specified user failed to log in.
javax.security.auth.login.FailedLoginException: [Security:090302]Authentication Failed:
User specified user denied]
```

Solution

Do the following:

1. Delete the **stage**, **tmp**, and **cache** directories from the following location:

   Domain_Home/**servers/ManagedServers**

2. Redeploy the cartridges.

Problem: Errors Observed After Domain Upgrade

After upgrading the domain, you observe the following errors:

```
weblogic.application.library.LibraryDeploymentException: [J2EE:160145]Failed
to deploy library Extension-Name: jax-rs, Specification-Version: 2,
Implementation-Version: 2.22.4.0, because of conflicting library Manifest
values, and library information registered with the server:
[Implementation-Version: 2.22.4.0 vs. 2.22.1.0]. Check the library
MANIFEST.MF file and correct version information there to match server
settings, or undeploy the misconfigured library.
     at
weblogic.application.internal.library.LibraryDeploymentFactory.getLibData(Libr
aryDeploymentFactory.java:129)
     at
weblogic.application.internal.library.LibraryDeploymentFactory.createDeploymen
t(LibraryDeploymentFactory.java:50)
     at
weblogic.application.internal.DeploymentManagerImpl.createDeployment(Deploymen
tManagerImpl.java:195)
     at
weblogic.application.internal.DeploymentManagerImpl.access$800(DeploymentManag
erImpl.java:61)
```

```
     at
weblogic.application.internal.DeploymentManagerImpl$DeploymentCreatorImpl.crea
teDeployment(DeploymentManagerImpl.java:628)
     Truncated. see log file for complete stacktrace
```

Solution

Do the following:

1. Log in to the WebLogic Administration Server Console.
2. In the left section, under **Domain Structure**, click **Deployments**.

   The Summary of Deployments page appears.
3. Select the check box beside the **jax-rs-2.0.war** library and click **Delete**.
4. Reinstall the **jax-rs-2.0.war** library from the following location:

   MW_Home/**wlserver/common/deployable-libraries/jax-rs-2.0.war**

Problem: Errors Observed During UIM Installation

When installing UIM, you observe the following errors:

```
Error: Unable to execute command. DB Tool utility execution failed. Internal error
occured. Please check installer log files for more details.
SEVERE: Error: Unable to check user privilege in Oracle database. Privilege check
failed : The DB user does not have required privileges.
Please check whether the user has the following privileges ''CREATE USER','CREATE
SESSION','GRANT ANY PRIVILEGE','GRANT ANY ROLE','SELECT ANY TABLE','SELECT ANY
DICTIONARY''.
Exception signaled in a SQL operation. Please checkinstaller log files for more details.
Exception in thread "main" java.sql.SQLException: ORA-28040: No matching authentication
protocol
at oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:439)
at oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:388)
at oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:381)
```

Solution

Do the following:

1. Add the following properties in the **ORACLE_HOME/network/admin/sqlnet.ora** file:

   ```
   SQLNET.ALLOWED_LOGON_VERSION_SERVER=8
   SQLNET.ALLOWED_LOGON_VERSION_CLIENT=8
   ```
2. Restart the database.

Problem: Error Occurred While Expanding oracle.communications.inventory in the Console

While expanding the **oracle.communications.inventory** deployment from a WebLogic console, you observe the IesRunTasksRemote exception.

Solution

Deploy the **uim_core_lib.ear** and set the **Targets** to both **Administration** and the **Cluster** servers.

9
Upgrading Unified Inventory Management

This chapter explains how to upgrade your existing system to the latest release of Oracle Communications Unified Inventory Management (UIM).

About Upgrading UIM

In this chapter, the release you are upgrading from is called the *old* release. The release you are upgrading to is called the *new* release.

Upgrading to a new release of UIM consists of the following tasks:

- Planning the upgrade
- Performing the pre-upgrade tasks
- Upgrading UIM
- Performing the post-upgrade tasks

Supported Upgrade Paths

This release of UIM supports the following direct upgrade paths:

- From release 7.3.x to release 7.5.1
- From release 7.4.0 to release 7.5.1
- From release 7.4.1, 7.4.2, or 7.5.0 to release 7.5.1

Planning Your Upgrade

Before you plan your upgrade, do the following:

- Read the Release Notes for the UIM version to which you are upgrading, specifically, the “Known Issues" section.
- Read the What's New for the UIM version to which you are upgrading, to know about the new features introduced in that release.

Depending on the components affected by the upgrade, your upgrade team may include the following:

- A database administrator, to manage the database upgrade and tune the database.
- A system integrator, to handle new and existing customizations.
- A system administrator, to manage the WebLogic Server and UIM software upgrade.
- A UNIX administrator, to manage accounts, network setup, and IP configurations.

Identify who might be affected by the upgrade. For example:

- You might need to give your system administrators and UIM users notice of any system downtime.

- Tell your system administrators in advance about any changes to the system architecture (for example, Oracle database, client, or WebLogic Server upgrades).
- Train your administrators, users, cartridge developers, or system integrators on new functionality introduced by the upgrade that has an impact on their role.

You might need to make changes to your system after the upgrade is complete to accommodate new or modified features or functionality. For example, if the new release provides new security functionality, additional system configuration steps may be required. See "Upgrade Impacts" for more information.

The best way to estimate the duration of an upgrade is to perform the upgrade procedure on a test system with a copy of the production data. See "Testing the Upgrade in a Test Environment" for more information.

It is not necessary to shut down UIM or the UIM WebLogic Server domain before an upgrade. However, you must ensure that UIM is not running any operations.

Oracle recommends scheduling your upgrade during non-peak hours to minimize the disruption to your operations.

Testing the Upgrade in a Test Environment

Oracle recommends running the upgrade procedure on a test system with a copy of your production data before upgrading your production system. Test the upgrade by doing the following:

- Successfully completing all the pre-upgrade, upgrade, and post-upgrade tasks.
- Comparing the default behavior between the old and the new releases.
- Recreating any custom configurations and extensions.
- Confirming that all new behavior and functionality works.
- Ensuring that the database tables are properly installed.
- Ensuring that the database data is correct.
- Starting the WebLogic Server domain.
- Ensuring that users and user permissions are correct.
- Ensuring that productized and custom cartridges build and deploy properly.
- Logging into UIM and verifying the version number of installed components.

Upgrade Impacts

This section explains any important system changes introduced by an upgrade.

New features and new functionality are described in *UIM Release Notes*.

When upgrading to a new release of UIM, you may need to address the following upgrade impacts:

- Database Software Changes
- Database Schema Changes
- Fusion Middleware Changes
- Java Development Kit Changes

- Application Component Changes
- API Changes
- Design Studio Changes
- Cartridge Changes

Database Software Changes

This section applies to all supported upgrade paths.

You must upgrade both the server and client to the required Oracle Database Software version. See *UIM Compatibility Matrix* for more information.

Database Schema Changes

This section applies to all supported upgrade paths.

The new version of UIM requires an updated database schema. Regardless of the UIM release from which you are upgrading, and regardless of whether you opt to upgrade the Oracle Database software, you must update the database schema.

The schema changes between releases are described in the **Comparison Betweeen 7.***X.X* **and 7.***X.X+1***.xls** file, which is available in the **config** folder after you extract the **ora_uim_dbtools.jar** file. See "About Upgrading UIM" for more information.

Fusion Middleware Changes

You must upgrade your version of Fusion Middleware, which includes WebLogic Server and ADF Runtime. Apply all applicable patches.

See *UIM Compatibility Matrix* for version information regarding Oracle Fusion Middleware Application Development Runtime (and applicable patches) and Repository Creation Utility.

Java Development Kit Changes

This section applies to all supported upgrade paths.

This version of UIM requires an updated version of the Java Development Kit (JDK). Regardless of the UIM release from which you are upgrading, you must update the JDK version. See *UIM Compatibility Matrix* for version information regarding Sun Hotspot (JDK) for Linux or Solaris.

Application Component Changes

The Oracle Application Installer updates all the UIM components.

API Changes

Review the *UIM_Home***/doc/ora_uim_delta.war** file when upgrading UIM to determine if any of the upgrades affect your current extensions. The **ora_uim_delta.war** file contains information regarding changes between releases.

Design Studio Changes

You must upgrade your version of Oracle Communications Service Catalog and Design - Design Studio.

See *UIM Compatibility Matrix* for version information regarding Design Studio.

Design Studio can be set up before or after you upgrade UIM. See the Design Studio installation documentation for more information. Rather than upgrading Design Studio, install the new version and keep the old version until after you have finished upgrading UIM.

Cartridge Changes

After the upgrade is complete, cartridges must be migrated to the new release of UIM using the Design Studio Cartridge Migration Tool. It is possible that migrated cartridges contain minor compilation errors that prevent them from building and deploying. If a cartridge fails to build, open it in Design Studio and correct any compilation errors.

Upgrading UIM

This section details the upgrade procedures to upgrade UIM:

- From release 7.3.*x* to release 7.5.1 (where 7.3.*x* is 7.3.0, 7.3.1, 7.3.2, 7.3.3, 7.3.4, or 7.3.5) by doing the following tasks:
  - Pre-Upgrade Tasks for Release 7.3.x
  - Upgrading UIM
  - Post-Upgrade Tasks
- From release 7.4.0 to release 7.5.1 by doing the following tasks:
  - Pre-Upgrade Tasks from Release 7.4.0 to Release 7.5.1
  - Upgrading UIM
  - Post-Upgrade Tasks
- From release 7.4.1, 7.4.2, or 7.5.0 to release 7.5.1 by doing the following tasks:
  - Pre-Upgrade Tasks from Release 7.4.1, 7.4.2, or 7.5.0 to Release 7.5.1
  - Upgrading UIM
  - Post-Upgrade Tasks

Pre-Upgrade Tasks for Release 7.3.x

Pre-upgrade tasks must be performed while the UIM WebLogic Server is inactive.

These pre-upgrade tasks apply if your old version of UIM is version 7.3.*x*. Perform the following pre-upgrade tasks:

1. Back up the UIM and MDS databases. See *UIM System Administrator's Guide* for more information.
2. Back up the UIM WebLogic Server domain. See the WebLogic Server documentation for more information.

> **Note:**
>
> Verify that the file/folder being backed up meets the file size or pathname length requirements for the backup utility being used. For example, the maximum pathname length for the tar application is 256 characters.

3. If the old version of your UIM user interface was customized, back up the changes.

> **Caution:**
>
> UIM does not maintain backward compatibility for the user interface. If the old version of your UIM user interface was customized and you do not back up the changes, you will lose them. (You will re-apply the changes when performing the post-upgrade tasks.)

4. Before upgrading the domain, perform a backup by copying the directories that contain Fusion Middleware files. You can do this by archiving and compressing the source Oracle home and the Administration Server domain. Do the following:
   a. Shut down all processes in the Oracle home. For example, shut down the Managed Servers, the Administration Server, and any system components.
   b. Back up the Oracle home (ORACLE_HOME) on all hosts. For example:

      ```
      (UNIX) tar -cf oracle_home_backup_062015.tar ORACLE_HOME/*
      (Windows) jar cMf oracle_home_backup_0462015.jar ORACLE_HOME\*
      ```

   c. Back up the Administration Server domain separately. This backs up Java components and any system components in the domain.

      ```
      (UNIX) tar -cf domain_home_backup_062015.tar DOMAIN_HOME/*(Windows) jar cMf
      domain_home_backup_062015.jar DOMAIN_HOME\*
      ```

5. Upgrade Oracle Fusion Middleware. MapViewer is an optional software that you need to install or upgrade separately.
6. Stop the UIM domain servers.
7. Upgrade the UIM MDS Schema:
   a. Navigate to *MW_HOME*/**oracle_common/upgrade/bin/ua**

      where *MW_HOME* is the directory in which Oracle Fusion Middleware is installed.

      This directory contains the Upgrade Assistant (UA) tool, which you use to upgrade the schema.
   b. Launch the UA tool to upgrade the schema.

      The Welcome screen appears.
   c. Click **Next**.

      The Upgrade Type screen appears.
   d. Select **Individually Selected Schemas**, and click **Next**.

      The Available Components screen appears, which enables you to select components to upgrade. Select the components that are present in the WebLogic domain:

      ```
      Oracle Audit Services
      Oracle Platform Security Services
      ```

```
Oracle Metadata Services
Common Infrastructure Services
```

e. Click **Next**.

   The Domain directory screen appears.

f. Select the domain directory for upgrade, and click **Next**.

   The Prerequisites screen appears.

g. Confirm that the database backup is complete by selecting the **All affected servers are down**, **All affected data is backed up**, **Database version is certified by Oracle for Fusion Middleware upgrade**, and **Certification and system requirements have been met** check boxes, and click **Next**.

   The IAU Schema screen appears.

> **Note:**
>
> The schemas (IAU, STB, OPSS, and MDS) may appear in different sequence after step 7g.

h. From the **Database Type** list, select the database type.

i. In **Connect String**, enter the *hostname:portnumber/SID* string.

> **Note:**
>
> For a clustered environment, the *hostname:portnumber/SID* must specify the primary Oracle RAC node.

j. In **DBA User Name**, enter the database administrator user name.

k. In **DBA Password**, enter the password for the administrator user.

l. Click **Connect**.

   If the provided details are valid, the **Schema User Name** and **Schema Password** fields become enabled.

m. From the **Schema User Name** list, select the IAU schema for the current WebLogic domain.

n. In **Schema Password**, enter the database password, and click **Next**.

   The OPSS Schema screen appears.

o. Verify the details of the OPSS schema and click **Next**.

   The MDS Schema screen appears.

p. Verify the details of the MDS schema and click **Next**.

   The STB Schema screen appears.

q. Verify the details of the STB schema and click **Next**.

   The Examine screen appears.

r. Click **Next**.

   The Upgrade Summary screen appears.

s. Verify the details of the services to be upgraded and click **Upgrade**.

   The Upgrading Components screen appears. You can monitor the progress of the upgrade from this screen.

t. After the upgrade completes, click **Next**.

   The Upgrade Success screen appears.

u. Verify that the upgrade was successful and click **Close**.

8. Create the WebLogic Services (WLS) schema using the Fusion Middleware RCU, which you open using the following command:

   ```
   ./MW_Home/oracle_common/bin/rcu
   ```

   See *Oracle Fusion Middleware Repository Creation Utility User's Guide* for more information.

9. Reconfigure the WebLogic domains using the Fusion Middleware Reconfiguration Wizard, which you open using the following command:

   ```
   ./MW_Home/oracle_common/common/bin/reconfig.sh
   ```

   a. On the Select Domain screen, from the **Existing Domain Location** list, select the UIM domain that you want to upgrade and click **Next**.

      The Reconfiguration Setup Progress screen appears, displaying the progress of the reconfiguration setup process.

   b. Click **Next**.

      The Domain Mode and JDK screen appears.

      The domain mode cannot be changed during reconfiguration. It is inherited from the original domain.

   c. Select the **JDK** option and browse to the folder (JAVA_HOME) where the JDK is installed and click **Next**.

      Ensure that you have installed the correct version of the JDK. See *UIM Compatibility Matrix* for more information.

      The Database Configuration Type screen appears.

   d. Select the **RCU Data** option, complete the required fields, and then click **Get RCU Configuration**, which retrieves the schema information.

      You select the **RCU Data** option to connect to the database to retrieve schema information for all schemas that are included in the domain.

   e. Click **Next**.

   f. Navigate through the different screens by clicking **Next** on each screen and specify your settings as necessary.

   g. On the Node Manager screen, under the **Node Manager Type** area, select **Manual Node Manager Setup** and click **Next**.

      The Advanced Configuration screen appears.

   h. Select **Administration Server** and then select the other categories for which you want to perform advanced configuration and click **Next**.

      The Administration Server screen appears.

   i. Do one of the following depending on your installation type:

For a single server installation, in the **Server Groups** list, select **MAPVIEWER-MAN-SVR** and **JRF-MAN-SVR** groups and click **Next**. (The Server Groups list may not display both the groups if you did not install MapViewer.)

For a cluster installation, in the Managed Servers screen, in the **Server Groups** list, select **MAPVIEWER-MAN-SVR** and **JRF-MAN-SVR** groups and click **Next**. (The Server Groups list may not display both the groups if you did not install MapViewer.)

For each category you selected in the previous step, the appropriate configuration screen is displayed to allow you to perform advanced configuration.

j. Navigate through the different screens by clicking **Next** on each screen and specify your settings as necessary.

k. On the Deployments Targeting screen, under **Targets**, select the **oracle.communications.inventory** application and then click the left arrow, which moves the application to the **Deployments** section.

l. On the Deployments Targeting screen, under **Deployments**, select **Library**, and then under **Targets**, select the server or cluster, and then click the right arrow, which moves all the libraries to the targeted server or cluster for deployment.

m. Click **Next**.

The Services Targeting screen appears.

n. Under **Services**, select all the services, and then under **Targets**, select the server or cluster, and then click the right arrow, which moves the services to the targeted server or cluster for deployment.

o. Click **Next** until the Configuration Summary screen appears.

p. Review the detailed configuration settings of the domain and click **Reconfig**.

The Reconfiguration Progress screen appears, which displays the progress of the reconfiguration process.

After the reconfiguration process completes, the Reconfiguration Success screen appears.

q. Click **Finish**.

See Oracle Fusion Middleware documentation for more information.

10. Upgrade the WebLogic domain configurations by doing the following:

a. Navigate to the *MW_Home*/**oracle_common/upgrade/bin/ua** directory.

This directory contains the Fusion Middleware Upgrade Assistant 12*c*, which you use to upgrade the WebLogic domain configurations.

b. Launch the Fusion Middleware Upgrade Assistant.

The Welcome screen appears.

c. Click **Next**.

d. Select **WebLogic Component Configurations**, and in the **Domain Directory** field, select the WebLogic domain directory you want to upgrade, and then click **Next**.

The Prerequisites screen appears.

e. Confirm that the database backup is complete by selecting the **All affected data is backed up**, **Database version is certified by Oracle for Fusion Middleware upgrade**, and **Certification and system requirements have been met** check boxes, and click **Next**.

f. Navigate through the different screens by clicking **Next** on each screen and specifying your settings as necessary.

g. On the Upgrade Success screen, verify that the upgrade was successful and click **Close**.

   See Oracle Fusion Middleware documentation for more information.

11. Upgrade the Oracle Database software. See "Database Software Changes" for more information.

    See the Oracle Database documentation for information on upgrading the database software to a newer version.

12. Apply any required Oracle Database patches.

    See *UIM Compatibility Matrix* for more information on the Oracle Database patches.

    See the Oracle Database documentation for information on applying patches to the database.

13. Upgrade the UIM database schema by performing the following steps:

> **WARNING:**
>
> Data can change when you upgrade the UIM database schema.

a. Create two temporary directories, *temp_dir* and *temp_dir_schema*.

b. Download the UIM software for your operating system from the Oracle software delivery website and save it to *temp_dir*.

c. From the ZIP file, extract the **ora_uim_dbtools.jar** file into *temp_dir_schema*.

   The **ora_uim_dbtools.jar** file is located in the root of the downloaded ZIP file.

d. In *temp_dir_schema*, open the **ora_uim_dbtools.jar** file and extract the contents into *temp_dir_schema*.

> **Note:**
>
> For dbtools to work, you must have both the **ora_uim_dbtools.jar** file itself, and its extracted contents, in the *temp_dir_schema* directory.

e. Open the *temp_dir_schema***/config/databases.xml** file in an editor, where will you see the following:

