Oracle® Fusion Applications

Installation Guide

11*g* Release 8 (11.1.8)

E16600-31

June 2014

Documentation for installers that describes Oracle Fusion Applications provisioning and discusses how its inter-related components orchestrate the installation, configuration, and deployment of Oracle Fusion Applications product offerings and the Oracle Fusion Middleware technology stack.

ORACLE

Oracle Fusion Applications Installation Guide, 11*g* Release 8 (11.1.8)

E16600-31

Primary Author: Anupama Pundpal

Contributor: Amy Lodato, Shelly Butcher, Karen Ram, Bor-Ruey Fu, Ronaldo Viscuso, Bill Jacobs, Jennifer Briscoe, Henriette Fux, Vickie Laughlin, Ellen Desmond,Vadim Milman, P.S.G.V.Sekhar, Nancy Schwab, Essan Ni, Subodh Nimbkar, Shankar Raman, Jatan Rajvanshi, Janga Aliminati, Michael Rhys, Pradeep Bhat, Bruce Jiang, Xiao Lin

Contents

2 Understanding What the Oracle Fusion Applications Environment Looks Like

6 Installing the Oracle Identity Management and Oracle Fusion Applications Provisioning Frameworks

9 Troubleshooting Database Installations

Part V Provisioning Oracle Identity Management

10 Oracle Identity Management Provisioning

11 Troubleshooting Oracle Identity Management Provisioning

14 Troubleshooting Your Oracle Fusion Applications Environment

Part VII Completing Oracle Fusion Applications Post-Installation Tasks

15 Completing Mandatory Common Post-Installation Tasks

16 Completing Conditional Common Post-Installation Tasks

17 Completing Conditional Common High Availability Post-Installation Tasks for Oracle Identity Management

18 Completing Conditional Common High Availability Post-Installation Tasks for Oracle Fusion Applications

19 Completing Oracle Fusion Customer Relationship Management Post-Installation Tasks

20 Completing Oracle Fusion Financials Post-Installation Tasks

Preface

The *Oracle Fusion Applications Installation Guide* provides information about setting up Oracle Fusion Applications Provisioning and using it to install and provision a new Oracle Fusion Applications environment. It includes specific instructions for installing prerequisite components; installing, configuring, and deploying applications product offerings; and deinstalling an environment.

> **Note:** If you are using Oracle VM environments, see the *Oracle Fusion Applications Installing and Managing in an Oracle VM Environment*. This guide describes how to install, configure, and manage instances of Oracle VM environments created from the Oracle VM templates for Oracle Fusion Applications. This document is applicable for the environments created from the official releases of Oracle VM templates for Oracle Fusion Applications Release 2 (11.1.2) and higher. The content is not applicable for any Oracle VM environments that are created using other methods.

Audience

This document is intended for users who are provisioning an Oracle Fusion Applications environment and installing product offerings for the first time and who are comfortable with system administration tasks such as installing Oracle Identity Management, setting up and configuring Oracle Database 11*g* (11.2.0.3), and applying patches on the computer where the product offerings will be installed. Users installing on a UNIX system need `root` access to run some of the scripts.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following documents:

- *Oracle Fusion Applications Installation Workbook*
- *Oracle Fusion Applications Administrator's Guide*
- *Oracle Business Intelligence Applications Installation Guide*
- *Oracle Database Installation Guide* for your platform
- *Oracle Fusion Applications Common Implementation Guide*
- *Oracle Fusion Applications Patching Guide*
- *Oracle Fusion Applications Upgrade Guide*
- *Oracle Fusion Applications Installing and Managing in an Oracle VM Environment*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in This Guide

This preface introduces the new and changed installation features of Oracle Fusion Applications that are described in this guide, and provides pointers to additional information.

New and Changed Features for 11*g* Release 8 (11.1.8)

Oracle Fusion Applications 11*g* Release 8 (11.1.8) includes the following new and changed features for this document.

- This document has been restructured and now includes the following new chapters:
  - Part I, "Introduction to Installing Oracle Fusion Applications"
  - Part II, "Planning an Oracle Fusion Applications Installation"
  - Chapter 6, "Installing the Oracle Identity Management and Oracle Fusion Applications Provisioning Frameworks"
  - Chapter 7, "Installing Databases for Oracle Identity Management"
  - Chapter 9, "Troubleshooting Database Installations"
  - Chapter 10, "Oracle Identity Management Provisioning"
  - Chapter 11, "Troubleshooting Oracle Identity Management Provisioning"
  - Part VII, "Completing Oracle Fusion Applications Post-Installation Tasks"
- The following chapters have been updated:
  - Chapter 5, "Preparing for an Installation"
  - Chapter 8, "Installing Oracle Fusion Applications Transaction Database"
  - Chapter 12, "Creating a Response File"
  - Chapter 13, "Provisioning a New Oracle Fusion Applications Environment"
  - Chapter 14, "Troubleshooting Your Oracle Fusion Applications Environment"
  - Chapter 27, "Uninstalling an Oracle Fusion Applications Environment"
- Added new section for troubleshooting postconfigure phase errors. See Section 14.8.
- Added a new section for instructions related to increasing the maximum number of user processes. See Section 5.3.2.2.

- Added a note for details related to schema password complexity rules. See Section 8.6.2.2.1.
- The Oracle Label Security database option is no longer required. Starting with this release, if you are installing Oracle database manually for Oracle Fusion Applications, you do not need to enable Oracle Label Security option in order to run Oracle Fusion Applications RCU. Deleted Oracle Label Security information from Section 8.2.2.1 and Section 8.4.2.1.1.
- Added note related to installing databases. See Section 8.1.

Part I

Introduction to Installing Oracle Fusion Applications

This part provides an overview of the process of installing and provisioning Oracle Fusion Applications, and an introduction to the environment as it appears after provisioning has completed.

Part I contains the following chapters:

1 Overview

This chapter introduces Oracle Fusion Applications Provisioning and discusses how its interrelated components orchestrate the installation, configuration, and deployment of Oracle Fusion Applications database, product offerings and their middleware dependencies.

It includes the following sections:

1.1 Introduction to Installing Oracle Fusion Applications

Provisioning is the entire set of operations required to install, configure, and deploy applications product offerings from a system point of view. It performs these operations:

- Installation provides the operations related to laying down all the component needed to create an Oracle Fusion Applications environment
- Configuration tailors components based on the applications topology, the creation of Oracle WebLogic Server Managed Servers and clusters, and the updating of endpoints and virtual hosts
- Deployment starts the Managed Servers and clusters and facilitates the actual use of product offerings

This orchestration by a single processing engine ensures that all components interact smoothly and consistently in the applications environment.

The main tasks to be completed when provisioning an Oracle Fusion Applications environment are:

- **Planning**: The first step to provisioning an Oracle Fusion Applications environment is planning the environment, specifically its topology, including the number and configuration of hardware units; and its components, including: storage, network, database, Oracle Identity Management, and security configuration. For more information, see Part II, "Planning an Oracle Fusion

Applications Installation".

- **Preparing**: Prior to provisioning an Oracle Fusion Applications environment, hardware and networking components must be prepared and configured, shared disk storage must be set up. The relevant software dependencies must be installed. For more information, see Part III, "Preparing to Provision Oracle Fusion Applications".
- **Installing Databases**: The next step is installing the databases for Oracle Fusion Applications, including the Oracle Identity Management and Oracle Fusion Applications transaction databases. Repository creation utilities are provided to help create the repositories required for a Oracle Fusion Applications environment. For more information, see Part IV, "Installing the Databases".
- **Provisioning**: After the environment has been planned, prepared, and the relevant databases installed, it is time to provision the Oracle Identity Management and Oracle Fusion Applications environments. The provisioning process installs and configures Oracle Identity Management and Oracle Fusion Applications and all their related components, such as the product offerings you wish to install and the applications used to manage, monitor, and troubleshoot your Oracle Fusion Applications environment. Provisioning frameworks are installed to help accomplish this task. For more information, see Part V, "Provisioning Oracle Identity Management" and Part VI, "Provisioning Oracle Fusion Applications".
- **Completing Post-Install Tasks**: Having provisioned a working Oracle Fusion Applications environment, the next step is completing a set of post-installation tasks. These tasks include a number of required an optional steps, and specific steps required for particular product offerings. For more information, see Part VII, "Completing Oracle Fusion Applications Post-Installation Tasks".

The process of provisioning is undertaken by a team composed of various specialists and technicians, each taking on different roles and responsibilities, as discussed in greater detail in Section 1.2, "Roles and Responsibilities." All told, a typical installation and provisioning process can take about five to fourteen days, not counting post-installation tasks.

1.2 Roles and Responsibilities

There are a number of roles and responsibilities to be undertaken in the context of provisioning Oracle Fusion Applications. These include the following:

- Business sponsor
- Project manager
- IT director
- Architect
- System administrator
- Network engineer
- Database administrator
- Oracle Identity Management and security specialist
- Oracle Fusion Applications technical lead or system administrator
- Oracle Fusion Applications functional lead
- Oracle Fusion Applications developer

- Oracle Business Intelligence and DW reporting specialist
- Support technician
- Oracle Fusion Applications system integrator

Some of these roles may overlap, and you may want to have the same individual fulfill more than one role. For example, many Oracle Fusion Applications technical leads are also database administrators, and an IT director may also act as the project manager for the duration of an Oracle Fusion Applications deployment. Similarly, Oracle Fusion Applications technical leads may inherit support technician duties after most of the deployment tasks have been completed.

On the other hand, it is common to have a number of people on call to fulfill a particular role. For example, it is typical to have a pool of system or database administrators on call at all times during the course of a deployment, as it is critical for back-end systems to be available and responsive so as to complete technical setup and configuration. For training purposes, several individuals may share principal Oracle Fusion Applications technical or functional Lead responsibilities among themselves.

The mapping of deployment tasks and responsibilities to organizational roles may vary across different types of enterprises depending on corporate culture and organizational structure.

1.2.1 Business Sponsor

The business sponsor is responsible for the Oracle Fusion Applications deployment, and determines the business needs to be met by the deployment. As a business sponsor, you work with Oracle to determine licensing, sizing, functional requirements, and selecting Oracle Fusion Applications components. You also work with systems integrators who assist you with deployment and functional setup.

In the context of your organization, you determine the budget, scheduling, resource allocation, and staffing for the deployment and ongoing support after rolling out the system.

Your primary tasks are as follows:

- Communicating requirements, licensing, sizing
- Budgeting
- High level scheduling
- Managing system interfaces (functional)
- Staffing and project management
- Filling out the Oracle Fusion Applications Offerings tab in the *Oracle Fusion Applications Installation Workbook* .

1.2.2 Project Manager

As a project manager, you are responsible for the day-to-day management of the deployment on several levels. This mainly involves reconciling the aggressive schedules set by business sponsors with the realities of staffing resources.

Your tasks include creating and managing the detailed project schedule, breaking down sets of tasks, and assigning them to team members acting in specialized functional roles. Daily project management requires you to monitor successful task completion against milestone targets identified in the project schedule. You may need to re-allocate resources to keep the deployment project on schedule. You may also

need to adjust the project schedule on occasion due to unexpected events or changes in staffing resources.

Your primary tasks are:

- Coordinating among staff performing technical and functional roles
- Building the project time line and task list
- Monitoring completed tasks against the project time line
- Project status reporting
- Managing the completion of the *Oracle Fusion Applications Installation Workbook*

1.2.3 IT Director

As an IT director, you oversee and prioritize all past, present, and future IT projects. You work closely with business sponsors to assess organizational needs and the importance of the Oracle Fusion Applications deployment relative to other ongoing projects. You must also coordinate resource allocations and staffing requirements with the project manager.