```
<db:database name="SID">
    <db:driver>oracle.jdbc.driver.OracleDriver</db:driver>
    <db:connectionUrlString>
        jdbc:oracle:thin:@DBHostName:port:SID
    </db:connectionUrlString>
    <db:schemaComparison fromSchema="UIM_701"
        fromFile="\\filepath\dist\scripts\create.sql" toSchema="UIM_710"
        toFile="\\filepath\dist\scripts\create.sql">
    </db:schemaComparison>
</db:database>
```

Modify the <db:database> element name attribute value (**SID** in the above XML) to be the SID value of the database you are upgrading.

Modify the <db:connectionUrlString> element value (**DBHostName:port:SID** in the above XML) to be the database you are upgrading.

> **Note:**
>
> For a clustered environment, the **DBHostName:port:SID** must specify the primary Oracle RAC node.
>
> For a pluggable database (PDB), specify <db:connectionUrlString> in the following format:
>
> jdbc:oracle:thin:@**DBHostName:port/SID**

f. Grant the execute permission for the **runDB.sh** script.

g. Run the DB upgrade with the following command:

```
runDB.sh DBTOOLS_PATH JAVA_HOME upgrade
```

where *DBTOOLS_PATH* is the directory location of the **ora_uimdbtools.jar** file, and where *JAVA_HOME* is the directory location of your Java installation (up to the **jdk/bin** directory).

For example:

```
./runDB.sh /home/uimdev/download/dbupgrade/temp_dir_schema
/usr/jdk1.8.0_patch/bin upgrade
```

where *patch* is the version of your JDK. You will be prompted to enter the database SID, and the UIM DB userid and password for the DB you want to migrate.

You will also be prompted to enter **upgrade** to confirm that an upgrade is to be performed on the database.

> **Note:**
>
> The database contains tables that record if a script has been run against the database and if the script can be re-run. If the script has been previously run and it has been identified as *Not re-runnable*, the message *Update has already run* displays next to the script name in the **DbVersionController.log** file.

The following is an example of the **DbVersionController.log** file:

```
1/11/17 6:34:22 AM PST: Applying Framework Update: sqlfrmwrk - Success
1/11/17 6:34:22 AM PST: Applying Framework Update: sqlfrmwrk1 - Success
1/11/17 6:34:22 AM PST: Applying Framework Update: sqlfrmwrk2 - Success
1/11/17 6:34:22 AM PST:
1/11/17 6:34:22 AM PST:
1/11/17 6:34:22 AM PST: DbVersionController Completed Wednesday, January 11,
2017 6:34:22 AM PST
```

View the **DbVersionController.log** file to verify that all the scripts were successful or have already been run.

14. If the domain names or managed server names for the old WebLogic domain and the new WebLogic domain are different, then delete the records from the UIM database schema tables named **WL_LLR**_*servername*.

    For example, if there were two managed servers (*uim_ms1* and *uim_ms2*) from the previous UIM release, you would need to delete the records from the following tables:

    WL_LLR_UIM_MS1 and *WL_LLR_UIM_MS2*

15. If you are upgrading from UIM Release 7.3.0 and you are using the MapViewer software, delete the older version of MapViewer currently deployed in the WebLogic domain by performing the following steps:

    a. Log in to the WebLogic Server Administration Console.

    b. On the Home page, under **Domain Structure**, click the **Deployments** link.

       The Summary of Deployments page appears.

    c. Select the check box for the **oracle.communications.inventory.mapviewer** application, and click **Stop**, and then select **Force Stop Now**.

       A confirmation message appears.

    d. Click **Yes**.

    e. Select the check box for the **oracle.communications.inventory.mapviewer** application and click **Delete**.

       A confirmation message appears.

    f. Click **Yes**.

    g. In the Change Center of the Administration Console, click **Activate Changes**, which activates these changes.

16. (Optional) Install the new version of MapViewer. See *UIM Compatibility Matrix* for software version information.

17. (Optional) If you are upgrading from UIM Release 7.3.0 (and you performed step 15), update the existing WebLogic domain for MapViewer using the Fusion Middleware Configuration Wizard, with the following command:

    ```
    ./MW_Home/oracle_common/common/bin/config.sh
    ```

    a. On the Select Domain screen, select the **update an existing domain** option and from the **Existing Domain Location** list, select the UIM domain that you want to upgrade and click **Next**.

       The Domain Template screen appears.

    b. Select **Oracle MapViewer - 12.2.1.4.0 [oracle_common]**.

    c. Click **Next**.

    d. Navigate through different screens by clicking **Next** on each screen and specify your setting as necessary.

    e. On the Configuration Summary screen, click **Update** to finish the upgrade.

    f. Start the UIM domain servers.

       You can now access the newly deployed MapViewer 12c application at the following URL:

       ```
       http://ServerName:Port/mapviewer/
       ```

where:

ServerName is the application server used by UIM.

Port is the port used by UIM.

> **Note:**
>
> If you do not delete the older version of MapViewer before deploying the new version, and then restart the UIM domain server, the new MapViewer is started by default and the status of the older version changes to Failed.

18. Restart all the servers, including the Administration server, using the following command:

```
./startUIM.sh
```

Pre-Upgrade Tasks from Release 7.4.0 to Release 7.5.1

Pre-upgrade tasks must be performed while the UIM WebLogic Server is inactive.

These pre-upgrade tasks apply if your old version of UIM is version 7.4.*x*. Perform the following pre-upgrade tasks:

1. Back up the UIM and MDS databases. See *UIM System Administrator's Guide* for more information.
2. Back up the UIM WebLogic Server domain. See the WebLogic Server documentation for more information.

> **Note:**
>
> Verify that the file/folder being backed up meets the file size or pathname length requirements for the backup utility being used. For example, the maximum pathname length for the tar application is 256 characters.

3. If the old version of your UIM user interface was customized, back up the changes.

> **Caution:**
>
> UIM does not maintain backward compatibility for the user interface. If the old version of your UIM user interface was customized and you do not back up the changes, you will lose them. (You will re-apply the changes when performing the post-upgrade tasks.)

4. Before upgrading the domain, perform a backup by copying the directories that contain Fusion Middleware files. You can do this by archiving and compressing the source Oracle home and the Administration Server domain. Do the following:
   a. Shut down all processes in the Oracle home. For example, shut down the Managed Servers, the Administration Server, and any system components.
   b. Back up the Oracle home (ORACLE_HOME) on all hosts. For example:

```
(UNIX) tar -cf oracle_home_backup_062015.tar ORACLE_HOME/*
(Windows) jar cMf oracle_home_backup_0462015.jar ORACLE_HOME\*
```

c. Back up the Administration Server domain separately. This backs up Java components and any system components in the domain.

```
(UNIX) tar -cf domain_home_backup_062015.tar DOMAIN_HOME/*(Windows) jar cMf
domain_home_backup_062015.jar DOMAIN_HOME\*
```

5. Upgrade Oracle Fusion Middleware. MapViewer is an optional software that you need to install or upgrade separately.
6. Stop the UIM domain servers.
7. Reconfigure the WebLogic domains using the Fusion Middleware Reconfiguration Wizard, which you open using the following command:

```
./MW_Home/oracle_common/common/bin/reconfig.sh
```

a. On the Select Domain screen, from the **Existing Domain Location** list, select the UIM domain that you want to upgrade and click **Next**.

The Reconfiguration Setup Progress screen appears, displaying the progress of the reconfiguration setup process.

b. Click **Next**.

The Domain Mode and JDK screen appears.

The domain mode cannot be changed during reconfiguration. It is inherited from the original domain.

c. Select the **JDK** option and browse to the folder (JAVA_HOME) where the JDK is installed and click **Next**.

Ensure that you have installed the correct version of the JDK. See *UIM Compatibility Matrix* for more information.

The Database Configuration Type screen appears.

d. Select the **RCU Data** option, complete the required fields, and then click **Get RCU Configuration**, which retrieves the schema information.

You select the **RCU Data** option to connect to the database to retrieve schema information for all schemas that are included in the domain.

e. Click **Next**.

f. Navigate through the different screens by clicking **Next** on each screen and specify your settings as necessary.

g. On the Node Manager screen, under the **Node Manager Type** area, select **Manual Node Manager Setup** and click **Next**.

The Advanced Configuration screen appears.

h. Select **Administration Server** and then select the other categories for which you want to perform advanced configuration and click **Next**.

The Administration Server screen appears.

i. Do one of the following depending on your installation type:

For a single server installation, in the **Server Groups** list, select **MAPVIEWER-MAN-SVR** and **JRF-MAN-SVR** groups and click **Next**.(The Server Groups list may not display both the groups if you did not install MapViewer.)

For a cluster installation, in the Managed Servers screen, in the **Server Groups** list, select **MAPVIEWER-MAN-SVR** and **JRF-MAN-SVR** groups and click **Next**.(The Server Groups list may not display both the groups if you did not install MapViewer.)

For each category you selected in the previous step, the appropriate configuration screen is displayed to allow you to perform advanced configuration.

j. Navigate through the different screens by clicking **Next** on each screen and specify your settings as necessary.

k. On the Deployments Targeting screen, under **Targets**, select the **oracle.communications.inventory** application and then click the left arrow, which moves the application to the **Deployments** section.

l. On the Deployments Targeting screen, under **Deployments**, select **Library**, and then under **Targets**, select the server or cluster, and then click the right arrow, which moves all the libraries to the targeted server or cluster for deployment.

m. Click **Next**.

The Services Targeting screen appears.

n. Under **Services**, select all the services, and then under **Targets**, select the server or cluster, and then click the right arrow, which moves the services to the targeted server or cluster for deployment.

o. Click **Next** until the Configuration Summary screen appears.

p. Review the detailed configuration settings of the domain and click **Reconfig**.

The Reconfiguration Progress screen appears, which displays the progress of the reconfiguration process.

After the reconfiguration process completes, the Reconfiguration Success screen appears.

q. Click **Finish**.

See Oracle Fusion Middleware documentation for more information.

8. Upgrade the WebLogic domain configurations by doing the following:

a. Navigate to the *MW_Home*/**oracle_common/upgrade/bin/ua** directory.

This directory contains the Fusion Middleware Upgrade Assistant 12*c*, which you use to upgrade the WebLogic domain configurations.

b. Launch the Fusion Middleware Upgrade Assistant.

The Welcome screen appears.

c. Click **Next**.

d. Select **WebLogic Component Configurations**, and in the **Domain Directory** field, select the WebLogic domain directory you want to upgrade, and then click **Next**.

The Prerequisites screen appears.

e. Confirm that the database backup is complete by selecting the **All affected data is backed up**, **Database version is certified by Oracle for Fusion Middleware upgrade**, and **Certification and system requirements have been met** check boxes, and click **Next**.

f. Navigate through the different screens by clicking **Next** on each screen and specifying your settings as necessary.

g. On the Upgrade Success screen, verify that the upgrade was successful and click **Close**.

See Oracle Fusion Middleware documentation for more information.

9. Upgrade the Oracle Database software. See "Database Software Changes" for more information.

   See the Oracle Database documentation for information on upgrading the database software to a newer version.

10. Apply any required Oracle Database patches.

    See *UIM Compatibility Matrix* for more information on the Oracle Database patches.

    See the Oracle Database documentation for information on applying patches to the database.

11. Install the UIM and RCU schemas. See "Installing UIM and RCU Schemas" in *UIM Cloud Native Deployment Guide* for instructions.

12. If the domain names or managed server names for the old WebLogic domain and the new WebLogic domain are different, then delete the records from the UIM database schema tables named **WL_LLR**_*servername*.

    For example, if there were two managed servers (*uim_ms1* and *uim_ms2*) from the previous UIM release, you would need to delete the records from the following tables:

    WL_LLR_UIM_MS1 and *WL_LLR_UIM_MS2*

13. If you are upgrading from UIM Release 7.3.0 and you are using the MapViewer software, delete the older version of MapViewer currently deployed in the WebLogic domain by performing the following steps:

    a. Log in to the WebLogic Server Administration Console.

    b. On the Home page, under **Domain Structure**, click the **Deployments** link.

       The Summary of Deployments page appears.

    c. Select the check box for the **oracle.communications.inventory.mapviewer** application, and click **Stop**, and then select **Force Stop Now**.

       A confirmation message appears.

    d. Click **Yes**.

    e. Select the check box for the **oracle.communications.inventory.mapviewer** application and click **Delete**.

       A confirmation message appears.

    f. Click **Yes**.

    g. In the Change Center of the Administration Console, click **Activate Changes**, which activates these changes.

14. (Optional) Install the new version of MapViewer. See *UIM Compatibility Matrix* for software version information.

15. (Optional) If you are upgrading from UIM Release 7.3.0 (and you performed step 13), update the existing WebLogic domain for MapViewer using the Fusion Middleware Configuration Wizard, with the following command:

    ```
    ./MW_Home/oracle_common/common/bin/config.sh
    ```

    a. On the Select Domain screen, select the **update an existing domain** option and from the **Existing Domain Location** list, select the UIM domain that you want to upgrade and click **Next**.

       The Domain Template screen appears.

b. Select **Oracle MapViewer - 12.2.1.4.0 [oracle_common]**.

c. Click **Next**.

d. Navigate through different screens by clicking **Next** on each screen and specify your setting as necessary.

e. On the Configuration Summary screen, click **Update** to finish the upgrade.

f. Start the UIM domain servers.

You can now access the newly deployed MapViewer 12c application at the following URL:

```
http://ServerName:Port/mapviewer/
```

where:

ServerName is the application server used by UIM.

Port is the port used by UIM.

> **Note:**
>
> If you do not delete the older version of MapViewer before deploying the new version, and then restart the UIM domain server, the new MapViewer is started by default and the status of the older version changes to Failed.

16. Restart all the servers, including the Administration server, using the following command:

```
./startUIM.sh
```

Pre-Upgrade Tasks from Release 7.4.1, 7.4.2, or 7.5.0 to Release 7.5.1

1. Back up the UIM and MDS databases. See *UIM System Administrator's Guide* for more information.
2. Back up the UIM WebLogic Server domain. See the WebLogic Server documentation for more information.

> **Note:**
>
> Verify that the file/folder being backed up meets the file size or pathname length requirements for the backup utility being used. For example, the maximum pathname length for the tar application is 256 characters.

3. If the old version of your UIM user interface was customized, back up the changes.

> **Caution:**
>
> UIM does not maintain backward compatibility for the user interface. If the old version of your UIM user interface was customized and you do not back up the changes, you will lose them. (You will re-apply the changes when performing the post-upgrade tasks.)

4. Stop the UIM domain servers.
5. Upgrade the Oracle Database software. See "Database Software Changes" for more information.

   See the Oracle Database documentation for information on upgrading the database software to a newer version.
6. Apply any required Oracle Database patches.

   See *UIM Compatibility Matrix* for more information on the Oracle Database patches.

   See the Oracle Database documentation for information on applying patches to the database.
7. Upgrade the UIM database schema by performing the following steps:

> **WARNING:**
>
> Data can change when you upgrade the UIM database schema.

   a. Create two temporary directories, *temp_dir* and *temp_dir_schema*.
   b. Download the UIM software for your operating system from the Oracle software delivery website and save it to *temp_dir*.
   c. From the ZIP file, extract the **ora_uim_dbtools.jar** file into *temp_dir_schema*.

      The **ora_uim_dbtools.jar** file is located in the root of the downloaded ZIP file.
   d. In *temp_dir_schema*, open the **ora_uim_dbtools.jar** file and extract the contents into *temp_dir_schema*.

> **Note:**
>
> For dbtools to work, you must have both the **ora_uim_dbtools.jar** file itself, and its extracted contents, in the *temp_dir_schema* directory.

   e. Open the *temp_dir_schema***/config/databases.xml** file in an editor, where will you see the following:

```
<db:database name="SID">
    <db:driver>oracle.jdbc.driver.OracleDriver</db:driver>
    <db:connectionUrlString>
        jdbc:oracle:thin:@DBHostName:port:SID
    </db:connectionUrlString>
    <db:schemaComparison fromSchema="UIM_701"
        fromFile="\\filepath\dist\scripts\create.sql" toSchema="UIM_710"
        toFile="\\filepath\dist\scripts\create.sql">
    </db:schemaComparison>
</db:database>
```

      Modify the <db:database> element name attribute value (**SID** in the above XML) to be the SID value of the database you are upgrading.

      Modify the <db:connectionUrlString> element value (**DBHostName:port:SID** in the above XML) to be the database you are upgrading.

> **Note:**
>
> For a clustered environment, the **DBHostName:port:SID** must specify the primary Oracle RAC node.
>
> For a pluggable database (PDB), specify <db:connectionUrlString> in the following format:
>
> jdbc:oracle:thin:@**DBHostName:port/SID**

f. Grant the execute permission for the **runDB.sh** script.

g. Run the DB upgrade with the following command:

```
runDB.sh DBTOOLS_PATH JAVA_HOME upgrade
```

where *DBTOOLS_PATH* is the directory location of the **ora_uimdbtools.jar** file, and where *JAVA_HOME* is the directory location of your Java installation (up to the **jdk/bin** directory).

For example:

```
./runDB.sh /home/uimdev/download/dbupgrade/temp_dir_schema
/usr/jdk1.8.0_patch/bin upgrade
```

where *patch* is the version of your JDK. You will be prompted to enter the database SID, and the UIM DB userid and password for the DB you want to migrate.

You will also be prompted to enter **upgrade** to confirm that an upgrade is to be performed on the database.

> **Note:**
>
> The database contains tables that record if a script has been run against the database and if the script can be re-run. If the script has been previously run and it has been identified as *Not re-runnable*, the message *Update has already run* displays next to the script name in the **DbVersionController.log** file.

The following is an example of the **DbVersionController.log** file:

```
1/11/17 6:34:22 AM PST: Applying Framework Update: sqlfrmwrk - Success
1/11/17 6:34:22 AM PST: Applying Framework Update: sqlfrmwrk1 - Success
1/11/17 6:34:22 AM PST: Applying Framework Update: sqlfrmwrk2 - Success
1/11/17 6:34:22 AM PST:
1/11/17 6:34:22 AM PST:
1/11/17 6:34:22 AM PST: DbVersionController Completed Wednesday, January 11,
2017 6:34:22 AM PST
```

View the **DbVersionController.log** file to verify that all the scripts were successful or have already been run.

8. Restart all the servers, including the Administration server, using the following command:

```
./startUIM.sh
```

Pre-upgrade tasks must be performed while the UIM WebLogic Server is inactive.

These pre-upgrade tasks apply if your old version of UIM is version 7.4.*x*. Perform the following pre-upgrade tasks:

POMS Cache Coordination MDB

While upgrading UIM Traditional instance from a release before 7.5.0 to a 7.5.x release, the following updates are required in each of the custom applications:

- Update to **<CUSTOM_APPLICATION.ear>/poms-ejbs.jar/META-INF/ejb-jar.xml**
- Update to **<CUSTOM_APPLICATION.ear>/poms-ejbs.jar/META-INF/weblogic-ejb-jar.xml**

In the **ejb-jar.xml** file, add the following **activation-config-property** elements under **activation-config**:

```
<activation-config>
   <activation-config-property>
     <activation-config-property-name>topicMessagesDistributionMode</
activation-config-property-name>
     <activation-config-property-value>One-Copy-Per-Server</activation-config-
property-value>
   </activation-config-property>
   <activation-config-property>
     <activation-config-property-name>distributedDestinationConnection</
activation-config-property-name>
     <activation-config-property-value>EveryMember</activation-config-
property-value>
   </activation-config-property>
</activation-config>
```

In the **weblogic-ejb-jar.xml** file, **ejb-name** has to be unique across all the custom applications. To ensure that is unique, prefix the name with your custom application name as follows:

```
<ejb-name>PREFIX_WITH_CUSTOM_APPLICATION_NAMECacheCoordinationMDB</ejb-name>
```

Upgrading UIM

This section assumes you have already performed the pre-upgrade steps appropriate for the release of UIM from which you are upgrading. This section also assumes you have downloaded the software pack to *temp_dir*.

Perform the following tasks to upgrade UIM:

1. Navigate to the *temp_dir* directory and extract the contents of the downloaded software pack:

   ```
   unzip -xvf Software_Pack.zip
   ```

   The extracted software pack has the following structure:

   uim/Disk1/install/

2. Navigate to the *temp_dir***/uim/Disk1/install/** directory, and run the following command to start the installer:

   ```
   ./runInstaller -jreloc jre_Path
   ```

where *jre_Path* is the JRE location.

Ensure that you have installed the correct version of the JRE. See *UIM Compatibility Matrix* for more information.

The installer Welcome screen appears.

3. Click **Next**.
4. In the Select Installation Type screen, select **Complete**, and click **Next**.

   The Specify Home Details screen appears.
5. Do the following:
   a. In **Name**, enter, browse to, or confirm the name of the folder that contains the installation files for the old version of UIM.
   b. In **Path**, enter, browse to, or confirm the directory where the folder specified in the **Name** field is located.
   c. Click **Next**.

   The installer scans the specified directory and folder.

   The installer displays a warning message if it detects a pre-existing installation of UIM.
6. Click **Yes** to acknowledge the message.

   The WebLogic Administration Server Connection Information screen appears.
7. Do the following:
   a. In **Host Name**, enter the Listen address of the Administration server (IP address or the host name of the host machine).
   b. In **Port Number**, enter the Administration server port number.
   c. In **User Name**, enter the user name with which you connected to the Administration Server.

   > **Note:**
   >
   > This user should belong to the WebLogic Server Administrator's group.

   d. In **Password**, enter the password for the user name you provided in **User Name**.
   e. Click **Next**.

      The WebLogic Server/Cluster Selection screen appears.

   > **Note:**
   >
   > In the following steps, the WebLogic Server should be running.

8. Select the same target WebLogic Server or cluster of servers belonging to the WebLogic Server domain to upgrade, and click **Next**.

   If you are upgrading a cluster of servers, the Cluster Member Server Selection screen appears, where you can select a cluster member for UIM to install or upgrade.

   The Database Type Selection screen appears.

9. Select the same database type that is used by your old UIM installation:
   - If your old installation is connected to a standalone database, select **Standard Oracle 19c Enterprise Database** and click **Next**.

     The Database Connection Information screen appears.

     Do the following:

     a. Verify that the retrieved field values are correct, and click **Next**.
     b. In **Password**, enter the database server password for the user name you provided in **User Name**.
     c. Click **Next**.
   - If your old installation is connected to an Oracle RAC database, select **Oracle 19c Real Application Cluster Database** and click **Next**.

     The Oracle RAC DB for MDS screen appears.

     Do the following:

     a. Verify that the retrieved field values are correct, and click **Next**.
     b. In **Password**, enter the database server password for the user name you provided in **User Name**.
     c. Click **Next**.

     The Oracle RAC DB Nodes Connection Information screen appears.

     Do the following:

     a. Verify that the retrieved field values are correct, and click **Next**.
     b. In **Password**, enter the database server password for the user name you provided in **User Name**.
     c. Click **Next**.

     The MDS Schema Information screen appears.
10. Enter the MDS Schema information by doing the following:
    a. In **Host Name**, enter the IP address or host name of the machine where the database server is installed.
    b. In **Port Number**, enter the port number with which the installer will connect to the database server.
    c. In **User Name**, enter the user name for the MDS schema.
    d. In **Password**, enter the password for the user name you provided in **User Name**.
    e. In **Service Name**, enter the service name for that uniquely identifies your database on the system.
    f. Click **Next**.

    The Database Connection Information screen appears.
11. Provide the database user name and password, and click **Next**.

> **Caution:**
>
> You must use the same user name and password that you provided when you set up the database schema using the Repository Creation Utility (RCU).
>
> The user must have the following privileges: CATALOG, CONNECT, Create User, Create Session, Grant Any Privilege, Grant Any Role, Select Any Table, Select any Dictionary.
>
> See "Creating the Database (MetaData) Schema for UIM" for more information.

The UIM database schema creation screen appears.

12. Enter the UIM database schema information, by doing the following:
    a. In **User Name**, enter the user name for the Unified Inventory Management schema.
    b. In **Password**, enter the password for the user name you provided in **User Name**.
    c. In **System Tablespace**, enter the name for the permanent tablespace.
    d. In **Temp Tablespace**, enter the name for the temporary tablespace.
    e. Click **Next**.

    The Security Provider Selection screen appears.
13. Select the security provider you want to use, and click **Next**.

    The CMWS User Information screen appears.
14. Enter the CMWS User information, by doing the following:
    a. In **User Name**, enter the user name for the CMWS user.
    b. In **Password**, enter the password for the user name you provided in **User Name**.
    c. In **Confirm Password**, enter the password again.
    d. Click **Next**.

       A warning message appears because the “cmwsuser" already exists.
15. Click **OK** to acknowledge the message.

    The UIM Administrator user creation (Optional) screen appears.
16. Enter the UIM User information, by doing the following:
    a. In **User Name**, enter the user name for the UIM user.
    b. In **Password**, define a password for the UIM user.

> **Note:**
>
> The UIM user password can be a maximum of 12 letters long, and should contain at least one numeric value and one capital letter. For example, Weblogic123.
>
> Also, the user name must not be part of the password.

In **Confirm Password**, enter the password again.

c. Click **Next**.

A warning message appears because “uimuser" already exists.

17. Click **OK** to acknowledge the message.

The Do you want to create the UIM file store or JDBC store? screen appears.

18. Select the same type of store you selected when UIM was initially installed, and click **Next**.

The SSL enable Information screen appears.

19. Select whether or not to enable SSL. If you select **Yes**, enter the **Port** number. Click **Next**.

The MapViewer information or a Summary screen appears.

20. In the **URL** field, enter the URL for MapViewer if you installed MapViewer.
21. Click **Next**.

The Summary screen appears.

22. Review the selections you have made in the preceding screens, and click **Install**.

The Install screen appears.

23. You can view the installation progress.

On successful installation of Unified Inventory Management, the End of Installation screen appears.

24. Perform the post-upgrade tasks. See "Post-Upgrade Tasks" for more information.

Post-Upgrade Tasks

These post-upgrade tasks apply if your old version of UIM is version 7.2.*x*, 7.3.*x*, 7.4.*x*, or 7.5.0. Complete all of the following post-upgrade tasks after upgrading UIM, if necessary:

1. Verify that the upgrade process completed successfully before performing the remaining post-upgrade tasks. See "Verifying the Unified Inventory Management Installation" for more information.
2. If the old version of your UIM user interface was customized, apply the changes to the new version of UIM. (You backed up these changes when performing the pre-upgrade tasks.)
3. Install the new version of Design Studio. See the Design Studio documentation for more information.

   Oracle recommends installing the new version of Design Studio along side the old version of Design Studio so that you can migrate custom cartridges to the new version more easily.
4. Deploy all the 7.5.1 base cartridges into the upgraded UIM environment. For information on base cartridges, see *UIM Cartridge Guide*.
5. Redeploy any custom cartridges and cartridge packs, after migrating and compiling the cartridges and cartridge packs using Design Studio. See the Design Studio documentation for more information.
6. Repackage the **7.5.1 custom.ear** file by doing the following, regardless of whether any custom code needs to be added:

   a. In the Oracle WebLogic Server Administration Console, undeploy the existing **7.4.x custom.ear** or **7.5 custom.ear** file.

   b. Make a backup copy of the **7.5.1 custom.ear** file located in the *UIM_Home*/**app/7_5_1** directory.

c. Extract the contents of the **7.5.1 custom.ear** file to a temporary directory, such as **tempDirCustom**.

d. Copy any custom code from **7.5 custom.ear** to **7.5.1 custom.ear** (which is extracted to **tempDirCustom**).

e. Repackage the **7.5.1 custom.ear** file with the upgraded content in the **tempDirCustom** directory.

f. Copy the upgraded and repackaged **custom.ear** file to the *UIM_Home***/app/7_5_1** directory.

> **Note:**
>
> You will deploy the repackaged **custom.ear** file in a later post-upgrade step, after you have restarted the WebLogic Server.

7. For cluster server upgrades, increase the **Stuck Thread Max Time** value of each server from 600 to 1200:

   a. Log in to the WebLogic Server Administration Console.

   b. In the left section, under Domain Structure, expand **Environment**.

   c. Click **Servers**.

      The Summary of Servers page appears.

   d. Click the link for each managed server.

      The Settings for *ManagedServer* page appears, where *ManagedServer* is the name of the managed server you selected.

   e. Click the **Configuration** tab.

   f. Click the **Tuning** sub-tab.

   g. In **Stuck Thread Max Time**, change the value from **600** to **1200**.

   h. Click **Save**.

8. For clustered server upgrades, configure the WebLogic Server proxy timeout value:

   a. Navigate to and open the *Domain_Home***/apps/OracleProxy4_cluster1_uim_proxy/WEB-INF/web.xml** file.

   b. Add the following parameter to the **web.xml** file:

```
<init-param>
    <param-name>WLIOTimeoutSecs</param-name>
    <param-value>1800</param-value>
</init-param>
```

   c. Save and close the **web.xml** file.

   d. Restart the WebLogic Server.

9. If upgrading from UIM 7.2.0, convert logical devices from UIM 7.2.0 to UIM 7.2.4. (In UIM 7.2.2, logical devices were enhanced to define rate codes; so, if upgrading from UIM 7.2.2 or 7.2.3, logical devices are already converted.) To convert logical devices, run the ruleset **CONVERT_LD_SR1_TO_SR2**, by giving it a list of associated Logical Device specifications. The list of Logical Device specifications is passed to the ruleset via a text file. For example, if your text file contains the following specifications:

   - Analog Telephony Adapter

- IP Phone
- Data Networking Device

Then all the Logical Device instances that have those respective specifications will be converted.

To run the ruleset, perform the following:

a. Create a text file and list all the Logical Device Specifications for which you want to upgrade. You should list one specification per line.

b. Log in to UIM and from the **Tasks** menu select the link **Execute Rule**.

c. From the **Ruleset** dropdown menu, select **CONVERT_LD_SR1_TO_SR2**.

d. Using the **Browse** button, select the text file that contains the list of Logical Devices to be converted.

e. Click the **Process** button (upper-right corner of the UIM UI) to start the conversion.

f. Restart the WebLogic Server.

If there is a large number of Logical Device instances per Logical Device specifications, then the conversion process should be split into multiple executions.

10. Deploy the **custom.ear** file by running the following command:

```
java -cp MW_Home/wlserver/server/lib/weblogic.jar weblogic.Deployer -adminurl t3://
ServerName:Port -user UserName -password Password -deploy Domain_Home/UIM/app/
uimVersion/custom.ear -targets ServerName -name custom -plan Domain_Home/UIM/app/
plan/Plan.xml
```

where:

- *MW_Home* is the directory in which the Oracle Fusion Middleware 12c products are installed.
- *Domain_Home* is the directory containing the configuration for the domain into which UIM is installed.
- *ServerName* is the name of the Administration Server machine.
- *Port* is the Administration Server port number.
- *UserName* is the user name with which you connect to the Administration server.
- *Password* is the password for the Administration server.
- *name* is the name of the file. This value defaults to the base name of the deployment file or directory.
- *targets* is the administration server name or cluster server name.
- *uimVersion* is the directory of the UIM release version.

11. If you are upgrading from UIM 7.3.0, define the UIM data source for MapViewer 12c if you installed MapViewer in step 16. See "Defining the Map Data Source" for more information.

12. UIM replaces the **system-config.properties** file during the upgrade process. If you do not back up the changes you made in the **system-config.properties** file, you will lose them; however, you must re-apply those changes after upgrading UIM.

About Rolling Back UIM

If the installer fails to successfully upgrade UIM, you must manually restore the WebLogic Server domain, the database schema, and the database domain. See the chapter, “Unified

Inventory Management Backup and Restore" in *UIM System Administrator's Guide* for more information about restoring the database. See the WebLogic Server documentation for more information about restoring the WebLogic Server domain.

10

Setting Up Unified Inventory Management for Single Sign-On Authentication

This chapter provides instructions for setting up Oracle Communications Unified Inventory Management (UIM) for single sign-on (SSO) authentication.

UIM implements the single sign-on (SSO) authentication solution using Oracle Access Manager, which enables you to seamlessly access multiple applications without being prompted to authenticate for each application separately. The main advantage of SSO is that you are authenticated only once, which is when you log in to the first application; you are not required to authenticate again when you subsequently access different applications with the same (or lower) authentication level (as the first application) within the same web browser session.

UIM also supports the single logout (SLO) feature. If you access multiple applications using SSO within the same web browser session, and then if you log out of any one of the applications, you are logged out of all the applications.

This solution supports SSO authentication between UIM and Network Integrity applications.

For more information, see *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

Installing Required Software

Install and configure the following software that UIM requires for implementing SSO authentication:

- External Lightweight Directory Access Protocol (LDAP) Server. Oracle recommends Oracle Internet Directory (OID) or Oracle Unified Directory (OUD) as the LDAP store external to the WebLogic Server.
- The following software can be optional if you use an Identity Provider other than OAM:
  - Oracle Access Manager (OAM), included with Oracle Identity and Access Management 12c (12.2.1.4.0)
  - Oracle WebLogic Server 12c (12.2.1.4.0)
  - Oracle HTTP Server (OHS) 12c (12.2.1.4.0)
  - Oracle HTTP Server 12c WebGate for OAM

> **Note:**
>
> - See "Configuring KeyCloak as Identity Provider for UIM, UTIA, and Message Bus" for information on using KeyCloak as an Identity Provider.
> - You can use any Identity Provider that supports SAML 2.0 protocol and OIDC or OAuth2.0 protocols.

Install the following required software only if you use OAM or OHS for traditional UIM. If you want to use OAM as a service, see **Common Authentication** chapter in *Unified Inventory and Topology Deployment Guide*.

> **Note:**
>
> You can skip installing the following software if your Identity Provider supports SAML2.0.

To install the required software, do the following:

1. Install Oracle WebLogic Server 12c and create the Oracle Middleware Home directory (*MW_Home*). This is the directory in which the Oracle Fusion Middleware products are installed.

   For more information, see *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server 12c*.

2. Install Oracle Access Manager (OAM) in the same Oracle Middleware Home directory that you created when you installed Oracle WebLogic Server 12c.

   For more information, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

3. Install and configure Oracle HTTP Server, which is a Web server that acts as the front end to the Oracle WebLogic Server.

   For more information, *Oracle Fusion Middleware Installing and Configuring Oracle HTTP Server*.

4. Install and configure Oracle HTTP Server WebGate for OAM.

   A WebGate is a web-server plug-in for Oracle Access Manager (OAM) that intercepts HTTP requests and forwards them to the Access Server for authentication and authorization. For more information, see *Oracle Fusion Middleware Installing WebGates for Oracle Access Manager.*

5. Install an external LDAP server. For example, Oracle Internet Directory (OID). Oracle recommends Oracle Internet Directory as an external LDAP store.

   For information on installing and configuring Oracle Internet Directory, see *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

6. Configure the external LDAP as the user identity store in OAM.

   For more information, see *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

7. Register the Oracle HTTP Server WebGate instance with OAM by using the Oracle Access Manager Administration Console.

   For more information, see the chapter on “Registering Partners (Agents and Applications) by Using the Console" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

8. Continue with the steps in "Configuring UIM to Enable SSO Authentication".

> **Note:**
>
> OAM, OHS, and WebGate are optional when you use UIM with UTIA, and if you use any other identity provider.

Configuring UIM to Enable SSO Authentication

Configuring UIM to enable SSO authentication involves the following tasks:

- Prerequisites
- Installing and Deploying UIM Specifying the External LDAP Provider
- Configuring the Frontend URL in Administration Console
- Creating and Configuring Providers for OAM SSO
- Configuring web.xml for the OAM Identity Asserter
- Configuring the mod_wl_ohs Plug-In for Oracle HTTP Server
- Protecting Resources For SSO Authentication
- Excluding Resources From SSO Authentication

Prerequisites

Before configuring UIM for SSO, ensure that the server on which UIM is installed can connect to the server on which OID is installed.

To enable the UIM server to connect to the OID server, edit the UIM server's **hosts** file and add the host name and IP address of the OID server. On Windows, the **hosts** file is typically located at **C:\Windows\System32\drivers\etc**. On Unix and Solaris, the **hosts** file is located at **/etc/hosts**.

Installing and Deploying UIM Specifying the External LDAP Provider

Install and deploy UIM specifying the external LDAP provider. When installing UIM, in the Security Provider Selection screen, select the **External_LDAP** option, and then enter the required information in the External Security Provider Connection Information screen. Follow the instructions provided in "Installing UIM by Using Interactive Install".

Configuring the Frontend URL in Administration Console

Set the front-end host and port so that all requests to access the applications (UIM/Network Integrity) deployed in the WebLogic administration server go through the Oracle HTTP server:

To configure the Frontend URL:

1. Log in to the WebLogic Server Administration Console.
2. In the **Domain Structure** tree, expand **Environment**, and click **Servers**.

   The Summary of Servers screen appears.
3. Click **AdminServer**.

   The Setting for AdminServer screen appears.

4. Click the **Protocols** tab.
5. Open the **HTTP** tab.
6. In the **Frontend Host** field, enter the name of the Oracle HTTP Server host machine.

   WebLogic Server uses this value instead of the one in the host header. All HTTP URLs are redirected to this HTTP host.
7. In the **Frontend HTTP Port** field, enter the Oracle HTTP Server port number.

   All HTTP URLs are redirected to this HTTP port.
8. Click **Save**.
9. In the Change Center of the Administration Console, click **Activate Changes**, which activates these changes.

To configure the Frontend URL in a cluster environment:

1. Open the domain, the corresponding environment, and then clusters.
2. Click **clusterName** and navigate to the **HTTP** tab.
3. Update the following:
   - Hostname, http port, and https port.
   - Frontend Host: ohs server hostname. If you use OAM as a service, the format is `<INSTANCE_NAME>.<PROJECT_NAME>.ohs.<hostSuffix>`
   - Frontend HTTP Port: The Traefik non-ssl port.
   - Frontend HTTPS Port: The Traefik ssl port.

Creating and Configuring Providers for OAM SSO

You must create a new OAMIdentityAsserter provider for OAM SSO in WebLogic Server Administration Console.

To create the OAMIdentityAsserter provider:

1. Log in to the WebLogic Server Administration Console.
2. Under Your Application's Security Settings, click **Security Realms**.

   The Summary of Security Realms screen appears.
3. Select the realm *YourRealmName*, for which you need to configure the OAM identity asserter.

   The Settings For *YourRealmName* screen appears.
4. Click the **Providers** tab, and then click the **Authentication** tab.
5. Click **New**.

   The Create a New Authentication Provider screen appears.
6. In the **Name** field, enter a name for the new provider; for example, **OAM ID Asserter**.
7. From the **Type** list, select **OAMIdentityAsserter**.
8. Click **OK**.

   The Settings For *YourRealmName* screen appears, showing the newly created authentication name in the **Authentication** tab.
9. Click the link for *AuthenticatorName* (For example, OAM ID Asserter).

The Settings for *AuthenticatorName* screen appears.

10. On the **Common** tab, from the **Control Flag** list, select **REQUIRED**.
11. Under **Active Types**, use the directional arrow buttons to move **OAM_REMOTE_USER** from the **Available** column to the **Chosen** column.
12. (Optional) If you use Oracle Internet Directory as the external LDAP store, ensure that you move **OAM_IDENTITY_ASSERTION** to the **Chosen** column.
13. Click **Save**.
14. Click the **Provider Specific** tab, beside the **Common** tab.
15. Update the following details:
    - Identity Domain: UnifiedIdDomain
    - Access Gate Name: `<INSTANCE_NAME>.<PROJECT_NAME>.ohs.<OHS-hostSuffix>` if OAM is used as a service.
    - Primary Access Server: `<INSTANCE_NAME>.<PROJECT_NAME>.ohs.<OHS-hostSuffix>:<TRAEFIKPORT>` if OAM is used as a service.
16. Click **Save**.
17. Click the **Providers** tab, and then click the **Authentication** tab.
18. Click the link for DefaultAuthenticator and ensure that the default authenticator's control flag is set to **SUFFICIENT**.
19. Click the link for OID/OUD Authenticator (for example, OracleInternetDirectoryAuthenticator) and ensure that the OID/OUD authenticator's control flag is set to **SUFFICIENT**.

    See "Installing and Configuring an Authentication Provider" for more information.
20. On the **Authentication** tab, click **Reorder**.

    The Reorder Authentication Providers screen appears
21. Use the Up and Down arrows to reorder the listed Authentication Providers as follows:
    - OAMIdentityAsserter (REQUIRED)
    - OracleInternetDirectoryAuthenticator (SUFFICIENT)
    - DefaultAuthenticator (SUFFICIENT)
22. Click **OK**.

Configuring web.xml for the OAM Identity Asserter

You configure the **web.xml** file for the OAM Identity Asserter by updating the deployment plan. You use deployment plans to change an application's WebLogic Server configuration for a specific environment without modifying existing deployment descriptors.

To configure the **web.xml** file:

1. For using Oracle Access Manager Identity Asserter, you must specify the authentication method as CLIENT-CERT in the **web.xml** file for the appropriate realm by editing the deployment plan. The **web.xml** file is located at *UIM_Home***/app/inventory.ear/inv.war/WEB-INF/**, where *UIM_Home* is the directory in which the UIM software is installed.
    - Depending on your deployment configuration, do one of the following:
        - If UIM is installed in a single server environment, navigate to and open the *UIM_Home***/app/plan/Plan.xml** file.

  - If UIM is installed in a clustered server environment, navigate to and open the *UIM_Home*/**app/plan/ClusterPlan.xml** file.

- Update the variable-definition and variable-assignment elements; specifically, add CLIENT-CERT as follows:

```
<variable-definition>
 <variable>
     <name>ClientCertAuthMethod</name>
     <value>CLIENT-CERT</value>
 </variable>
 <variable>
     <name>RealmName</name>
     <value>myrealm</value>
 </variable>
</variable-definition>
<module-override>
    <module-name>inv.war</module-name>
    <module-type>war</module-type> <module-descriptor external="false">
      <root-element>web-app</root-element>
      <uri>WEB-INF/web.xml</uri>
 <variable-assignment>
     <name>ClientCertAuthMethod</name>
     <xpath>/web-app/login-config/auth-method</xpath>
     <operation>replace</operation>
 </variable-assignment>
 <variable-assignment>
     <name>RealmName</name>
     <xpath>/web-app/login-config/realm-name</xpath>
     <operation>add</operation>
  </variable-assignment>
    </module-descriptor>
</module-override>
```

- Save and close the **Plan.xml/ClusterPlan.xml** file.

2. Update the deployment plan for the currently-deployed UIM application:
   a. Log in to the WebLogic Server Administration Console.
   b. In the **Domain Structure** tree, expand **Environment**, and click **Deployments**.

      The Summary of Deployments screen appears.
   c. Select the check box for oracle.communications.inventory.
   d. Click **Update**.

      The Update Application Assistant page appears.
   e. Select **Update this application in place with new deployment plan changes** and click **Next**.
   f. (Optional) Click **Change Path** beside the **Deployment Plan Path** filed and browse to the location of the **Plan.xml/ClusterPlan.xml** file.

      The Summary page appears.
   g. Click **Finish**.
   h. In the Change Center of the Administration Console, click **Activate Changes**, which activates these changes.

Configuring the mod_wl_ohs Plug-In for Oracle HTTP Server

You must configure the mod_wl_ohs plug-in and edit the mod_wl_ohs.conf file to enable the Oracle HTTP Server instances to forward requests to the applications deployed on the Oracle WebLogic Server or clusters.

For more information, see *Oracle Fusion Middleware Using Web Server Plug-Ins with Oracle WebLogic Server*.

Configuring the mod_wl_ohs plug-in involves the following tasks:

- Configuring the WebLogic Proxy Plug-In
- Editing the mod_wl_ohs.conf File

Configuring the WebLogic Proxy Plug-In

To configure the WebLogic Proxy Plug-in:

1. Log in to the Oracle WebLogic Server administration console.
2. In the **Domain Structure** tree, expand **Environment**, and do one of the following:
   - Select **Clusters** (if the server instances to which you want to proxy requests from Oracle HTTP Server are in a cluster)
   - Select **Servers**.

     The Summary of Servers page appears.
3. Select the server or cluster to which you want to proxy requests from Oracle HTTP Server.
4. Click the **Configuration** tab.
5. On the **General** tab, in the Advanced section, select the **WebLogic Plug-In Enabled** checkbox.
6. If you selected Servers in step 2, repeat steps 3 and 4 for the other servers to which you want to proxy requests from Oracle HTTP Servers.
7. Click **Save**.
8. Restart the WebLogic Server.

Editing the mod_wl_ohs.conf File

> **Note:**
>
> You can skip this procedure if you use OAM as a service. See **Common Authentication** in *Unified Inventory and Topology Deployment Guide* for more information.

To edit the **mod_wl_ohs.conf** file:

1. Open the **mod_wl_ohs.conf** file from the following location:

   *Domain_Home***/config/fmwconfig/components/OHS/ohs1/**

   where:

Domain_Home is the directory containing the configuration for the domain into which UIM is installed.

2. Add directives within the <IfModule weblogic_module> element in the configuration file as follows:

   - To forward requests to the UIM application running on a single Oracle WebLogic Server instance, specify **/Inventory** within the <location> element as follows:

     ```
     <IfModule weblogic_module>
     <Location /Inventory>
     SetHandler weblogic-handler
     WebLogicHost host
     WebLogicPort port
     </Location>
     </IfModule>
     ```

     where:

     – *host* is the name of the WebLogic Administration server machine

     – *port* is the port of the server on which UIM is installed

   - To forward requests to the UIM application running on a cluster of Oracle WebLogic Server instances, specify **/Inventory** within a new <location> element as follows:

     ```
     <IfModule weblogic_module>
     <Location /Inventory>
     SetHandler weblogic-handler
     WebLogicCluster host1:port1,host2:port2
     </Location>
     </IfModule>
     ```

     where:

     – *host1* and *host 2* are host names of the managed servers

     – *port1* and *port2* are ports of the managed servers

   - To forward requests to the UIM Web services running on a single Oracle WebLogic Server instance, specify **/InventoryWS** within the <location> element as follows:

     ```
     <IfModule weblogic_module>
     <Location /InventoryWS>
     SetHandler weblogic-handler
     WebLogicHost host
     WebLogicPort port
     </Location>
     </IfModule>
     ```

     where:

     – *host* is the name of the WebLogic Administration server machine

     – *port* is the port of the server on which UIM is installed

   - To forward requests to the UIM Web services running on a cluster of Oracle WebLogic Server instances, specify **/InventoryWS** within a new <location> element as follows:

     ```
     <IfModule weblogic_module>
     <Location /InventoryWS>
     SetHandler weblogic-handler
     WebLogicCluster host1:port1,host2:port2
     </Location>
     </IfModule>
     ```

where:

- *host1* and *host 2* are host names of the managed servers
- *port1* and *port2* are ports of the managed servers

- To forward requests to the UIM application running on a single Oracle WebLogic Server instance into which you want to deploy cartridges, specify **/cartridge** within the <location> element as follows:

```
<IfModule weblogic_module>
<Location /cartridge>
SetHandler weblogic-handler
WebLogicHost host
WebLogicPort port
</Location>
</IfModule>
```

where:

- *host* is the name of the WebLogic Administration server machine
- *port* is the port of the server on which UIM is installed

- To forward requests to the UIM application running on a cluster of Oracle WebLogic Server instances into which you want to deploy cartridges, specify **/cartridge** within a new <location> element as follows:

```
<IfModule weblogic_module>
<Location /cartridge>
SetHandler weblogic-handler
WebLogicHost host
WebLogicPort ms_port
</Location>
</IfModule>
```

where:

- *host* is the machine where the managed server is running
- *ms_port* is the port of the managed server running on the host specified in the *host* variable above

For example, if a managed server **uim_ms1** with listen port **8065** is running on the machine **UIM1**, you must specify the following:

```
<IfModule weblogic_module>
<Location /cartridge>
SetHandler weblogic-handler
WebLogicHost UIM1
WebLogicPort 8065
</Location>
</IfModule>
```

Protecting Resources For SSO Authentication

You must protect resources (for example, the UIM application) in Oracle Access Manager for SSO authentication. For more information, see *Fusion Middleware Administrator's Guide for Oracle Access Management*.

To protect resources for SSO authentication:

1. Open the Oracle Access Management Console.
2. On the **Policy Configuration** tab, expand the **Application Domains** node.

3. Expand the node for the application domain.
4. Within the application domain, expand the **Resources** node.
5. Click the **Resources** tab, and then click the **New Resource** button in the upper-right corner of the Search page.

   The Resource Definition page appears.
6. Do the following to configure the UIM application as a protected resource for SSO authentication:
   - From the **Type** list, select **HTTP**.
   - In the **Resource URL** field, enter **/Inventory/***.
   - From the **Protection Level** list, select **Protected**.
7. Click **Apply**.

Excluding Resources From SSO Authentication

You can exclude HTTP resources that do not require SSO authentication. For example, when accessing a Web Services Description Language (WSDL) document for Web services. The excluded resources are public and do not require an OAM Server check for authentication.

When allowing access to excluded resources, WebGate does not contact the OAM Server. Excluded resources cannot be added to any user-defined policy in the console. For more information, see *Fusion Middleware Administrator's Guide for Oracle Access Management*.

To exclude resources from SSO authentication:

1. Open the Oracle Access Management Console.
2. On the **Policy Configuration** tab, expand the **Application Domains** node.
3. Expand the node for the application domain.
4. Within the application domain, expand the **Resources** node.
5. Click the **Resources** tab, and then click the **New Resource** button in the upper-right corner of the Search page.

   The Resource Definition page appears.
6. Do the following to exclude UIM Web services from SSO authentication:
   - From the **Type** list, select **HTTP**.
   - In the **Resource URL** field, enter **/InventoryWS/.../***.
   - From the **Protection Level** list, select **Excluded**.
7. Click **Apply**.
8. Click the **New Resource** button in the upper-right corner of the Search page.

   The Resource Definition page appears.
9. Do the following to exclude the UIM cartridge deployment process from SSO authentication:
   - From the **Type** list, select **HTTP**.
   - In the **Resource URL** field, enter **/cartridge/.../***.
   - From the **Protection Level** list, select **Excluded**.
10. Click **Apply**.

Configuring SSO using SAML 2.0 Protocol from IDCS Identity Provider

You can use SAML 2.0 for enabling SSO in UIM. SSO allows you to log into applications using a single username and password combination.

For security concepts and definitions, see the **Security Assertion Markup Language (SAML)** section in *Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server*.

Configuring SAML for SSO

To configure SAML for SSO:

1. Create SAML Assertion Provider and SAML Authenticator.
2. Enter **General Information**.
3. Configure SAML Service Provider.
4. Publish the Service Provider metadata.
5. Register IdP in WebLogic.
6. Update the **Deployment Plan** of UIM.
7. Verify the SAML configuration.

Creating SAML Assertion Provider and SAML Authenticator

1. Access the WebLogic Server Console as administrator.
2. Click **Lock & Edit**.
3. Select **Security Realm**.
4. Select **myrealm**.
5. Select **Providers**, and then click **New**.
6. Enter **SAML2IdentityAsserter** as **Name**, select **SAML2IdentityAsserter** as **Type**, and then click **OK**.
   The **SAML2IdentityAsserter** is displayed under the **Authentication Providers** table.
7. On the **Providers** page, click **New**.
8. Enter **SAMLAuthenticator** as **Name**, select **SAMLAuthenticator** as **Type**, and then click **OK**.
   The **SAMLAuthenticator** is displayed under the **Authentication Providers** table.
9. Click **Reorder**.
10. Select and reorder the providers in the following order:
    a. SAML2IdentityAsserter
    b. SAMLAuthenticator
    c. DefaultAuthenticator
    d. DefaultIdentityAsserter
11. Click **OK**.
12. Click **SAMLAuthenticator**.

13. Select **SUFFICIENT** as **Control Flag** and then click **Save**.
14. Return to the Providers page.
15. Click **DefaultAuthenticator**.
16. Select **SUFFICIENT** as **Control Flag** and then click **Save**.
17. Click **Activate Changes**.
18. Restart the server.

Specifying General Information

To specifiy General Information:

1. Access the WebLogic Server Console as administrator.
2. Click **Lock & Edit**.
3. Click **Environment** and then select **Servers**.
4. Click the manager server (AdminServer) that has the Inventory application (for example, **ms1**).
   - In a clustered environment, the later steps must be performed on each managed server that has the Inventory application. (other than **proxy** and **admin server**)
5. Click **Federation Services** and then select **SAML 2.0 General**.
6. Define the site information and additional settings for the SAML assertion.
7. Generate the service provider metadata file.
8. Modify the **General** settings as showin the the table by replacing the information according to your requirement and the server.
9. Click **Save**.

Table 10-1 Attribute and Values

Attribute	Sample Value
Published Site URL	`http://<InventoryHostName>:<InventoryPort>/saml2`
Entity ID	`samlUIM` **Note**: You can enter any identification value, as long it is unique in Identity Cloud Service and in your WebLogic Domain.
Recipient Check Enabled	`Deselected`
Replicated Cache Enabled	`Deselected` (for single instance or non-clustered) `Selected` (for clustered environment)

Configuring the SAML Service Provider

To configure the SAML service provider:

1. Access the WebLogic Server Console as administrator.
2. Click **Lock & Edit**.

3. Click **Environment** and then select **Servers**.
4. Click the manager server (AdminServer) that has the Inventory application (for example, **ms1**).
   - In clustered environment, the later steps must be performed on each managed server that has the Inventory application (other than **proxy** and **admin server**).
5. Select **Configuration**, then **Federation Services** and then **SAML 2.0 Service Provider**.
6. Select **Enabled**.
7. Select **Single Logout Enabled**.
8. Select **Assertion Subject Timeout Check**.
9. Select **POST** as **Preferred Binding**.
10. (Optional) Provide the list of **Allowed redirect URIs** to be used by Service Provider for after logout redirections.
11. Select **POST** as **Preferred Binding**.
12. Enter *https://<InventoryHost>:<InventoryPort>/Inventory/* as **Default URL**, and then click **Save**.
13. Click **Activate Changes**.

Publishing the Service Provider Metadata

To publish the service provider metadata:

1. Access the WebLogic Server Console as administrator.
2. Click **Lock & Edit**.
3. Click **Environment** and then select **Servers**.
4. Click the manager server (AdminServer) that has the Inventory application (for example, **ms1**).
   - In a clustered environment, the later steps must be performed on each managed server that has the Inventory application. (other than **proxy** and **admin server**)
5. Select **Configuration**, **Federation Services**, and then **SAML 2.0 General**.
6. Click **Publish Meta Data**.
   The Publish SAML 2.0 Meta Data page appears.
7. In the **Path** field, enter the full path and filename of the metadata file. For example, **C:\mydomain\myserver\sppmeta.xml**.
8. Click **OK**.

Registering Identity Provider in WebLogic

To register a SAML Identity Provider in WebLogic:

1. Upload the **IdPMetadata.xml** file from the Identity Provider to the server hosting WebLogic (for example, **/path/to/metadata/file/IDCSMetadata.xml**).
2. Open the WebLogic Administration Server Console as administrator.
3. Click **Security Realm** and then select **myrealm**.
4. Click **Providers**, and then select **SAML2IdentityAsserter**.

5. Click **Management**, click **New**, and then select **New Web Single Sign-On Identity Provider Partner**.
   The Create a Web Single Sign-On Identity Provider Partner page appears.

> **Note:**
>
> This is required for enabling Identity Provider users with UIM group to access the UIM UI. See Configuring the SAML Authentication Provider for more information.

6. In the **Name** field, enter **WebSSO-IdP-Partner-1**.
7. In the **Path** field, enter the path to the XML file that contains the Identity Provider metadata.
8. Click **OK**.
9. Click the **WebSSO-IdP-Partner-1** link.
10. Ensure that the Identity Provider details appear in the **Site Info** and **Single Sign-On Signing Certificate** tabs.
11. In the **General** tab, select **Enabled**, **Virtual User**, and **Process Attributes** check boxes.
12. In the **Redirect URIs** field, enter **/Inventory/***.
13. Click **Save**.
    The WebLogic server displays a confirmation message.
14. Sign out of the WebLogic server and close your browser.

Updating the Deployment Plan of Unified Inventory Management

Update the Plan.xml (Standalone) file or ClusterPlan.xml (Cluster) file depending on your environment, for the authentication to happen. These changes are applicable for a traditional UIM installation.

To update the deployment plan of UIM:

1. Within **<variable-definition>**, override the value of the existing **logoutURL** variable with the Identity Provider logout URL.
   Replace **/oracle/communications/platform/logout.jspx** with the Identity Provider logout URL. For example, **https://*<WL_SP_hostname>*:*<WL_SP_port>*/saml2/sp/slo/init**.