Your primary tasks are:

- Managing the following:
  - Staffing and resource allocations
  - Budgeting
  - System interfaces
- Managing licensing and sizing
- Project management
- Making topology decisions
- Coordinating the completion of the *Oracle Fusion Applications Installation Workbook*

1.2.4 Architect

As an enterprise architect, your job straddles the middle ground between fulfillment of business requirements and technical implementation. You are responsible for making most of the key technical decisions after consulting with IT specialists in the system administration, networking, security, and database roles.

Along with the system administrator, your task is to to ensure the technical correctness and completeness of the system in its entirety, including the base Oracle Fusion Applications installation and all extensions, customizations, and integrations with other external systems.

Your primary tasks are:

- Making topology decisions
- Managing system interfaces
- Delineating security requirements
- Filling out the following tabs in the *Oracle Fusion Applications Installation Workbook*:
  - General tab: Environmental Information
  - Offerings tab: Post-Install Tasks

  - Topology & Components tab: Topology
  - Topology & Components tab: Component Assignment
  - Virtual Hosts tab: All

1.2.5 System Administrator

As a system administrator, you are responsible for the critical hardware and operating system layers of the Oracle Fusion Applications deployment. Your task is to ensure that all hardware meets with organizational standards and, along with the architect, that operating systems are configured in accordance with Oracle Fusion Applications requirements.

You are also responsible for overall systems testing, and coordinating all necessary system and subcomponent migrations from testing to QA, and, finally, production platforms.

Your primary tasks are:

- Procuring and setting up hardware
- Installing and configuring operating systems
- Filling out the following tabs in the *Oracle Fusion Applications Installation Workbook*:
  - Topology & Components tab: All
  - Storage tab: All
  - Ports tab: All

1.2.6 Network Engineer

As a network engineer, you are responsible for the setup and ongoing maintenance and monitoring of all components that facilitate communication among computers within the enterprise computing infrastructure. Your tasks include the configuration and setup of machine interfaces such as hosts tables, network cards, network interfaces, IP address allocations, and network equipment such as switches, routers, gateways, and load balancers.

Your primary tasks are:

- Setting up and configuring machine interfaces and network equipment
- Monitoring and maintaining the network infrastructure
- Filling out the following tabs in the *Oracle Fusion Applications Installation Workbook*:
  - General tab: Email Server
  - General tab: Web Proxy
  - Topology and Components tab: Topology
  - Virtual Hosts tab: All
  - Storage tab: All
  - Ports tab: All

1.2.7 Database Engineer

Your task is to manage the database layer of the Oracle Fusion Applications deployment, and fill out the Database tab in the *Oracle Fusion Applications Installation Workbook*.

1.2.8 Oracle Identity Management and Security Specialist

As a security specialist, your job is to create and maintain policies to protect corporate data and computing resources from a variety of real and potential threats.

In the context of Oracle Identity Management, your tasks include creating and managing the enterprise computing components that authenticate, authorize, and account for individual access to computing resources and systems. You may also control the corporate LDAP directories and their associated AAA systems.

Oracle Fusion Applications deployments require creating and configuring identity and policy stores that may differ from pre-existing Oracle Identity Management components in the enterprise. As such, you must coordinate the effort to install and manage Oracle Identity Management components bearing in mind the effects the new components may have on existing components in the enterprise.

Your primary tasks are:

- Creating and managing authentication and authorization enterprise computing components
- Creating and configuring identity and policy stores for Oracle Identity Management, in conjunction with existing Oracle Identity Management components
- Managing security certificates
- Managing password policies (functional security)
- Managing roles and responsibilities (functional setup)
- Managing system account password maintenance policies
- Setting up the database (Vault, if applicable)
- Filling out the following tabs in the *Oracle Fusion Applications Installation Workbook*:
  - Offerings tab: Oracle Identity Management Products
  - Virtual Hosts tab: IDM, LDAP
  - IDM tab: All
  - SSL tab: SSL & Certificates
  - DMZ Topology Decisions
  - Web Proxy

1.2.9 Oracle Fusion Applications Technical Lead or System Administrator

As an Oracle Fusion Applications technical lead, you work closely with other IT specialists, including the database, network, and system administrators as they install and configure the Oracle Fusion Applications infrastructure. Your main responsibility is the hands-on management of low-level tasks to be completed during technical setup and validation.

Your primary tasks are:

- Managing technical setup and validation tasks during Oracle Fusion Applications deployment
- Managing system interfaces

1.2.10 Oracle Fusion Applications Functional Lead

As the Oracle Fusion Applications functional lead, you are responsible for the functional setup of Oracle Fusion Applications following the completion of its technical deployment. You work closely with the business sponsor to ensure the system is configured in accordance with business requirements, and with technical leads and architects to ensure the successful completion of post-installation tasks.

It is useful to have a background in performing systems integration and specializing in the Oracle Fusion Applications pillars being installed and configured.

- Managing the functional setup of Oracle Fusion Applications
- Managing system interfaces
- Filling out the following tabs in the *Oracle Fusion Applications Installation Workbook* :
  - Offerings tab: Post-Install Tasks

1.2.11 Oracle Fusion Applications Developer

As an Oracle Fusion Applications developer, you are responsible for extending or customizing Oracle Fusion Applications pillars to meet specific enterprise business requirements. Typically, Oracle Fusion Applications are customized and extended after the provisioning the installation. However, it may be useful to participate in provisioning so as to establish continuity between the installation and customization.

1.2.12 Oracle Business Intelligence or Data Warehouse Reporting Specialist

If your organization's particular Oracle Fusion Applications deployment requires reporting and data warehouse capabilities, you may have a primary role in the technical deployment. Your expertise will mostly be required for the functional setup of the project, after reporting requirements have been determined and implemented.

Your primary tasks are:

- Depending on the requirements of your organization, assisting in the technical deployment and functional setup
- Filling out the following tabs in the *Oracle Fusion Applications Installation Workbook*:
  - Databases tab: Oracle Fusion Applications Data Warehouse Database

1.2.13 Support Technician

As a support technician, your primary responsibility is to assist end users with any computing applications in the enterprise. The Oracle Fusion Applications deployment is usually one of many systems you might cover.

Many organizations have technical and functional areas of specialization within the support technician role.

1.2.14 Oracle Fusion Applications Systems Integrator

Some organizations choose to hire Oracle Fusion Applications system integrators on a consulting basis who can fill gaps in technical expertise when necessary. Depending on

your enterprise and the scope and scale of your deployment, you may choose to hire an external Oracle Fusion Applications system integrator for a short or long period. Ideally, the systems integration consulting team will be able to transfer substantial knowledge to support staff.

1.3 Prerequisites and Dependencies

The following prerequisites are needed before provisioning an Oracle Fusion Applications environment:

- Oracle Database
- Oracle Identity Management
- Oracle Business Intelligence

1.3.1 Oracle Database

You must have installed and configured a transaction database before you install product offerings. You can use the Provisioning Wizard to create an empty, single-instance database instance. This is a discrete and separate task from the other provisioning options. Alternatively, you can install the database manually without using the wizard.

In either case, you finish the database installation by running the Oracle Fusion Applications Repository Creation Utility (Applications RCU) to load applications and middleware content into the database. This process creates the applications and middleware schemas, loads seed data, and creates the tablespaces, as well all other required packages.

1.3.2 Oracle Identity Management

Oracle Identity Management is a core component and prerequisite for provisioning an Oracle Fusion Applications environment. It enables enterprises to manage the end-to-end life cycle of user identities across all enterprise resources — both within and beyond the firewall. An installation of Oracle Fusion Applications relies on Oracle Identity Management components to provide web Single Sign-on capability and to act as the policy, credential, and identity store. Although the majority of these components fall within the prerequisite environment, the resource WebGate that acts as the proxy for user authentication must be provisioned along with the applications.

The Oracle Identity Management components required to be present in an Oracle Fusion Applications environment are:

- Oracle Identity Manager (OIM): Provides identity administration, user self-service, and self-registration
- Oracle Access Manager (OAM): Manages authentication and authentication policies, including Oracle Single Sign-On, security functions, user self-service, policy management, and delegated administration
- Oracle Virtual Directory (OVD): A Lightweight Directory Access Protocol (LDAP)-enabled service that provides a virtualized abstraction of one or more enterprise data sources in a single directory view
- Oracle Internet Directory (OID): A general-purpose directory service that enables fast retrieval and centralized management of information about dispersed users and network resources

1.3.3 Oracle Business Intelligence

Oracle Business Intelligence is a portfolio of technology and applications comprising an integrated toolset (for querying, reporting, analysis, alerts, mobile analytics, data integration and management, and desktop integration), as well as financial performance management, applications, operational business intelligence applications, and data warehousing.

Typically, Oracle Business Intelligence products are integrated with, and accessible from, other operational applications, such as Oracle Fusion Applications. This integration provides business metrics in the context of an organization's business function and industry.

The Oracle Business Intelligence products integrated with Oracle Fusion Applications include:

- Oracle Business Intelligence Enterprise Edition (Oracle BI EE): A suite of business intelligence tools that delivers a full range of analytic and reporting capabilities.

  Oracle Business Intelligence Enterprise Edition is installed and provisioned as part of the Oracle Fusion Applications installation and provisioning process. The BI Provisioning step creates a WebLogic domain, the BI Web application (J2EE) components, and the BI Server and BI Presentation Services, which are deployed on the computer that hosts the domain. The resulting environment is referred to as the "Business Intelligence domain" or "BI Domain."

- Oracle Business Intelligence Applications: Uses Oracle Business Analytics Warehouse, a unified data repository for all customer-centric data that supports the analytical requirements of Oracle Business Intelligence Applications. Oracle Business Intelligence Applications supplies the warehouse database schema, as well as the logic that extracts data from the Oracle Fusion Applications transactional database and loads it to the warehouse.

  The Oracle Fusion Applications installation and provisioning process installs the Oracle BI Applications software components in the Business Intelligence Oracle Home but does no further setup. To finish setting up Oracle BI Applications, you must follow the instructions in the "Functional Configuration for Oracle Business Intelligence Applications" section of the *Oracle Business Intelligence Applications Configuration Guide*.

- Oracle Transactional Business Intelligence: An ad hoc query and self-service reporting solution offered to all Oracle Fusion Applications customers. Paired with Oracle BI EE, it provides business users with an easy-to-use interface for performing current state analysis of their business applications. Constructed queries and reports are executed in real time against the transactional schema supported by a layer of view objects. This product is configured and deployed during provisioning.

- Oracle Essbase: An online analytical processing (OLAP) server that provides an environment for deploying prepackaged applications or developing custom analytic and enterprise performance management applications.

- Oracle Business Intelligence Publisher: An enterprise reporting solution for authoring, managing, and delivering reports from multiple data sources in multiple formats via multiple channels.

  For more information, see the "Managing Report Delivery Servers" chapter of *Oracle Fusion Applications Administrator's Guide*.

- Oracle Real-Time Decisions: A platform that combines both rules and predictive analytics to apply real-time business intelligence at the point of contact. It

optimizes all interactions with your customers by infusing analytical decisions into each transaction.

For more information, see *Oracle Fusion Middleware Administrator's Guide for Oracle Real-Time Decisions*.

1.4 Features of Provisioning

Oracle Fusion Applications Provisioning is a full-featured process that provides all the tools you need to set up a repository of installers and installation-related processes, present product configurations that you can install in your environment, provide a means to collect configuration details about those offerings, and run the installation phases necessary to perform configuration and deployment tasks.

1.4.1 Oracle Fusion Applications Provisioning Repository

The Oracle Fusion Applications software provides a repository of installers, each called silently when needed to perform application-specific tasks during the provisioning of your new environment. During the creation of your response file, you indicate the location of the repository in the Provisioning Wizard interview.

The provisioning repository must be on a network drive that is visible to all hosts that you will associate with your Oracle Fusion Applications environment. See Section 5.5 for details.