```
<variable>
    <name>logoutURL</name>
    <value>IDP_LOGOUT_URL</value>
</variable>
```

2. Update the **<module-override>** section of **inv.war** module name as follows:

```
<module-override>
    <module-name>inv.war</module-name>
    <module-type>war</module-type>
    <module-descriptor external="false">
        <root-element>weblogic-web-app</root-element>
        <uri>WEB-INF/weblogic.xml</uri>
        <variable-assignment>
            <name>cookie-path</name>
```

```
            <xpath>/weblogic-web-app/session-descriptor/cookie-path</xpath>
            <operation>remove</operation>
        </variable-assignment>
    </module-descriptor>
    <module-descriptor external="false">
        <root-element>web-app</root-element>
        <uri>WEB-INF/web.xml</uri>
        <variable-assignment>
            <name>logoutURL</name>
            <xpath>/web-app/context-param[param-name="loginURL"]/param-
value</xpath>
            <operation>replace</operation>
        </variable-assignment>
     <variable-assignment>
            <name>endURL</name>
            <xpath>/web-app/context-param[param-name="endUrl"]/param-
value</xpath>
            <operation>replace</operation>
        </variable-assignment>
    </module-descriptor>
</module-override>
```

Verifying SAML Configuration

To verify the SAML configuration:

1. Enter the URL **http://<InventoryHostname>:<InventoryPort>/Inventory** to open the Inventory login page.
   The login page of the Identity Provider appears.
2. Enter the login credentials.
   The UIM home page appears.
3. After you log in, you can logout using the **Logout** option from the top right corner of the page.
   The login page of Identity Provider appears or a successful logout message appears, based on the configurations entered in Identity Provider.
4. Close the browser or tab.

To register UIM in Identity Provider:

1. Use **Entity ID** (for example, **samlUIM**).

> **Note:**
>
> This value must be same as the value provided in "Configuring the SAML Service Provider" under the **SAML 2.0 General** section within the **Federation Services** section.

2. Enter **Assertion consumer URL** as **http://<InventoryHostname>:<InventoryPort>/saml2/sp/acs/post**

Registering UIM in IDCS Identity Provider

You can register UIM in Oracle Identity Cloud Service (IDCS) Identity Provider as a SAML application.

> **Note:**
>
> - Instructions mentioned in this section are with reference to Identity Cloud Services (IDCS). In case you use a different Identity Provider, ensure that you follow the corresponding instructions of the Identity Provider while registering UIM.
> - Ensure SAML response contains the **groups** information as **SAML 2.0 attributeStatement**.
> - According to WebLogic document: https://docs.oracle.com/en/middleware/fusion-middleware/weblogic-server/12.2.1.4/scprg/saml.html#GUID-448300EA-75C0-453C-8131-B9DDC9DE7F3D, the attributes shared through SAML response must be in **basic** format for them to be considered.

To register a service provider (SP) with any Identity Provider, you can perform a manual configuration or import the SP Metadata (xml) file to the Identity Provider.

To import SP metadata files for creating SAML clients, use any Identity Provider other than IDCS. If you are using any other Identity Provider, and if it supports configuration using a service provider metadata file (for example: KeyCloak), you can publish the metadata file of UIM and use it to create a SAML client.

Manually Configuring UIM Details in IDCS Identity Provider

To manually configure UIM in IDCS Identity Provider:

1. Access the IDCS console and log in as administrator.
2. Navigate to the **Domains** and select the domain (*Default domain*) to add UIM as a SAML application.
3. Click **Add Application** button to register UIM as a SAML application.
   a. Select **SAML Application** and click **Launch app catalog**.
   b. Enter **UIM Inventory Application** as **Name** and **UIM Inventory Application as SAML application** as **Description**.
   c. Click **Next**.
   d. Enter **Entity ID**, for example: *samlUIM*. This should be same as the value provided in "Configuring the SAML Service Provider" under the **SAML 2.0 General** section under **Federation Services**.
   e. Enter **http://InventoryHostname:InventoryPort/saml2/sp/acs/post** as **Assertion consumer URL**.
   f. Select **Unspecified** as **Name ID format**.
   g. Select **Username** as **Name ID value**.

h. Upload the SSL Certificate of UIM. This is required for SLO to work.

i. Enter **https://<WL_SP_hostname>:<WL_SP_port>/saml2/sp/slo** as **Single logout URL**.

j. Enter **https://<WL_SP_hostname>:<WL_SP_port>/saml2/sp/slo** as **Logout response URL**.

k. Click **+ Additional attribute** at the bottom-right corner of the page.

   i. Enter **Groups** as **Name**.

   ii. Select **User attribute** as **Type**.

   iii. Select **Group membership** as **Type value**.

   iv. Select **All groups** as **Condition**.

l. Click **Finish**.

4. Click **Activate** buttonfor the create application (UIM Inventory Application)
5. Click **Activate application** button in the pop-up window.
6. Click **Download identity provider metadata** button for downloading the IdP's metadata xml. (for example, IDCSMetadata.xml)
7. Click **Users** on the left side pane to assign users. (Ensure desired users are added to your domain prior to this step)

   a. Click **Assign groups** for adding domain groups to the registered application.

   b. Choose the desired users from the pop-up window and click **Assign**.

8. Click **Groups** on the left-side pane to assign groups.

> **Note:**
>
> Ensure **uim-users** group is created or added to your domain before performing this step.

   a. Click **Assign users** for adding the domain users to the registered application.

   b. Choose **uim-users** from the pop-up window and click **Assign**.

Creating SAML2.0 Client in Identity Provider by Importing UIM Metadata (xml)

If your Identity Provider provides you an option to create SAML 2.0 client by importing the metadata file, you can use the published metadata file of UIM to create SAML2.0 client.

> **Note:**
>
> You can create SAML2.0 client in an identity provider other than IDCS.

For traditional UIM, to publish the metadata file, verify the step on "Publishing the Service Provider Metadata".

For UIM cloud native, to publish metadata file, see **Publishing UIM CN (service provider) Metadata file** section in *UIM Cloud Native Deployment Guide*.

Configuring WebLogic for Using Identity Provider for Authorization

You configure WebLogic to access the Identity Provider users in the Oracle Enterprise Manager (EM) console for authorization (in UIM).

For WebLogic server to authenticate users with the Identity Provider, the Identity Provider must be associated with an OAuth client that is registered with the Identity Provider. The OAuth client allows the provider access to the Identity Provider.

For authorization, the roles or groups information must be shared as **basic** format attributes in the SAML assertion response. For more information, see SAML 2.0 Basic Attribute Profile Required.

Updating the SSL.hostnameVerifier Property

The IDCS provider can access IDCS only if you update the **SSL.hostnameVerifier** property.

To update the **SSL.hostnameVerifier** property:

1. Go to the WebLogic administrator console and open **Environment**, **Servers**, your server (**AdminServer**), **Configuration** and then **SSL**.
2. Click **Lock & Edit**.
3. Open **Advanced**.
4. Change **Hostname Verification** from **BEA Hostname Verifier** to **Custom Hostname Verifier**.
5. Set **Custom Hostname Verifier** to **weblogic.security.utils.SSLWLSWildcardHostnameVerifier**.
6. Click **Save** and then **Activate Changes**.
7. Start the Administration server and all Managed WebLogic servers.

Configuring Oracle Identity Cloud Integrator Provider

The Oracle Identity Cloud Integrator provider is an authentication and identity assertion provider that accesses users, groups, and Identity Provider scopes, and application roles stored in the IDCS Identity Provider.

Before you can configure the provider, you must obtain the required OAuth client information from IDCS Identity Provider. To do so, you create a trusted application in the Identity Provider. A trusted application in the Identity Provider is a type of custom application that can be accessed by multiple users and hosted in a secure and protected place (server) where the trusted application uses OAuth 2.0. Because you know where the application is hosted, you can treat that application as trusted. Creating the application in Identity Provider results in the provisioning of an OAuth client.

Creating the OAuth Client

To create OAuth client in the Identity Cloud Service console:

> **Note:**
>
> Perform similar steps for any Identity Provider.

1. Log into the Identity Cloud Service console as an administrator.
2. Create a trusted application. See Adding a Trusted Application in Administering Oracle Identity Cloud Service.

> **Note:**
>
> The OAuth client can be used only within the specific tenant in which it was provisioned.

In the **Add Trusted Application** window:

1. Enter a client name and a description (optional).
2. Select **Configure this application as a client now** to configure the authorization settings:
   a. Select only **Client Credentials** as the allowed grant type.
   This setting is used when the authorization scope is limited to the protected resources under the control of the client or to the protected resources registered with the authorization server. The client presents the corresponding credentials to obtain an access token.
   b. Assign the client to the Identity Domain Administrator application role. To do so, select **Grant the client access to Identity Cloud Service Admin APIs** and then, in the pop-up window that appears, select **Identity Domain Administrator**.

> **Note:**
>
> Using the Identity Domain Administrator application role provides write access to the Oracle Identity Cloud Service user store. The WebLogic Server Oracle Identity Cloud Integrator provider does not support any update operations. Therefore, you must use the Identity Cloud Service Administration Console to modify the content of the user store.

3. Go through the remaining pages in the wizard and click **Finish**.
4. Note down the Client ID and Client Secret that appear when you create the application. You need these values when you configure the Oracle Identity Cloud Integrator provider. The attributes that you must provide while configuring the provider are:
   - Tenant: Name of the primary tenant in the Identity Provider where you provisioned the OAuth client.
   - ClientId: The OAuth client ID used to access the Identity Provider identity store.
   - ClientSecret: The OAuth Client Secret (password) used to generate access tokens.
   - Client tenant (Optional): Name of the OAuth client tenant in which the Client ID is available. This attribute is not required if the Client tenant is same as the primary tenant.
5. Activate the application.

Configuring Identity Cloud Integrator Provider

To configure Identity Cloud Integrator Provider:

1. Log into the WebLogic Server Administration console.
2. Select **Security Realm** in the **Domain Structure** pane.
3. On the Summary of Security Realms page, select the name of the realm (for example, **myrealm**) and click **myrealm**.
   The **Settings for myrealm** page appears.
4. On the **Settings for Realm Name** page, select **Providers** and then **Authentication**.
5. To create a new Authentication Provider in the **Authentication Providers** table, click **New**.
6. In the **Create a New Authentication Provider** page, enter the name of the authentication provider. For example, **IDCSIntegrator**.
7. Select the **OracleIdentityCloudIntegrator** type of the authentication provider from the drop-down list and click **OK**.
8. In the **Authentication Providers** table, click the newly created Oracle Identity Cloud Integrator **IDCSIntegrator** link.
9. In the **Settings for IDCSIntegrator** page, select **Sufficient** from the drop-down list for **Control Flag** and click **Save**.
10. Go to the **Provider Specific** page to configure the additional attributes for the security provider.
11. Enter the values for the following fields and click **Save**:
    - Host
    - Port 443(default)
    - select SSLEnabled
    - Tenant
    - Client Id
    - Client Secret.

    > **Note:**
    >
    > If the IDCS URL is **idcs-abcde.identity.example.com**, then IDCS host is **identity.example.com** and tenant name is **idcs-abcde**. Keep the default settings for the other sections of the page.

12. Select **Security Realm**, **myrealm**, and then **Providers**.
13. In the **Authentication Providers** table, click **Reorder**.
14. In the **Reorder Authentication Providers** page, move **IDCSIntegrator** to the top and click **OK**.
15. In the **Authentication Providers** table, click the **DefaultAuthenticator** link.
16. In the **Settings for DefaultAuthenticator** page, select **Sufficient** from the drop-down list for **Control Flag** and click **Save**.
    All changes are activated.
17. Restart the Administration server.

Setting Up Trust between IDCS and WebLogic

To set up `trust` between IDCS and WebLogic:

1. Import the certificate in KSS store.
   a. Open the Administration Server node.
   b. Get the IDCS certificate as follows:

```
echo -n | openssl s_client -showcerts -servername <IDCS_URL> -connect
<IDCS_URL>:443|sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
> /tmp/idcs_cert_chain.crt

#sample echo -n | openssl s_client -showcerts -servername
xyz.identity.oraclecloud.com -connect idcs-
xyz.identity.oraclecloud.com:443|sed -ne '/-BEGIN CERTIFICATE-/,/-END
CERTIFICATE-/p' > /tmp/idcs_cert_chain.crt
```

   c. Import the certificate and run the **<ORACLE_HOME>/oracle_common/common/bin/wlst.sh** file.
   d. Run the following commands:

```
connect('weblogic','<admin_pwd>','t3://<WEBLOGIC_HOST>:7001')
svc=getOpssService(name='KeyStoreService')
svc.importKeyStoreCertificate(appStripe='system',name='trust',password='
',alias='idcs_cert_chain',type='TrustedCertificate',filepath='/tmp/
idcs_cert_chain.crt',keypassword='')
syncKeyStores(appStripe='system',keystoreFormat='KSS')
```

   e. Run `exit()`.
2. Restart the Administration server and Managed servers.

Creating an Administrator User in IDCS Administration Console for WebLogic

You must create an Administrator user in IDCS because once the Managed servers are configured for SAML, the domain administrator user (usually, the **weblogic** user) cannot log into the Managed servers.

> **Note:**
>
> You must perform this procedure only if you use IDCS as Identity Provider.

To create WebLogic Administrator user in IDCS for WebLogic JaxWS connection:

1. In IDCS, go to the **Groups** tab and create the **Administrators** and **sysmanager** roles.
2. Go to the **Users** tab and create a **wls admin** user, for example, **weblogic** and assign it to the **Administrators** and **sysmanager** groups.
3. Restart all Managed servers.

Managing Group Memberships, Roles, and Accounts

To manage group memberships, roles, and accounts, you must update **OPSS** and **libOVD** to access IDCS.

The following procedure is required only if you use IDCS for user authorization.

Ensure that all servers are stopped (including **Administration**) before proceeding further.

To manage group memberships, roles, and accounts:

1. Shutdown all servers that use WebLogic Server Administration Console.

   > **Note:**
   >
   > You must use – `kubectl` patch domain command for starting or stopping pods and not the WebLogic Server Administration Console.

2. Run the following:

   ```
   #Run the wlst.sh
   cd /u01/oracle/oracle_common/common/bin/
   ./wlst.sh
   ```

   > **Note:**
   >
   > This does not require a connection to the WebLogic Administration Server.

3. Read the domain as follows:

   ```
   readDomain(<DOMAIN_HOME>)
   ```

4. Add the template as follows:

   ```
   addTemplate(<MIDDLEWARE_HOME>/oracle_common/common/templates/wls/
   oracle.opss_scim_template.jar")
   ```

   > **Note:**
   >
   > This step may throw a warning, which can be ignored. The **addTemplate** is deprecated. Use **selectTemplate** followed by **loadTemplates** instead of **addTemplate**.

5. Update the domain as follows:

   ```
   updateDomain()
   ```

6. Close the domain as follows:

   ```
   closeDomain()
   ```

7. Exit from the Administration server container using `exit()`.
8. Start the Administration and Managed servers.

11

Installing UIM Patches

This chapter describes how to install patches on Oracle Communications Unified Inventory Management (UIM).

See the patch ReadMe file, included in the patch download, for information about the contents of a patch.

About Patching UIM

UIM patches are posted on the My Oracle Support website:

https://support.oracle.com

Most UIM patches are installed using the Oracle Universal Installer. If the installer fails to install the patch, you must restore your database schema and domain, and your WebLogic Server domain.

The patch ReadMe file specifies whether to use the installer to install a patch or whether to follow other installation instructions.

> **Caution:**
>
> Always read the patch ReadMe file in its entirety before installing a patch.

UIM patches are released as cumulative patches. This means that if there is more than one patch, the last patch will contain the changes for the other patches. For example, patch #3 will contain the changes for patch #1 and patch #2.

Some patches contain fixes and functionality that may not be of any interest to you or may apply to features that you have not installed or purchased. Read the patch ReadMe file to determine if you must install the patch.

Some patches are password protected. To request the password to download a protected patch, open a Service Request on the My Oracle Support website.

> **Note:**
>
> If you have multiple UIM installations on the same machine, you need to specify the appropriate UIM home details for the current installation. Perform the following:
>
> 1. Open the installer log from the last successful installation of UIM (the latest release).
> 2. Look for the ORACLE_HOME and ORACLE_HOME_NAME entries in the installer log.
> 3. Select the value for ORACLE_HOME_NAME from the drop down menu as the name in the **Specify Home Details** installer screen.
> 4. Browse to the directory referred by ORACLE_HOME in the **Specify Home Details** installer screen.

Planning Your Patch Installation

Before installing a patch, verify your version of UIM and ensure the patch is not already installed.

Oracle recommends scheduling your patch installation during non-peak hours to minimize the disruption to your operations.

Ensure that UIM is not running any operations.

As a precaution against a failed patch installation, Oracle recommends that you back up your database schema for UIM, database domain for UIM, WebLogic Server domain for UIM, the *UIM_Home* directory, and the installer inventory directory. See *UIM System Administrator's Guide* for more information about backing up and restoring the database. See your WebLogic Server documentation for more information about backing up your WebLogic Server domain.

Oracle recommends installing a patch on a test system with a copy of your production data before installing the patch on your production system. Test the patch by logging into UIM and verifying the version number of installed components.

Installing a Patch

To install a patch on UIM:

1. Create a temporary directory (*temp_dir*).
2. Download the patch from the My Oracle Support website:

   `https://support.oracle.com`

   and save it to *temp_dir*.
3. Unzip the patch package and select a patch installer package based on your specific platform.

> **Note:**
>
> The package contains patch installer packages for the Linux, Solaris, and AIX platforms.

4. Extract the contents of the installer package to *temp_dir*.

   The extracted software pack has the following structure:

   PatchSet-UnifiedInventoryManagement-*release***-***version***/uim/Disk1/install/**

5. Run the following command:

   ```
   /dir/PatchSet-UnifiedInventoryManagement-release-version/Disk1/install/runInstaller
   ```

   The JRE Location command prompt appears.

6. Enter the path to the JRE location.

   The Oracle Universal Installer Welcome screen appears.

7. Click **Next**.

   The Specify Home Details screen appears.

8. Do the following:

   a. In the **Name** field, confirm the name of the folder that contains the installation files for UIM.

   b. In the **Path** field, confirm the directory where the folder specified in the **Name** field is located.

   c. Click **Next**.

   The installer scans the specified directory and folder and retrieves information about your UIM installation, such as connection details and user names.

   The WebLogic Administration Server Connection Information screen appears, displaying the current connection information.

9. Do the following:

   a. In the **Host Name** field, confirm the IP address or host name for the server that UIM was installed on.

   b. In the **Port Number** field, confirm the port used by UIM.

   c. If SSL is not being used, uncheck the **Use SSL?** box.

   d. In the **Password** field, enter the WebLogic Administration server password.

   e. Click **Next**.

   The WebLogic Server/Cluster Selection screen appears.

> **Note:**
>
> The installer does not proceed from the WebLogic Administration Server Connection Information screen if any field contains errors.

10. Select the same target WebLogic Server or cluster of servers belonging to the WebLogic Server domain and click **Next**.

If you are installing a patch on a cluster of servers, the Cluster Member Server Selection screen appears, where you can select a cluster member for UIM to patch.

The Database Type Selection screen appears.

11. Select the same database type that is used by your old UIM installation:

- If your old installation is connected to a standalone database, select **Standard Oracle 19c Enterprise Database** and click **Next**.

  The Database Connection Information screen appears.

  Do the following:

  a. Verify that the retrieved field values are correct and click **Next**.

  b. In the **Password** field, enter the database server password for the user specified in the **User Name** field.

  c. Click **Next**.

  The UIM Schema User Information screen appears.

- If your old installation is connected to an Oracle Real Application Clusters (Oracle RAC) database, select **Oracle 19c Real Application Cluster Database** and click **Next**.

  The Oracle RAC DB Nodes Connection Information screen appears.

  Do the following:

  a. Verify that the retrieved field values are correct and click **Next**.

  b. In the **Password** field, enter the database server password for the user specified in the **User Name** field.

  c. Click **Next**.

  The UIM Schema User Information screen appears.

> **Note:**
>
> The installer does not proceed from either the Database Connection Information screen or the Oracle RAC DB Nodes Connection Information screen if any field on these screens contains errors.

12. Do the following:

  a. Verify that the retrieved value in the **Schema User Name** field is correct.

  b. In the **Schema User Password** field, enter the schema user password for the user specified in the **Schema User Name** field.

  c. Click **Next**.

  The Summary screen appears.

13. Review the Summary screen and click **Install**.

  The Install screen appears, showing the status of the installation.

  When the installer completes the installation, the End of Installation screen appears. This screen provides the URLs for accessing the new release of UIM. Make a note of the URLs.

14. Click **Installed Products** and verify that the patch is listed.

15. Click **Exit**.

16. It is recommended to restart the WebLogic Administration server by using the following command from within the *Domain_Home*/**bin** directory:

```
./startUIM.sh
```

12

Configuring Oracle Maps

This chapter provides instructions on configuring Oracle MapViewer for use with Oracle Communications Unified Inventory Management (UIM) that has Unified Topology for Inventory and Automation (UTIA) microservice enabled.

Choosing a Map Option

UIM provides different options for you to point to your map data. UIM supports the following options:

- Point to the Oracle Map service (default). See "Pointing to the Oracle Map Service (Default)".
- Use existing map data. See "Using Existing Map Data".
- No existing map data. See "Using a Sample Map".

Pointing to the Oracle Map Service (Default)

UIM is preconfigured for the Oracle Map service.

The default map can be previewed from the following link:

`http://elocation.oracle.com/elocation/ajax/`

To review the proprietary information statements, see:

`http://elocation.oracle.com/elocation/legal.html`

World Mercator (Oracle Spatial SRID 54004) is a projection coordinate system widely used by tile-based online mapping services. The **elocation_mercator.world_map** served by `elocation.oracle.com` is rendered in this coordinate system.

See "Linking UIM Map Profile to MapViewer".

Using Existing Map Data

If you already have map data, you can define a custom data source that points to it. See the steps starting from "Defining the Map Data Source".

Using a Sample Map

If you do not have map data but would like to see your UIM data on a map background, you may download a world sample map from the Oracle Technology Network at the following link:

`http://www.oracle.com/technetwork/middleware/mapviewer/downloads/index.html`

After you have accessed the link, download the sample:

1. You must accept the *OTN License Agreement* to download this software. Click **Accept License Agreement**.

2. Click **Download Data Bundle**.
3. Follow the instructions in the downloaded ZIP file.

Next, see the steps starting from "Defining the Map Data Source".

Configuring MapViewer

To configure MapViewer for UIM, perform the procedures in the following sections:

1. Defining the Map Data Source
2. Defining Base Maps
3. Modifying the Map Profile Defaults
4. Linking UIM Map Profile to MapViewer
5. Enabling Map View
6. Installing Map Builder

Defining the Map Data Source

To define the data source:

1. Log in to MapViewer by entering the following in a Web browser:

   http://*ServerName:PortNumber*/mapviewer

   where *ServerName* is the application server used by UIM and *PortNumber* is the port used by UIM.

   The **Log In** page is displayed.
2. Enter the **user name and password** that you used for the WebLogic Server installation and then select **Log In**.

   The MapViewer home page is displayed.
3. To define the map data source, select **Configuration**.

   The Edit **mapViewerconfig.xml** file is displayed.
4. Scroll down to the **Predefined Data Sources** section within the file.
5. Copy the entire contents starting from the map_data_source tag to the end and paste the copied information below the existing predefined data source information within the Predefined Data Sources section.