1.4.2 Oracle Fusion Applications Provisioning Framework

The provisioning installer (`faprov`) creates the Oracle Fusion Applications Provisioning framework. It includes the following components:

- **Provisioning Wizard**: A question-and-answer interview that guides you through the process of installing a database, creating or updating a response file, and installing or deinstalling the components of an Oracle Fusion Applications environment. You can only use Provisioning Wizard on the database host to install a single instance database, or on the primordial host (refer to Section 1.5.1) for the other provisioning options such as creating a response file, updating a response file, provisioning an applications environment and deinstalling an applications environment.
- **Provisioning Command-Line Interface (CLI)**: Used for starting the provisioning wizard and running installation phases on the primary, secondary, and DMZ hosts (when present). You can also use provisioning CLI on the primordial host for manual cleanup and restore, and for running provisioning phases as needed.
- **Provisioning-related files and utilities**: Repository of ANT utilities, binary files, library files, templates, locations of saved response files and provisioning build scripts, and other provisioning utilities required for performing provisioning tasks. These utilities are installed in a location you choose, for example, *`framework_location`*`/provisioning`.

See Chapter 6, "Installing the Oracle Identity Management and Oracle Fusion Applications Provisioning Frameworks" for details.

1.4.3 System Requirements

This release of Oracle Fusion Applications relies on supported platforms documentation for Oracle Fusion Applications to supply certified versions of Oracle components. This documentation provides details about hardware and software,

minimum disk space and memory requirements, required system libraries, packages, or patches, and minimum database requirements. Consult an Oracle Fusion Applications sizing-certified representative to obtain specific, customized system hardware requirements.

> **Note:** The self-signed certificate is set to three years when provisioning is complete.

1.4.3.1 Download Instructions

If you are downloading Oracle Fusion Applications 11g Media Pack for the following platforms, then use the following version (and above) of the UnZip / 7-Zip utility to extract the Oracle software to a location of your choice (*REPOSITORY_LOCATION*). UnZip is freeware that is available at: `http://www.info-zip.org`. Oracle has also made copies available for most commonly used platforms at: `https://updates.oracle.com/unzips/unzips.html`.

- Linux x86-64 (64-bit) - Info-ZIP version 6.0
- Oracle Solaris on SPARC (64-bit) - Info-ZIP version 6.0
- Oracle Solaris on x86-64 (64-bit) - Info-ZIP version 6.0
- IBM AIX on POWER Systems (64-bit) - Info-ZIP version 6.10
- Microsoft Windows x64 (64-bit) - 7-Zip version 9.20

1.4.4 Supported Platforms

Oracle Fusion Applications is supported on the following platforms:

- Linux x86-64 (64-bit)
- Oracle Solaris on SPARC (64-bit)
- Oracle Solaris on x86-64 (64-bit)
- IBM AIX on POWER Systems (64-bit)
- Microsoft Windows x64 (64-bit)

As the Oracle Fusion Applications 11g Media Pack is specific for a platform, you must install Oracle Fusion Applications on the same platform. This includes the Oracle Database, Oracle Identity Management, and Oracle Fusion Applications.

1.4.5 Oracle Identity Management Provisioning Wizard

The Oracle Identity Management Provisioning Wizard steps you through all Identity Management provisioning tasks. Using the wizard, you can create or update a response file, configure the Identity Management environment, install an Identity Management database, and configure a load balancer.

The wizard allows you to accomplish the following tasks.

- **Response File Creation**. You must create a response file before provisioning the Identity Management environment. You can use a pre-existing response file, if one exists, or create a new one. Response file information includes the name, version, creation date, and so on.
- **Install Location Configuration**. Specify the software repository and installation locations, as well as the shared configuration location.

- **Node Topology Configuration**. Select Identity Management node configuration options and provide information about hosts and products.
- **Virtual Hosts Configuration**. Configure virtual hosts for the Identity Management servers, as required for Oracle Fusion Applications.
- **Common Passwords**. Set the common password for all administrative Identity Management users and keystores.
- **Oracle Internet Directory Configuration**. Specify the distinguished name of the Oracle Internet Directory realm.
- **Oracle Directory Services Manager Configuration**. Select configuration options for Oracle Directory Services Manager (ODSM).
- **Oracle HTTP Server for Identity Management Configuration**. Change the installation ports used for Oracle HTTP Server (OHS).
- **Oracle Identity Manager Configuration**. Use the OIM Configuration Page to modify the ports used by Oracle Identity Manager and, optionally, to configure an email server.
- **Oracle Access Manager Configuration**. Use the OAM Configuration Page to select installation options for Oracle Access Manager.
- **SOA Configuration**. Use the SOA Configuration Page to enter the ports to be used by the SOA managed servers.
- **Oracle Internet Directory Identity Store Database configuration**. Use the OID Identity Store DB Configuration Page to enter the database connection details for your Oracle Internet Directory Database.
- **Oracle Identity Manager Database Configuration**. Use the OIM DB Configuration Page to enter information about the Database that contains the schemas for Oracle Identity Manager, SOA, Oracle Access Manager, and Oracle Identity Federation.
- **Load Balancer Configuration**. Configure the load balancer for multiple host installations.

1.4.6 Oracle Fusion Applications Provisioning Wizard

The Provisioning Wizard steps you through all provisioning-related tasks. Using the wizard, you can install a transaction database, create or update a response file, provision a new environment, and deinstall an applications environment.

- **Install an Applications Transaction Database**. You must install a database to hold transactional data *before* you create a response file. Then, you enter the database configuration values set up during the database installation in your response file. The provisioning process uses those values to connect your database to the new applications environment. Complete the process by running Oracle Fusion Applications RCU to create schemas and tablespaces, load seed data, and perform other database configuration tasks.
- **Create a New Applications Environment Response File**. A response file is a provisioning configuration file containing information about credentials, applications, and middleware hosts; used to install a new environment. You specify the location of this response file when you are ready to provision your new environment. The wizard also allows you to update an existing response file.

- **Update an Existing Response File**. Select this option to add or change the details in a partially completed response file or to update a completed response file that has not yet been used to provision an applications environment.
- **Provision an Oracle Fusion Applications Environment**. Select this option and specify the location of a response file as the first step in initiating the installation, configuration, and deployment of your product offerings. In a multiple host environment, the installation runs on each host individually, in phase order, using a combination of the provisioning wizard and command line interface.
- **Deinstall an Oracle Fusion Applications Environment**. Selecting this option removes all components installed to an existing Oracle Fusion Applications environment using the wizard. You must run this process on all hosts. The wizard does *not* remove the database and LDAP.

1.4.7 Response File

With the Provisioning Wizard question-and-answer interview tool, you specify one or more provisioning configurations and collect details associated with the product offerings in those configurations. These responses are the basis for creating a **response file**. This response file contains the structural outline of the applications environment topology that you are implementing. When you are ready to provision your environment, specify the location of the response file and initiate the installation process.

The wizard interview questions fall into the following general areas:

- Global and contextual
- Database configuration and application dependency
- Shared middleware services

Global and Contextual Questions

These questions set the context and define the focus of the questions to be asked later in the interview. The approach is to progressively refine the scope of the questions, starting with the most generic and narrowing down to a specific path based on the selected provisioning configurations. For example, the **Installation Location** screen captures global information about the location of installation and configuration directories, and the **Database Configuration** screen records information about the transactional database.

Database Configuration and Application Dependency Questions

The interview is tied directly to the provisioning of one or more product configurations. With the product configuration chosen, the interview guides you through the questions related to the product offerings and their dependencies. Dependencies include application and middleware products required by Oracle Fusion Applications, as well as details about your transaction database. For example, the **Domain Topology Configuration** screen collects information about the hosts where domains are to be deployed.

Shared Middleware Questions

At the conclusion of the application interview, you move to interview questions about middleware services that are shared across domains, for example, the **Web Tier Configuration**, **Load Balancer Configuration**, **Web Proxy Configuration**, **Identity Management Configuration**, and **IDM Database Configuration** screens.

1.4.8 Provisioning Configurations

During the creation of a response file, you select one or more offerings in any of the provisioning configurations listed in the wizard interview. During the actual provisioning process, all application and middleware products (components) associated with your selections are installed, configured, and deployed. However, only the Managed Servers for the product offerings that you selected are started.

Later, to start using an offering that was part of your initial provisioning configuration but has not yet been enabled, navigate to the Oracle Fusion Applications Setup Manager and start the Managed Servers for that offering.

For example, in the Oracle Fusion Customer Relationship Management configuration, there are two product offerings: Oracle Sales and Oracle Marketing. If you select only Oracle Sales, the Managed Servers for that offering are started when you provision your new environment. If you later decide to enable Oracle Marketing, you use the Oracle Fusion Applications Functional Setup Manager to do so. There is no need to run provisioning a second time.

See Section 12.1.2 for more information about provisioning configurations.

1.5 Provisioning a Multiple Host Installation

Oracle Fusion Applications must be provisioned on multiple hosts for a production deployment and installed from a shared drive that is accessible to all hosts. To properly install all the necessary components for an applications environment on multiple hosts, you must run the physical installation in phases across all hosts.

1.5.1 Types of Hosts in a Multiple-Host Environment

The classification of hosts in a multiple-host environment determines the order in which you run the installation. The following types of hosts are available.

- **Primordial host**: Location of the common domain, specifically the administration server of the common domain. There is one primordial host in each provisioned environment where the administration server of the common domain will be.
- **Primary host**: Location of the administration server for a domain. Only one primary host exists in a domain.
- **Secondary host**: Location of the managed servers for any application when they are not on the same host as the administration server of the same domain. This term is typically used along with primary host to differentiate the physical hosts when a domain spans across them.
- **DMZ host**: A host that cannot access the shared storage behind the firewall is said to be in a demilitarized zone (DMZ). Typically used to install Oracle HTTP Server so as to enforce restrictions on communication with components behind the firewall.

For information about Oracle Fusion Applications environments, see Section 2.2, "Oracle Fusion Applications Topologies."

1.5.2 Installation Phases

Installation actions are completed in phases, across all hosts, in a prescribed phase order. Each phase must be completed on all hosts before you can run the next phase. For example, you must complete the preverify phase on hosts A, B, and C successfully before you run the install phase on any other host. Any one phase can run

simultaneously on multiple hosts. For example, you can run the install phase on hosts A, B, and C simultaneously. Oracle recommends that you start the installation on the primordial host.

The provisioning installation phases are as follows (listed in phase order). See Section 13.2 for complete details.

- **Preverify**: Checks to see that the prerequisites for an installation are met.
- **Install**: Installs middleware and applications components and applies database patches shipped with provisioning (for databases created with the wizard).
- **Preconfigure**: Updates the Oracle Application Development Framework (Oracle ADF) configuration.
- **Configure**: Creates domains, Managed Servers, and clusters. Configures data sources and performs Node Manager registration of servers on the primordial and primary hosts.
- **Configure-secondary**: Performs the configuration actions on a primary or secondary host (or both), registers Managed Servers with the Node Manager on secondary hosts, and creates a web tier instance. If there are no primary or secondary hosts, or if there are only primary hosts, this phase runs, but takes no action.
- **Post-Configure**: Configures Oracle SOA Suite composite deployment and Oracle HTTP Server, and populates policies and grants. Configures middleware and applications that require servers to be online.
- **Startup**: Starts the Administration Server and Managed Servers on the current host. Performs online configuration, including global unique identifier (GUID) reconciliation and Financial/IPM configuration.
- **Validate**: Validates the deployment configuration and starts the Managed Servers.

1.6 Planning for Provisioning

Before you create a response file for your new Oracle Fusion Applications environment, you should decide what your topology will look like, including what product offerings you want to install, port allocations, and the type and number of hosts that you will configure in the domains created for the product offerings. For example, Oracle recommends that you choose a separate host for each domain that will be installed. However, even in that scenario, some large product configurations must be split across multiple hosts.