```
<!--*****************************************************************************-->
<!--*************************Predefined Data Sources*************************-->
<!--*****************************************************************************-->
<map_data_source name="UIMDATA"
                  container_ds="jdbc/InventoryMapDataSource"
                  number_of_mappers="8"
                  allow_jdbc_theme_based_foi="false"
                  editable="false"
   />
```

   You should create the data source on the domain where the mapviewer is installed and should be pointing to the UIM database, otherwise this step will fail.

   See "Copying the JNDI URL of Map Data Source" for information about copying the JNDI URL for your map data source.

6. Find <*mds_config*> under **Map Data Server Configs** section and add the following datasource within the <*mds_config*> tag:

```
<!-- ********************************************************************* -->
  <!-- ******************* Map Data Server configs  ******************* -->
  <!-- ********************************************************************* -->
<data_source name="UIMDATA">
       <allow_predefined_themes>true</allow_predefined_themes>
       <allow_dynamic_themes>true</allow_dynamic_themes>
    </data_source>
```

7. Click **Save & Restart**.

   Two messages **File mapViewerConfig.xml has been saved** and **MapViewer has been restarted** are displayed above the Config area. The jdbc_password is displayed as encrypted.

8. Select **Admin**.

   The UIMDATA data source that is configured should appear in the existing **Data Sources** table.

9. Select **Datasources** and verify if the corresponding value (for example, MAPDATA) is displayed in the *Existing data sources* table.

10. Go to **Admin** tab and open **Create tile layer**.

11. From **Tile layer type**, select **Oracle Maps** and click **Next**.

    The Tile Layer Properties page appears.

12. Under **External tile layer** section, enter the **Name** as **ELOCATION_MAP**.

13. From **Data source**, select **UIMDATA** and click **Next**.

    The Tile Layer XML page appears.

14. Click **Submit**.

    The system saves the configuration changes and you can verify the changes from **Existing map tile layers** section in **Manage tile layers** page.

Copying the JNDI URL of Map Data Source

This section provides information on how to copy the JNDI name of the map data source in the WebLogic domain where MapViewer is installed.

To copy the JNDI name of the map data source:

1. Log in to the WebLogic Server Administration Console.
2. Click **Lock & Edit**.
3. In the Domain Structure tree, expand Services, and then click **Data Sources**.

   The Summary of JDBC Data Sources page appears.

4. Click *YourDataSource*.

   The Settings for *YourDataSource* page appears.

5. In the **JNDI Name** field, copy the JNDI name, **jdbc/***YourDataSource*.

Defining Base Maps

There is no limit to the number of base maps that can be used for UIM. For example, you can use an existing world map as the base map.

To point to the world map:

1. Go to **Admin** tab and open **Create tile layer**.
2. From **Tile layer type**, select **Oracle Maps** and click **Next**.

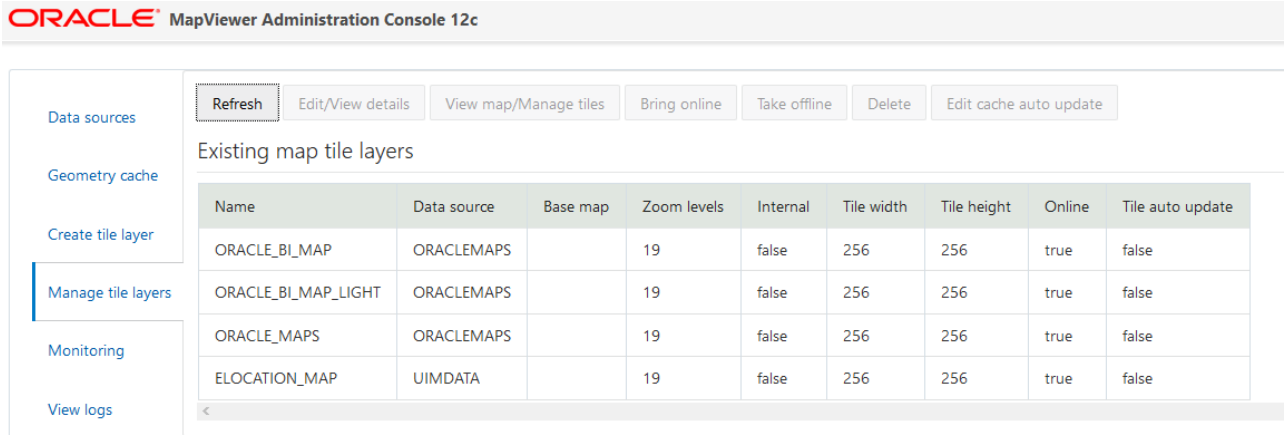
   The Tile Layer Properties page appears.
3. Under **External tile layer** section, enter the **Name** as **ELOCATION_MAP**.
4. From **Data source**, select **UIMDATA** and click **Next**.

   The Tile Layer XML page appears.
5. Click **Submit**.

   The system saves the configuration changes.
6. Verify the map is set up changes from **Existing map tile layers** section in **Manage tile layers** page.

   Figure 12-1 shows an example of existing map tile layers.

Figure 12-1 Example of Existing Map Tile Layers



The map tile layer is the link between UIM and MapViewer.

There is no limit to the number of map tile layers you can set up.

Modifying the Map Profile Defaults

If you want to change the default settings for the map profile, set the *UIM_Home*/**config/resources/event/topologyProcess.properties** file on the application server to:

```
# Map Profile Default Settings
defaultBaseMap=ELOCATION_MAP
defaultApplicationDatasource=UIMDATA
defaultMapTileServerUrl=http://elocation.oracle.com/mapviewer/mcserver
defaultMapCopyright=Copyright \u00a9 2007, 2021 Oracle Corp
```

> **Note:**
>
> If you are pointing to an internal base map and not the Oracle map service, leave the `defaultMapTileServerUrl=` blank.

Linking UIM Map Profile to MapViewer

This section is applicable only for Networks Map View.

For other Map View pages (in Pipe, Service and Connectivity), you cannot set the Map Profile values. For these Map View pages, the map profile values from **Map Profile Default Settings** section in the **topologyProcess.properties** file are considered by default.

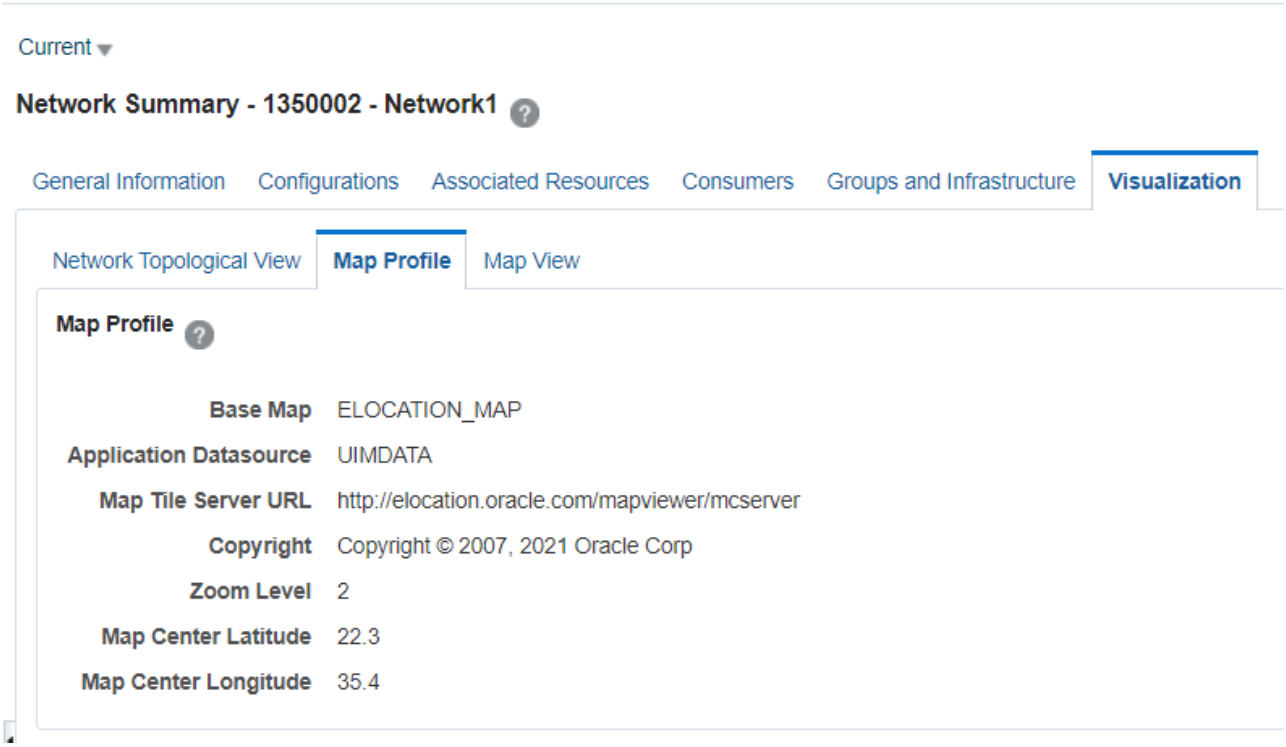
To link the UIM map profile to MapViewer:

1. Ensure you are logged into UIM.
2. Select the **Network** link.
3. Search for and open any **Network**.
4. Open the **Map Profile** subtab under the **Visualization** tab.

   The Map Profile page is displayed.
5. Enter Map Center Latitude.
6. Enter Map Center Longitude.

   Figure 12-2 points to a MapViewer DataSource/Map Tile Layer Name combination.

Figure 12-2 Example of Network Information



7. Click **Save**.

   The Network Summary page is displayed.
8. Open the **Map View** subtab under the **Visualization** tab.
9. The **Map View canvas** is displayed.

Enabling Map View

To enable Map View:

1. Provide the following permissions to <UIMSCHEMA> user:
   - Set **global_names** value to **FALSE**.
   - Provide **Create SYNONYM** and **DATABASE LINK** permissions.

   > **Note:**
   >
   > You need to log in as the database administrator to provide these permissions.

2. Log out of the database administrator's profile and log in as <UIMSCHEMA> user.
3. Open **system-config.properties** file from the UIM domain **{DOMAIN_HOME}/UIM/config** and set the **uim.ui.mapViewEnabled** property value to **true**.
4. Go to the extracted **ora_uim_dbtools.jar** file and open the **sqlscripts** folder.
5. Run **UIM_TOP_DBLINK.sql** and provide the Topology schema details when the system prompts for it.

   See "Database Schema Changes" for more information.

   > **Note:**
   >
   > Run the **UIM_TOP_DBLINK.sql** script every time you migrate to a new Topology schema.

Installing Map Builder

Oracle Map Builder is a standalone application that lets you create and manage the mapping metadata (styles, themes, and base maps) that is stored in the database.

Oracle Map Builder is downloaded as a JAR file (**mapbuilder.jar**) from the Oracle software delivery website. You can run it as a standalone Java application in the JRE:

```
java -jar mapbuilder.jar [Options]
```

It is important to use the **Mapbuilder.jar** file that is downloaded from the Oracle software delivery website in order to stay on the same release with the MapViewer application that is shipped with UIM.

See the *User's Guide For Oracle MapViewer* for detailed information on MapViewer. For a link to the document, see "Viewing MapViewer Documentation".

Viewing MapViewer Documentation

The *Oracle Fusion Middleware User's Guide For Oracle MapViewer* contains detailed MapViewer documentation. The following is a link to the library page, where the document is located:

http://www.oracle.com/technetwork/middleware/mapviewer/documentation/index.html

13
Uninstalling Unified Inventory Management

This chapter describes how to uninstall Oracle Communications Unified Inventory Management (UIM).

About Uninstalling UIM

You use the Oracle Universal Installer to uninstall UIM. The installer uninstalls the core application and other components of UIM.

Interactive mode: Use the interactive mode when you want to interact with the installer UI during installation. See "Uninstalling UIM or UIM Components".

> **Note:**
>
> WebLogic Server must be running before proceeding with the uninstall procedure.

Uninstalling UIM or UIM Components

To uninstall UIM, or a component belonging to the UIM product:

1. From a command line, navigate to the *Oracle_Home*/**oui**/**bin** directory and run the following command to initiate the Oracle Universal Installer **runInstaller** executable file:

   ```
   ./runInstaller
   ```

   The Oracle Universal Installer installation wizard starts.

   The Welcome screen appears.
2. Click **Deinstall Products**.

   The Inventory screen appears.
3. Select the components you want to uninstall.
4. Click **Remove**.

   > **Note:**
   >
   > Selecting **Show Empty Homes** displays any previously created Oracle product homes. Select displayed homes, or folders, to remove them.

   The User Input screen appears.
5. In the **WebLogic User Password** field, enter your WebLogic user password, and click **OK**.

> **Note:**
>
> Ensure that the correct password is entered. There is no password validation for this step. If the password is incorrect, the uninstall will continue and the UIM JAR and EAR files are not undeployed from the WebLogic domain.

The Confirmation screen appears.

6. View and confirm your selection, and click **Next**.

   You can see the progress as the selected components are uninstalled.

   The installer removes all of the files except the logs. If required, delete the log files manually. The logs can be found at the following location:

   CentralInventorylocation/**logs**/

> **Note:**
>
> The UIM schema, UIM user, Cartridge Deployer Client and CMWS user will not be removed during uninstallation. The database schema and application users can be used by other applications, so they should not be deleted.

7. Remove the MDS schema user. See *Oracle Fusion Middleware Repository Creation Utility User's Guide* for details on removing/dropping the schema.

14

Enabling Geographic Redundancy and Disaster Recovery

This chapter describes a generic architecture for UIM across multiple geographically redundant sites in a primary-standby (active-passive) deployment. This chapter provides the following information:

- Architecture for Geographically Redundancy (GR) in UIM
- Installation, configuration, and operational best practices
- Switchover and failover test procedures and test results

About Geographic Redundancy and Disaster Recovery in UIM

The UIM application architecture supports high availability across distributed application and database clusters in a typical single site deployment. UIM operations run continuously regardless of the failure of a single application or database node in a production environment. However, in some cases, continuity of operations with minimal loss of service is required, in the event of a complete failure (due to a natural disaster) in the primary UIM or OSS application stack.

The following figure shows a highly available single-site architecture is comprised of: UIM, deployed to a clustered WebLogic domain with two or more managed servers on multiple hosts, and an active-active RAC database. When a single managed server or database instance becomes unavailable, the surviving nodes can automatically take up the excess load. For more information on system requirements for attaining UIM high availability, see Unified Inventory Management System Requirements.

Figure 14-1 UIM Single-Site High Availability Architecture

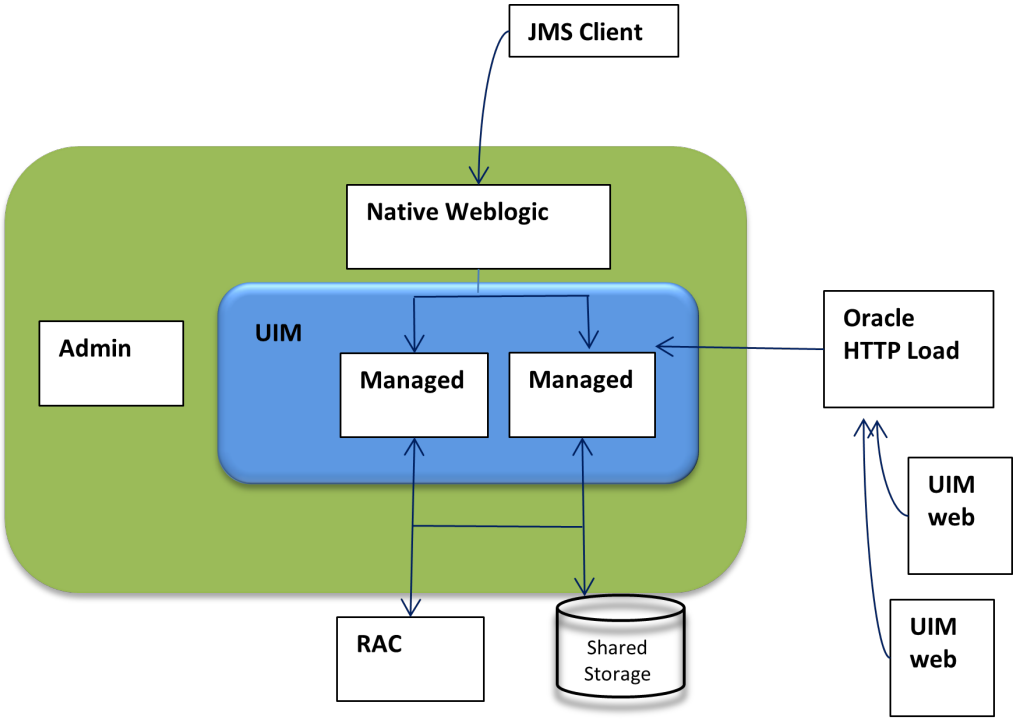
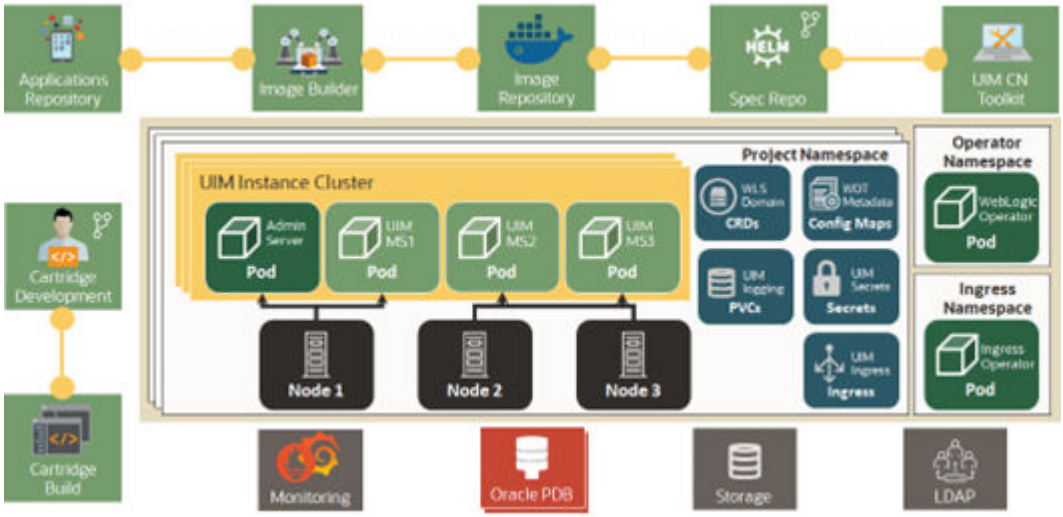


Figure 14-2 UIM Cloud Native Single-Site Availability Architecture



Additional resiliency is achieved when UIM is deployed to geographically redundant sites in a symmetric primary-standby configuration, where the standby site is a duplicate of the primary site. When the primary site becomes unavailable and cannot be recovered within a reasonable amount of time or with a reasonable amount of effort, UIM services can fail over to the standby site, effectively making the standby site the new primary site.

This chapter describes a generic architecture for UIM across multiple geographically redundant sites in a primary-standby (active-passive) deployment. The architecture described provides guidelines for projects with geographically redundant site availability requirements.

This chapter provides information about the following:

- Architecture for Geographically Redundancy(GR) for UIM
- Installation, configuration, and operational best practices
- Switchover and failover test procedures and test results

About Switchover and Failover

The purpose of a geographically redundant deployment is to provide resiliency in the event of a complete loss of service in the primary site, due to a natural disaster or other unrecoverable failure in the primary UIM site. The resiliency is achieved by creating one or more passive standby sites that can take the load when the primary site becomes unavailable.

The role reversal from the standby site to the primary site can be accomplished in any of the following ways:

- Switchover, in which the operator performs a controlled shutdown of the primary site before activating the standby site. This is primarily intended for planned service interruptions in the primary UIM site. Following a switchover, the former primary site becomes the standby site. The site roles of primary site and standby site can be restored by performing a second switchover operation, which is switchback.
- Failover, in which the primary site becomes unavailable due to unanticipated reasons and cannot be recovered. The operator then transitions the standby site to the primary role. The primary site that is down cannot act as a standby site and will require reconstruction of the database as a standby database before restoring the site roles.

Geographically Redundant Traditional UIM Deployment

A geographically redundant UIM deployment comprises two or more geographically distant sites: a primary site, which has the production environment, and one or more offline standby sites where each site includes the UIM deployment and its associated RAC database as shown in the following figure.

Figure 14-3 UIM Multi-Site Geographically Redundant Architecture

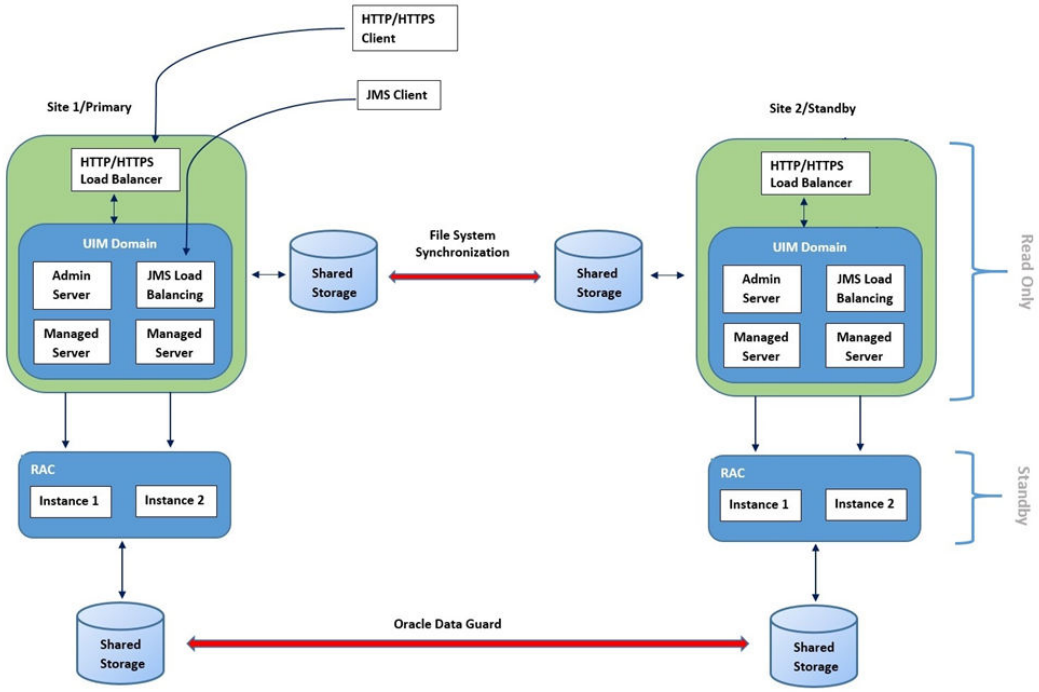


Figure 2. UIM Multi-Site Geographically Redundant Architecture.

About the Primary Site

The primary site is identical in nature to a typical single-site deployment of UIM (see Figure 1). The application layer consists of a clustered WebLogic domain with two or more managed servers, an Admin server, and an HTTP/HTTPS load balancer. Additionally, using a Node Manager on each machine in the domain is recommended to manage the admin server and managed server processes.

The UIM workload is distributed across the managed servers in the WebLogic cluster. If a cluster node goes down, the workload is redistributed across the surviving cluster nodes. A Store-and-Forward (SAF) agent can provide additional resiliency for JMS messages by buffering incoming requests, if the destination JMS targets become unavailable.

The database layer consists of a RAC database, typically in an active-active configuration, where each managed server is affiliated with a given database instance. In the event of a failure in a single database instance, the surviving instance will pick up the load. The database layer stores all transactional data including:

- JMS messages backed by a JDBC persistent store
- SAF messages
- UIM data and Metadata
- LDAP Policy data

About the Standby Site

After either a switchover or failover operation, the targeted standby site assumes the role of a primary site for both the application stack and the database. Standby sites are synchronized

periodically with the primary site to maintain service continuity in the event of a catastrophic failure at the primary site.

The above figure shows a two-site active/passive UIM configuration for geographic redundancy. In this deployment scenario, the primary and standby site(s) are installed in geographically different locations, typically in different data centers. Interconnection is established through WAN. This multi-site deployment has the following features:

- Multiple symmetric sites: In a multiple symmetric site, the primary site runs and actively processes service requests while the secondary site is passive; the secondary UIM WLS cluster is available but cannot process **create** and **update** requests while the database is in a standby role.
- The UIM WLS domain is replicated from the primary site to the secondary site using file system replication utilities such as.**rsync**.
- Oracle Data Guard is used to replicate the UIM RAC database from the primary site to the secondary site. All updates to the primary database (including database sequences) are automatically propagated to the secondary database in near-realtime.

The Oracle Data Guard standby database is not read-write accessible. As a result, the UIM application cluster cannot be run in the standby site.

Geographically Redundant UIM Cloud Native Deployment

A geographically redundant UIM CN deployment comprises two or more geographically distant sites: a primary site, which has the production environment, and one or more offline standby sites where each site includes the UIM CN deployment and its associated RAC database as shown in the following figure.

UIM in data center1 is the primary and active instance and UIM in data center 2 can be a cold/ warm standby.

Figure 14-4 UIM Cloud Native Deployment and the Associated RAC Database

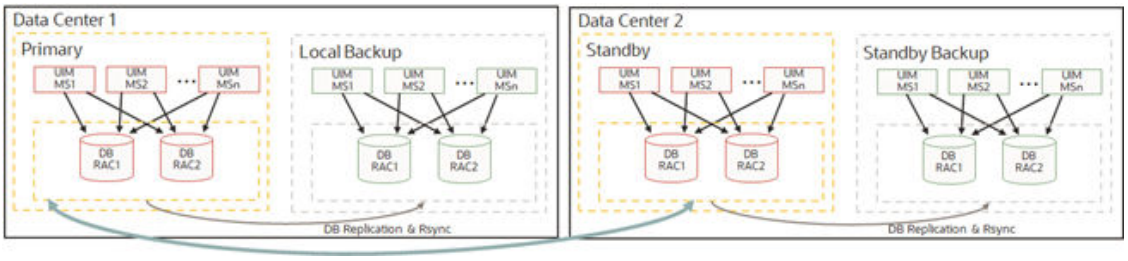
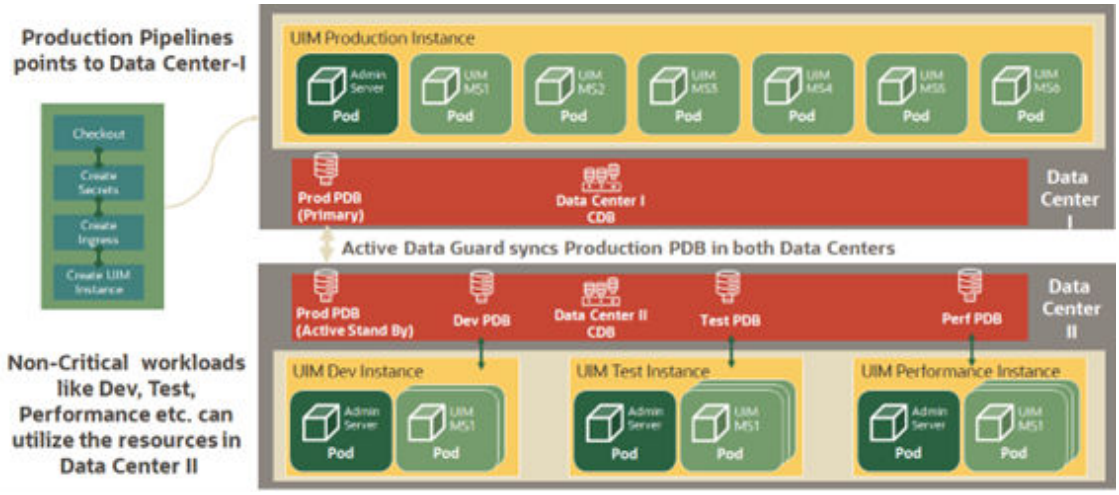


Figure 14-5 Active-Passive Deployment



About the Primary Site

The primary site is identical to a typical single-site deployment of UIM. The application layer consists of a clustered WebLogic domain with two or more managed server pods, an Admin server pod, and an Ingress pod as load balancer. Additionally, there is a WebLogic Operator pod to support WebLogic server on Kubernetes environment. UIM CN pipelines are used for continuous deployment and these pipelines point to Data Center 1 in normal operations.

The UIM workload is distributed across the managed servers in the WebLogic cluster. If a pod goes down, the workload is redistributed across the surviving cluster pods. And if a Kubernetes worker node goes down, then workload is distributed across managed servers on surviving Kubernetes nodes. A Store-and-Forward (SAF) agent can provide additional resiliency for JMS messages by buffering incoming requests when the destination JMS targets become unavailable.

The database layer consists of a RAC database, in an active-active configuration, where each managed server is affiliated with a given database instance. In the event of a failure in a single database instance, the surviving instance will pick up the load. The database layer stores all transactional data including:

- JMS messages backed by a JDBC persistent store
- SAF messages
- UIM data and Metadata
- LDAP Policy data

About the Standby Site

After a switchover or a failover operation, the targeted standby site assumes the role of a primary site for both the application stack and the database. Standby sites are synchronized periodically with the primary site to maintain service continuity in the event of a catastrophic failure at the primary site. The above figure shows a two-site active/passive UIM configuration for geographic redundancy. In this deployment scenario, the primary and standby site(s) are installed in geographically different locations, typically in different data centers. Interconnection is established through WAN. This multi-site deployment provides:

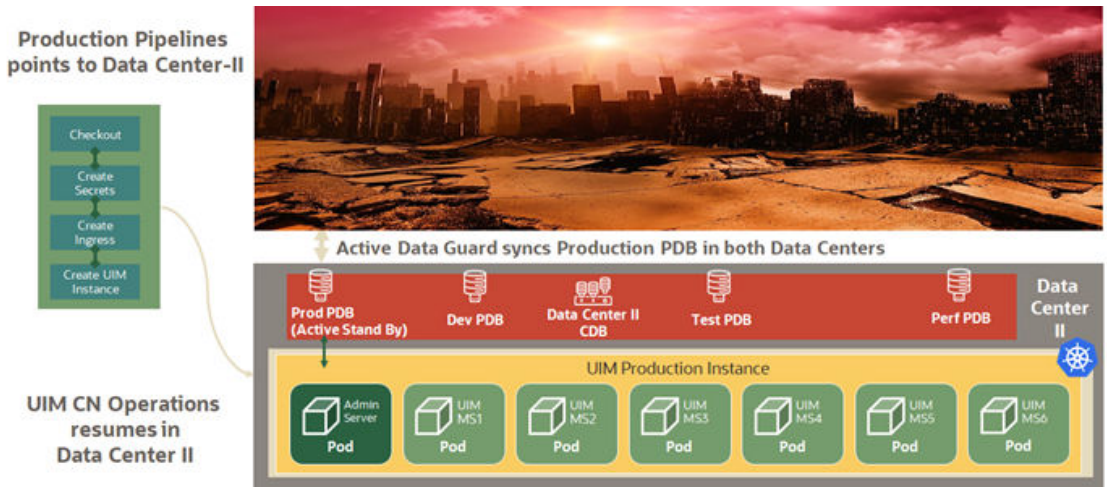
- Multiple symmetric sites: In multiple symmetric sites, the primary site runs and actively processes service requests while the secondary site is passive. The secondary UIM WLS

cluster is available but cannot process create and update requests while the database is in a standby role.

- Non-critical workloads such as development, testing, and performance can utilize the resources in Data Center 2.
- Oracle Data Guard is used to replicate the UIM RAC database from the primary site to the secondary site. All updates to the primary database (including database sequences) are automatically propagated to the secondary database in near-realtime.

The Oracle Data Guard standby database is not read-write accessible. As a result, the UIM application cluster cannot be run in the standby site.

Figure 14-6 Active-Passive Deployment During Disaster and Recovery



When a disaster strikes on DataCenter1, the following operations are performed:

- Stop all non-critical workloads in Data Center 2
- Redirect the production pipeline to use Data Center 2

Prerequisites for Geographic Redundancy

This section provides the prerequisites for supporting geographic redundancy in UIM.

Synchronize File Systems

For UIM geographic redundancy, Oracle recommends using a common file system utility such as **rsync** for replicating and synchronizing the primary site file system with the standby site. The **rsync** utility has the following advantages:

- It is available on most Unix and Linux distributions, including Oracle Solaris and Oracle Enterprise Linux.
- Differences between source and target files are computed using an algorithm that ensures that only the changes to files are copied from the primary site to the standby site.
- It can use SSH as a secure channel.
- If network bandwidth is an issue, **rsync** can compress data during transfer.

The **rsync** utility does not support creation of nested target subdirectories. You cannot create a full target directory path unless the target directory is a subdirectory of the source directory. For example, if the source directory is specified as **/share/apps/Oracle** and the target is specified as **/share/apps/Oracle/Middleware/user_projects/domains/UIM_domain**, **rsync** does not create the directories under **../Oracle**.

Other options for file system replication include:

- Using ZFS. ZFS is available for Oracle Solaris and available in open-source variants for Linux
- Oracle Solaris Cluster Geographic Edition
- File system utilities such as rcp, scp, ftp, or sftp are not well suited for incremental synchronization, but can be used for initial file system replication

Synchronize UIM Domain

Oracle Data Guard can manage database synchronization without any additional file system updates. The standby UIM domain, on the other hand, must be kept in synchronous with the primary site by using ZFS, Oracle Solaris Cluster Geographic Edition, or other file system utilities that can be used for initial file system replication. Files that must be kept in continuous synchronization include any files that are expected to be created or modified during the normal course of UIM operation. For example:

- The **system-config.properties** file and other property files
- Java code changes that include hotfixes or changed rulesets containing Java code

If the **rsync** utility is used to incrementally update the standby site, it will also detect differences in any files in the UIM domain that contain site-specific configuration such as host name, IP address, local directory name, and data source information (such as database host names, service names, and so on). When **rsync** detects the differences, it replaces the content in the standby site with the versions currently on the primary site which could prevent the standby UIM site from operating correctly. These files must be updated after synchronization to reflect local site-specific values. The impact can be minimized using virtual host names.

Oracle Data Guard

Oracle Data Guard is used to replicate the primary UIM Oracle RAC database for the standby sites. Oracle Data Guard can be configured with either a physical standby database or a logical standby database. The main considerations for each are as follows:

- Physical Standby: The physical standby database is a block-by-block duplicate of the primary database, synchronized by the automatic application of archived redo logs transferred to the standby database through Oracle Net (SQL*Net). By default, a physical standby database is mounted for archive recovery only. With the purchase of an additional license, the physical standby can be opened for read-only access using Active Data Guard.
- Logical Standby: The logical standby database is a logical copy of the primary standby database that does not necessarily have to match the schema of the primary standby database. Logical standby databases transform archived redo logs into SQL DML (insert, delete, and update) statements, which are then populated into the standby database and applied automatically. Logical standby databases are opened in read-only mode and can have additional tables, views, and indexes that are not present in the primary standby database.

Oracle recommends using a logical standby database for implementing a geographic redundancy solution for UIM to ensure that a standby database is in **read only** mode and to have the standby site ready to start when needed.

Data Protection Modes

Oracle Data Guard can operate in one of following data protection modes:

- **Maximum Performance:** This is the default data protection mode. This mode allows transactions to commit as soon as all redo data generated by those transactions has been written to the online redo log. Transmission of redo data to the standby database is done asynchronously, so that the primary database performance is not affected by the transmission delays when writing the redo logs to the standby database.
- **Maximum Availability:** This mode guarantees zero data loss if the primary database fails but only if the complete set of redo logs has been successfully transmitted to the standby database. In maximum availability mode, transactions commit only after all redo data required for those transactions has been successfully transmitted to the standby database. If there are delays in transmitting the redo logs, the primary database will continue to process transactions but will operate as if it is in the maximum performance mode.
- **Maximum Protection:** This mode is similar to the maximum availability mode. In the maximum protection mode transactions are allowed to commit only after the complete set of redo logs required to recover those transactions has been successfully written to the standby database. However, the primary database will shut down if anything prevents the transmission of the redo logs. For this reason, it is recommended that at least two standby databases be configured in the maximum protection mode to reduce the risk of a single standby database failure.

> **Note:**
>
> Oracle recommends you operate Oracle Data Guard in the Maximum Performance mode for UIM geographic redundancy solutions.

Network Configuration

Oracle recommends that a network performance assessment be conducted, considering the current or anticipated redo rates, both peak and average. While configuring a network, the following considerations must be considered:

- The network bandwidth required for the average or peak redo rates, depending on the typical redo dynamics of the primary database. For example, if redo rates are stable and **ASYNC** transport is used, the high but short-lived peaks in redo generation can be ignored. The estimation network bandwidth is mentioned in the later sections.
- The impact of network latency on redo transmission, which is dependent on the transport mode:
  - **SYNC**: Both Maximum Protection and Maximum Availability modes require SYNC transport. In this case, minimal network latency is required to reduce the performance impact on the primary database.
  - **ASYNC**: The default Maximum Performance mode uses ASYNC transport which minimizes performance impact on the primary database and is not as susceptible to issues related to network latency.

* Multiple redundant network paths

For more information regarding network configuration and tuning for Oracle Data Guard, see *Oracle Database High Availability Best Practices*.

Network Bandwidth Estimation

There is no precise network bandwidth that can be applied to generic Data Guard deployments. The bandwidth must be sufficient to accommodate the typical redo log generation rate, which is dependent on the number and size of transactions during a given period.

Assuming an overhead of 30% for Oracle Net, the following calculation, as described in *Oracle Data Guard 11gR2 Administration Beginner's Guide*, provides an estimate of the required network bandwidth for Data Guard redo log transmission:

```
Required Bandwidth (Mbps) = ((Redo Rate bytes per second / 0.7) * 8) /
1,000,000
```

There are several methods available for determining the redo generation rate and typical bandwidth requirement based on the actual performance of the primary system:

- AWR snapshot reports: The Load Profile section of this report provides an average 'Redo Generated Per Sec' value that shows the redo rate in bytes-per-second averaged over the snapshot period.
- **Sysmetric** views that can provide more accurate estimates as they are averaged over 60 and 15 second intervals. For example, the **dba_hist_sysmetric_history** view can be queried directly for this value.
- For a more historical calculation, the data provided by the **v$archived_log** view provides the amount of redo generated for each log change.

Example 14-1 Estimation for a Simple Network Bandwidth

To estimate the bandwidth requirement for Data Guard, in an environment averaging 7500 orders per hour, the following query is executed on the primary database server as a **sysdba** user:

```
SELECT
(AvgRedorate_Bps * 8 / 0.7) / (1000000) AvgBandwidth_Mbps FROM (
SELECT
AVG(value) AvgRedoRate_Bps FROM
dba_hist_sysmetric_history WHERE
metric_name = 'Redo Generated Per Sec'
AND begin_time >= (select sysdate - 7 from dual)
);
```

For 7 days and an average redo rate of 727304.442 bytes per second, the above calculation provides the following results:

- **Period (days)**: 7
- **Average Redo Rate (bytes per second)**: 727304.442
- **Average Bandwidth (Mbps)**: 8.312

In this example, rounding upwards yields a conservative network bandwidth estimate of 10 Mbps for Data Guard redo log transmission.

If the recommended Maximum Performance Data Guard data protection mode is used, infrequent spikes in redo log activity can be accommodated if the network is tuned for the average redo generation rate. If, however, there are frequent peaks or the variation in redo rate is significant, the maximum redo rate for the specified period will have to be taken into consideration.

Advanced Compression in Oracle Data Guard

If network bandwidth or latency cannot accommodate the primary database redo dynamics and there is sufficient memory and CPU to perform the compression, Oracle Database Advanced Compression may be configured to send the redo logs in compressed form, thus reducing pressure on the network and potentially increasing transmission speed.

The Advanced Compression feature uses **zlib** compression at level 1, similar to the **gzip** utility.

To estimate the effectiveness of the compression, locate and compress a redo log file using the following **gzip** command:

```
$gzip -1 <archive.arc>
```

Then use the following gzip command to compare the compressed and uncompressed data:

```
$gzip --list <archive.arc.tgz>
```

> **Note:**
>
> Oracle Database Advanced Compression requires additional licensing.

Host Configuration

This section describes considerations for host configuration.

Shared Storage Configuration

Both UIM WebLogic domain and Data Guard configurations benefit from shared storage for data files. Ideally, the names of the shared directories should be identical on both primary and standby sites to facilitate site replication. For Oracle Data Guard, archived redo log directories should have the same name.

For the UIM WebLogic domain, this is not a mandatory requirement, but reduces the complexity of synchronizing configuration files across sites as the domain configuration files and scripts necessarily contain full paths for JRE and script locations.

Hostname Virtualization

The primary and standby sites must be created on hosts that are separated geographically and may belong to different subnets. In UIM domain configuration, hostnames are stored in domain configuration files, which are then site-specific. As described in the section on file system synchronization, hostnames must be associated with the local site.

Oracle recommends that some form of hostname virtualization should be used to simplify UIM domain replication and that hostnames, rather than IP addresses, should be used for all cluster and server configuration. An easy approach is to add additional entries to the local **/etc/hosts**

file for each WebLogic and RAC database host. For example, on the first node of the primary site, the relevant hosts file entry might appear as follows:

```
10.1.2.3    real.primary_host_1.domain v-UIM-appserver-node-1
```

On the first node in the standby site, the entry may appear as follows:

```
10.1.2.4    real.standby_host_1.domain v-UIM-appserver-node-1
```

When UIM domain is created on the primary server, the hostname **v-UIM-appserver-node-1** is used for the first node, resulting in the following entries in the generated UIM domain configuration file (domain config.xml):

```
<server>
    <name>AdminServer</name>
    <machine>UnixMachine_1</machine>
    <listen-address>v-UIM-appserver-node-1</listen-address>
    <server-diagnostic-config>
        <name>AdminServer</name>
        <diagnostic-context-enabled>true</diagnostic-context-enabled>
    </server-diagnostic-config>
</server>
```

While synchronizing the domain configuration, the hostnames will not have to be modified in the two sites.

IP Address Virtualization

Within the UIM domain, for communication between the managed servers and the admin server, the hostname virtualization process that is explained above can be used. Remote clients, however, may be unable to connect to UIM following a switchover or failover operation. To mitigate this, IP address management software (IPAM) can be used to reassign the UIM application host names to the IP addresses reserved for the standby UIM application servers.

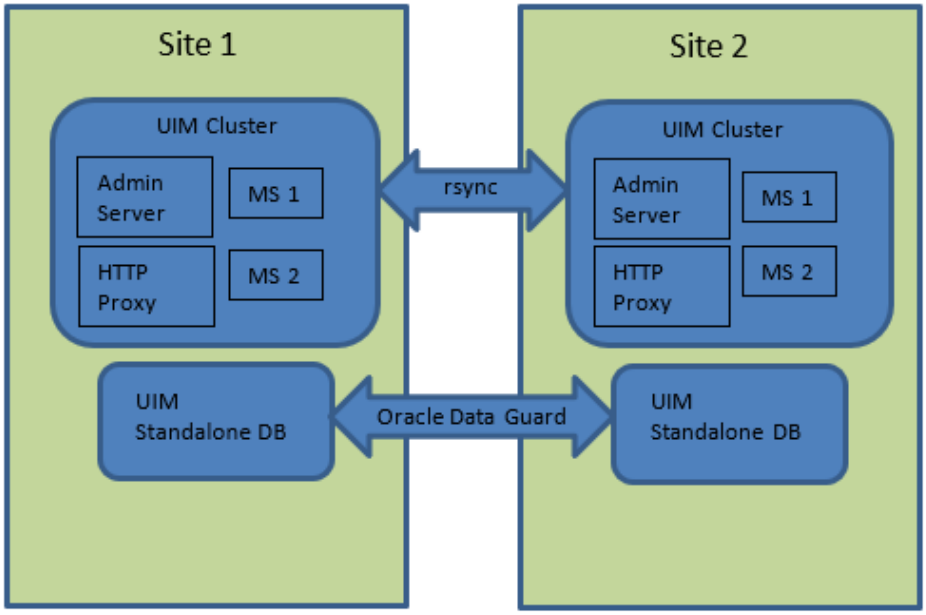
UIM Geo-Redundancy Lab Architecture

To demonstrate the feasibility of a multi-site geo-redundant deployment for UIM, a Geo-Redundancy (GR) lab environment has been established as described in the later sections.

The UIM Geo-Redundancy (GR) lab architecture, as shown in the following figure, is based on the two-site high-availability deployment discussed earlier. Each site in the GR lab deployment comprises two Oracle Enterprise Linux virtual machines (VM); one each for the WLS domain and the Oracle standalone database, respectively.

The UIM application includes UIM installed on the corresponding Oracle WebLogic Server with 19c Standalone database. The list of hardware and software components is mentioned in the later sections.

Figure 14-7 UIM Geo-Redundancy Lab Architecture



UIM Application Architecture

UIM is installed on a cluster with two managed servers: domain admin server and a HTTP proxy. A second domain is configured on node 1 comprising only an admin server.

Database

The UIM database is configured as 19c standalone database nodes. Oracle Data Guard handles database replication: the Data Guard documentation procedure is used to manage the primary and standby databases and to run the switchover and failover operations.

Installation and Configuration

This section describes the installation and configuration of the geo-redundancy test environment. For more information on UIM high-availability installation and configuration, *UIM Installation Guide*.

Hardware Components

The application and database servers are configured as follows:

- Operating System: Oracle Linux Server release 7.7
- CPU: Intel Xeon E5-2699 v3 @2.30 GHz
- RAM: 28 GB
- NFS Storage: 292 GB

Software Components

The list of installed software components is as follows:

Table 14-1 UIM GR Lab Software Components

Software Component	Installed Version
UIM	7.4.1.0 (or later)
Oracle WebLogic	12.2.1.3 (or later)
Java Development Kit (JDK)	1.8.0_221 (or later)
Oracle Enterprise Database	19.4.0.0.0 (or later)

Installing Oracle Data Guard

To install Oracle Data Guard:

1. On site 1, configure the primary UIM database.
2. Create and configure the standby UIM database on site 2. See the Oracle Data Guard documentation for detailed instructions, Oracle Data Guard configuration details are listed in the following section.

UIM GR Lab Data Guard Configuration

The configuration details for Oracle Data Guard for the UIM GR lab are as follows:

- Symmetric Topology. Disaster recovery configuration that is identical (identical number of hosts, load balancers, instances, applications, and port numbers) across tiers on the primary and standby sites. The systems are configured identically, and the applications access the same data.
- Logical Standby Database.
- Maximum Performance Mode. Transactions commit as soon as all redo data generated by those transactions has been written to the online log. Redo data is asynchronously written to the standby database.

Mapviewer themes and styles are saved in the MDSYS schema. As part of Data Guard syncing process, the MDSYS schema is not synced to the standby database. For Mapviewer to work properly in the standby environment, run the following scripts in the MDSYS schema in the standby database:

```
<domain_home>/UIM/scripts/usersdothemes.sql
<domain_home>/UIM/scripts/uimdefaultstyles.sql
```

Installing the Applications

To install the applications:

1. On site 1, install the WebLogic Server and Oracle Application Development Framework.
2. On site 1, configure and start a clustered WebLogic domain with two managed servers for UIM. Where ever applicable, use hostnames, instead of IP addresses.
3. On site1, install UIM and configure both the database schema and the application server.

> **Note:**
>
> While configuring the WebLogic domain for UIM, Oracle recommends using a JDBC store for the JMS persistent store, instead of the default file store. Replication of JMS transactional data is managed automatically through Oracle Data Guard, ensuring a consistent transactional state across the sites.

4. Replicate WebLogic and UIM domain directories to the standby site.
   For the geo-redundancy test environment, use **rsync** to synchronize the complete WebLogic and UIM domain file systems including deployed cartridges, property file changes and security changes, except for log and temporary directories from site 1 to site 2.
5. After the synchronization, domain configuration files on site 2 are modified using the Unix/Linux sed utility to ensure that all host-specific entries correspond to the correct site.

Error

After completing the installation procedures, if you see the following error while starting the UIM server on site 2, then follow the resolution provided.

```
Caused By: oracle.security.jps.JpsRuntimeException: JPS-01050: Opening of
wallet based credential store failed.
```

Resolution

Create an empty **/tmp** directory in the <*domain_home*>/**UIM** folder in site 2 with required folder permissions.

Switchover and Failover Test Procedures

This section describes the procedures to run the UIM GR test scenarios.

Switchover Procedure (Graceful Shutdown)

The switchover procedure is used to test continuity of service after a controlled context switch from the primary site to the secondary site.

1. Ensure that UIM is running on the primary site and that request submission is in progress.
2. Stop the operations.
3. Wait for UIM to stop processing incoming requests.
4. Perform a graceful shutdown of the UIM domain.
5. Switch the primary database role to the backup database.
6. Start UIM on the secondary site.
7. Resume request submission.

As an alternative, UIM can be shut down gracefully before request submission is stopped.

Failover Procedure

In a production environment, failover is the result of a catastrophic loss of service on the primary site. If the primary database becomes unavailable and cannot be recovered, the Data Guard **Activate** commands can be issued on the backup server. This results in change of role from a backup database to the primary database, but it will not convert the primary database to the backup database. As a result, when the failed primary site becomes available again, it will have to be rebuilt as a physical standby database to re-enable Data Guard protection.

1. Ensure that UIM is running on the primary site and that request submission is in progress.
2. When the number of in-progress requests has reached a steady state, abort the primary database.
3. Shut down UIM. Graceful shutdown is not required.
4. Issue Data Guard Activate statement on the standby database.
5. Start UIM on the secondary site.
6. Ensure that request submission has resumed.

> **Note:**
>
> After the original primary site is recovered, the same switchover procedure can be repeated to switch back to the original primary site.

Test Cases

Perform the following test cases for switchover and failover scenarios to ensure that secondary site has all the information replicated and is available to resume the operations:

- Cartridge Deployment
- Entities creation from UI
- Property file changes
- Security changes from console (Users create/update)

A

Configuring KeyCloak as Identity Provider for UIM, UTIA, and Message Bus

This chapter helps you with information on configuring KeyCloak as an Identity Provider for UIM, UTIA, and Message Bus.

For more information on UTIA and Message Bus, see *Unified Inventory and Topology Deployment Guide*.

Prerequisites for Configuring KeyCloak

The following prerequisites are required for configuring KeyCloak:

- Install **KeyCloak**.
- Download all artifacts required to deploy all UIM, UTIA and Message Bus.

Creating a New Realm

To create a new realm:

1. Provide a name for the realm. For example **IdentityGuard**.
2. Set **Enabled**.
3. Click **Create**.
   A new realm is created.

Downloading the Identity Provider Metadata File

To download the Identity Provider metadata file:

1. Switch to the realm you created.
2. Go to **Realm Settings**.
3. Click **SAML 2.0 Identity Provider Metadata**.
4. Save the file at a desired location.

Creating a UIM Cloud Native Instance

Follow the instructions mentioned in the "**Configuring SSO using SAML 2.0 for UIM CN"** section from *UIM Cloud Native Deployment Guide*.

Create a UIM cloud native instance as follows:

1. Build UIM CN images using the above downloaded IdP metadata file.
2. Create UIM CN instance. You can provide a SAML **entityId** of your choice and the same will be used by the KeyCloak SAML client. For example: **samlUIM**.

3. Publish UIM CN Metadata file as KeyCloak supports SAML client creation using Service Providers Metadata file.

For more information on creating a UIM cloud native instance, see *UIM Cloud Native Deployment Guide*.

Creating a SAML Client for UIM

To create a SAML client for UIM:

1. Log in to KeyCloak and switch to your realm.
2. Click on the **Clients** tab.
3. Choose the **import client** option and add **UIMCNMetadata.xml** (the SP metadata file) to **resource file**.
4. **Client ID** is automatically selected from SP metadata file. It is the same as provided in the **project.yaml** of UIM CNTK.
5. Turn off the **Client Signature Required** flag.
6. Click **Save** and verify the client configuration.
7. If SSL is enabled, add UIM certificates to **JAVA_HOME** of KeyCloak.

Creating a SAML Client Role

To create a SAML client role:

1. Log into KeyCloak and switch to your realm.
2. Click on the **Clients** tab.
3. Click on the client you have created above.
4. Click **Roles.**
5. Create a role with the name **uim-users.**

Adding Role Mapper in SAML Client Scope

To add role mapper in SAML client scope:

1. Log into KeyCloak and switch to your realm.
2. Click on the **Clients** tab.
3. Click on the client you have created above.
4. Click **Client Scopes**.
5. Under the **Mappers** tab, add the role list mapper by clicking **Add Mapper** under the clientId-dedicated scope.
6. Provide **Groups** as **Role attribute name**.
7. Enable **Single Role Attribute**.
8. Under the **Scope** tab, enable **Full scope allowed**.

Adding Users and Mapping the Users to the SAML Client Role

To add users and map them to the SAML client role:

1. Log in to KeyCloak and switch to your realm.
2. Click on the **Users** tab.
3. Click **Add User** to create users in keycloak.
4. Add UIM Embedded LDAP and External LDAP users.
5. Map the users to the SAML client role as follows:
    a. Click on the user you created, under the **Users** tab.
    b. Click **Role Mapping** and then **Assing Role.**
    c. Switch to **filter by clients** and search for the **uim-users** role.
    d. Select the **uim-users** role and click **Assign.**

Creating OAUTH Client for UTIA and Message Bus

To create OAUTH client for UTIA and Message Bus:

1. Log in to KeyCloak and switch to your realm.
2. Click on the **Clients** tab.
3. Click **Create Client**.
4. Choose **client type** as **OpenID Connect**.
5. Provide **client id** of your choice. For example: **topologyOauthClient**.
6. Click **Next**.
7. Enable **client Authentication** and select **Standard Flow**, **Direct access grants**, and **Service accounts roles**.
8. Click **Next**.
9. Add the following **Valid redirect URIs** :
    - https://<unified-topology-hostname>:<loadbalancer-port>/topology
    - https://<unified-topology-hostname>:<loadbalancer-port>/redirect/unified-topology-ui
10. Add `https://<topology-hostname>:<loadbalancer-port>/apps/unified-topology-ui` as **Valid post logout redirect URIs**.
11. Click **Save** and verify the client configuration.

Configuring the Client Scope and Audience

To configure the client scope and audience:

1. Log in to KeyCloak and switch to your realm.
2. Click **Client Scopes**.
3. Click **Create Client Scope**.
4. Provide the name as **utiaScope**.
5. Enter the protocol as **OpenID Connect**.
6. Enable the **Include in token scope**.
7. Click **Save**.
8. Go to **Mappers** and then **configure a New Mapper**.

9. Choose the Mapper type as **Audience**.
10. Provide a **Name** and **Included Custom Audience** as **utiaAudience**.
11. Enable **Add to access token**.
12. Click **Save**.

Adding Scope to the Client

To add scope to the client:

1. Log in to KeyCloak and switch to your realm.
2. Click on the **Clients** tab.
3. Click on your OIDC client. For example: **topologyOauthClient**.
4. Click on the **Client Scope** tab.
5. Choose the above created Scope (**utiaScope**) by clicking **Add Client Scope** .
6. Click **Save**.

Getting OpenID Endpoint Configurations

To get **OpenID** endpoint configurations:

1. Log in to KeyCloak and switch to your realm.
2. Click on the realm settings.
3. Click **OpenID Endpoint Configuration**.
   The OpenID endpoint configurations appear.

Configuring Message Bus and UTIA with OAUTH Client

To configure Message Bus and UTIA with OAUTH client:

1. Create the **oauthConfig** secret.

> **Note:**
>
> See the **Enabling Authentication for UTIA and Message Bus** section from *Unfied Inventory and Topology Deployment Guide*, for more information.

2. Create aapUIUser secret and aapUser Secret for topology UI and API.

> **Note:**
>
> See the **Creating Secrets for Authentication on Unified Topology UI** and **Creating Secrets for Authentication on Unified Topology API** sections in *Unified Inventory and Topology Deployment Guide* for more information.

3. Add **openid** as an additional base scope in the **topology-ui-user-credentials.yaml** and **topology-user-credentials.yaml** files. For example, the base scope must be as follows:

   ```
   base-scope: "utiaScope openid"
   ```

4. Use the client ID and client secret of **topologyOauthClient** for the above steps and for all endpoint URLs.

> **Note:**
>
> See Getting OpenID Endpoint Configurations for more information.

Integrating UIM with UTIA and Message bus

To integrate UIM with UTIA and Message bus:

1. See the **Integrating UIM with UTIA and Message Bus** section from *Unified Inventory and Topology Deployment Guide* and use the appropriate values configured through KeyCloak IDP.
   The sample properties for KeyCloak IdentiyGaurd Realm are as follows:

   ```
   Client Id : topologyOauthClient
   Client Secret: xxxxxxxxxxxxxx
   Client scope: utiaScope
   Client Audience: utiaAudience
   ```

> **Note:**
>
> These are OpenID connect values.

2. Use the endpoint URLs mentioned in your realm. See "Getting OpenID Endpoint Configurations" for more information.