You must determine the necessary system requirements to complete the provisioning of a new environment, based on how you will use the environment. For example, if you are installing a single instance database for use as a test system, the requirements will differ from the installation of a multi-instance database to use for your production environment. You must also determine the access privileges for the database administrator (DBA) or system administrator who will perform the provisioning tasks.

You must supply directory locations, user names, and passwords associated with the prerequisite installations of Oracle Database and Oracle Identity Management components. These installations must be completed before you can create a response file.

Note: Note that the Oracle Fusion Applications environment is a fully integrated environment. You should not deploy custom applications in the environment.

1.7 What to Do Next

Following is an overview of the Oracle Fusion Applications provisioning process flow.

Table 1–1 Provisioning Process Flow

Task	Description	Link
Planning	This part describes how to plan the topology and provisioning of your installation, and the configuration of the components of your installation: storage, network, databases, and Oracle Identity Management.	Part II, "Planning an Oracle Fusion Applications Installation"
Preparing for provisioning	This part describes the components required to prepare for provisioning, including storage, servers, the network, and the provisioning repository; and how to install the Oracle Fusion Applications and Oracle Identity Management provisioning frameworks.	Part III, "Preparing to Provision Oracle Fusion Applications"
Installing databases	This part explains how to install and troubleshoot databases for Oracle Identity Management database, the Oracle Fusion Applications transactional databases, and the Oracle Fusion Applications repository.	Part IV, "Installing the Databases"
Provisioning Oracle Identity Management	This part describes how to provision and troubleshoot Oracle Identity Management for basic and enterprise topologies.	Part V, "Provisioning Oracle Identity Management"
Provisioning Oracle Fusion Applications	This part describes how to use the Provisioning Wizard to create a response file, install the provisioning framework, and provision and troubleshoot Oracle Fusion Applications.	Part VI, "Provisioning Oracle Fusion Applications"
Completing Post-Installation tasks	After provisioning the Oracle Fusion Applications installation, you must configure the installed components to suit your business and functional requirements. This part describes the post-installation tasks, both optional and required.	Part VII, "Completing Oracle Fusion Applications Post-Installation Tasks"
Uninstalling	This part explains how to uninstall Oracle Fusion Applications, clean up after uninstalling, deleting the database, and uninstalling the Oracle Fusion Applications Provisioning Framework.	Part VIII, "Uninstalling Oracle Fusion Applications"

You will want to continue to the next chapter, which explains in detail what the provisioned Oracle Fusion Applications environment looks like. It covers topics such as sample topologies, directory structures, and the products to be installed.

2

Understanding What the Oracle Fusion Applications Environment Looks Like

This chapter describes the topology, directory structure, and installed products and components of Oracle Fusion Applications.

It includes the following sections:

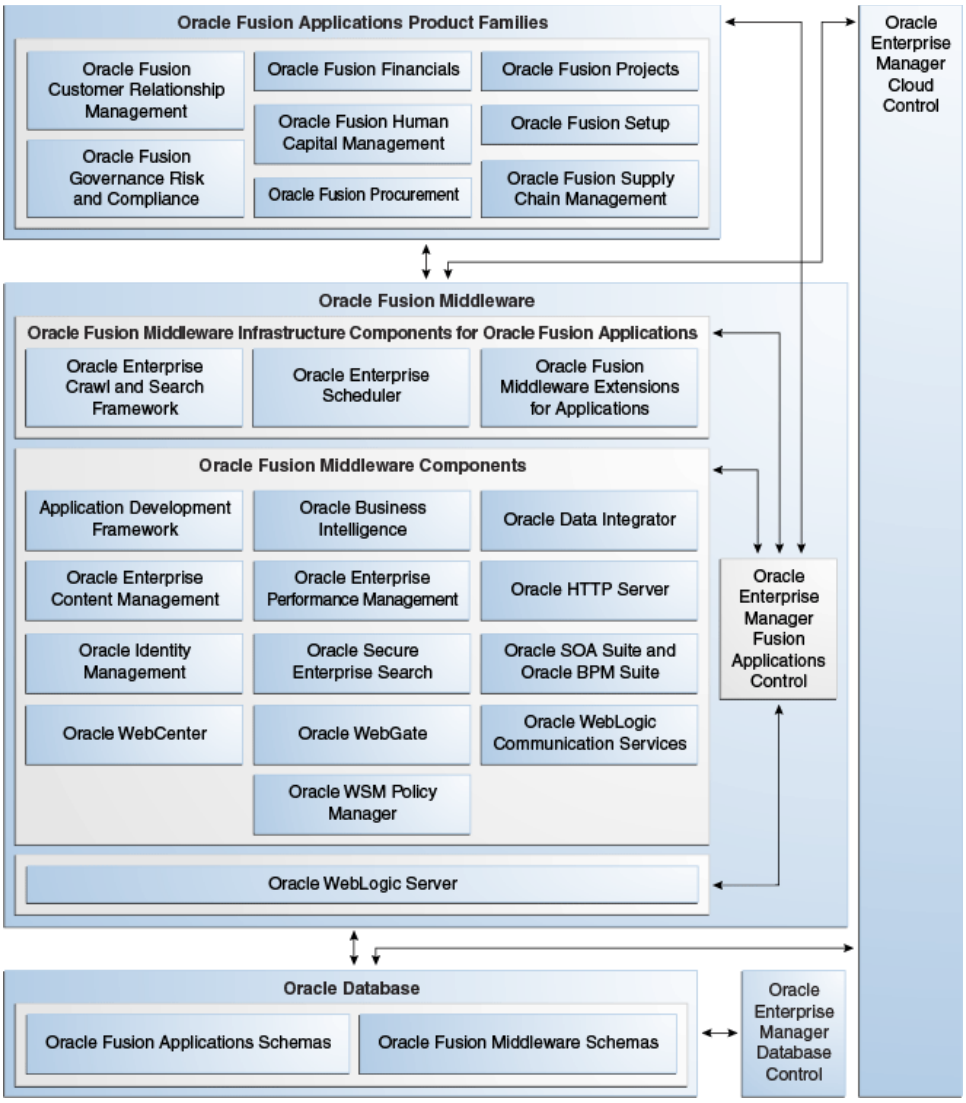
2.1 Introduction to What the Oracle Fusion Applications Environment Looks Like

Once fully installed, the Oracle Fusion Applications environment contains several Oracle as well as third party products which make up its technology stack. Oracle Fusion Applications is built on the Oracle Fusion Middleware stack and uses Oracle Database.

Understanding what the environment will look like after the installation process is complete will help you to better understand the installation process, and plan for the installation so as to fit the environment configuration you desire.

The Oracle Fusion Applications architecture is depicted in the following diagram.

Figure 2–1 Oracle Fusion Applications Architecture



2.1.1 Oracle Fusion Applications Product Families and Product Offerings

An installation of Oracle Fusion Applications is logically broken up into groups of features. Each set of features is known as **product offerings**, which represent the highest-level collection of functionality that you can license and implement. A **product family** is a collection of one or more product offerings. During installation, you select a product offering or a combination of offerings as a way to install the Oracle Fusion Applications products you wish to use.

Product families are dependent on companion applications—for example, Oracle Fusion Human Capital Management relies on Oracle Fusion Financials payroll—and Oracle Fusion Middleware components such as Oracle SOA Suite. The wizard allows for application and middleware configuration at the domain level during domain topology configuration.

When selecting particular product offerings within a configuration rather than all of them, the wizard starts the managed servers only for the selected offerings. However, because the dependency details for the entire configuration are included in the

response file, you can activate additional functionality later using Oracle Fusion Applications Functional Setup Manager to start the other managed servers.

Oracle Fusion Applications includes the product families and product offerings described in the following table.

Table 2–1 Product Offerings

Oracle Fusion Applications Product Families	Oracle Fusion Applications Product Offerings	Description
Oracle Fusion Customer Relationship Management	■ Sales ■ Marketing ■ Customer Data Hub ■ Enterprise Contracts	Manages customers, contracts, and resources, including data quality configuration.
Oracle Fusion Financials	■ Financials ■ Accounting Hub	Manages financial flows, including assets, ledgers, cash cycle, invoices and payments, accounts receivable, collections, and setup of subledger accounting and tax configuration.
Oracle Fusion Governance, Risk, and Compliance (**Not** installed by Oracle Fusion Applications.)	This product family is not installed by Oracle Fusion Applications. Download the software from Oracle Software Delivery Cloud and install it separately.	Provides critical business controls to manage risk, multi-regulatory compliance, and controls enforcement. The connector for Oracle Fusion Applications provides a prebuilt solution for managing Separation of Duties (SoD) within and across product families. You can also use Oracle Fusion Governance, Risk, and Compliance to analyze suspect transactions and configuration settings based on user defined conditions. This allows organizations to actively determine the risk that exists within their application that can materially impact the reliability of the information that exists for reporting and decision making purposes. Finally, Oracle Fusion Governance, Risk, and Compliance can apply preventive controls that will limit what a user can see and do within an Oracle Fusion Applications user interface according to user-defined conditions. The objective is to pro-actively mitigate the risk of extraneous access or improper transactions from existing.
Oracle Fusion Human Capital Management	■ Compensation Management ■ Workforce Development ■ Workforce Development	Provides employee management for an organization.
Oracle Fusion Procurement	Procurement	Manages the procurement process including requisitions, purchase orders, and supplier negotiations.

Table 2–1 (Cont.) Product Offerings

Oracle Fusion Applications Product Families	Oracle Fusion Applications Product Offerings	Description
Oracle Fusion Project Portfolio Management	Projects	Manages projects, including how to plan, budget, forecast, collect costs, bill customers, and report performance.
Oracle Fusion Supply Chain Management	■ Product Management ■ Order Orchestration ■ Material Management and Logistics	Integrates and automates all key supply chain processes, from design, planning and procurement to manufacturing and fulfillment, providing a complete solution set to enable companies to power information-driven value chains.
Oracle Fusion Setup	This product family is installed along with all product offerings.	Supports the other product families. In addition to Oracle Fusion Functional Setup Manager for setting up functional data, this product family includes applications to assist application users: ■ The Oracle Fusion Home page provides a Welcome dashboard with a collection of portlets and task flows for answering common questions. ■ Oracle Fusion Applications Help delivers content users need to complete their tasks. You can optionally install a local version of Oracle Fusion Applications Help, enabling you to extend and customize the help.

Table 2–2 Product Offering and Dependent Weblogic Server Domains

Oracle Fusion Applications Product Families	Oracle Fusion Applications Product Offering	Provisioned Weblogic Server Domains (Primary + Dependent Domains)
Oracle Fusion Customer Relationship Management	Customer Data Management	Oracle Business Intelligence, Common, Oracle Identity Management,Oracle Fusion Customer Relationship Management, Oracle Fusion Financials, Oracle Fusion Human Capital Management
Oracle Fusion Customer Relationship Management	Enterprise Contracts	Oracle Business Intelligence, Common, Oracle Identity Management,Oracle Fusion Customer Relationship Management, Oracle Fusion Financials, Oracle Fusion Human Capital Management
Oracle Fusion Customer Relationship Management	Marketing	Oracle Business Intelligence, Common, Oracle Identity Management,Oracle Fusion Customer Relationship Management, Oracle Fusion Financials, Oracle Fusion Human Capital Management, Oracle Fusion Supply Chain Management

Table 2–2 (Cont.) Product Offering and Dependent Weblogic Server Domains

Oracle Fusion Applications Product Families	Oracle Fusion Applications Product Offering	Provisioned Weblogic Server Domains (Primary + Dependent Domains)
Oracle Fusion Customer Relationship Management	Sales	Oracle Business Intelligence, Common, Oracle Identity Management,Oracle Fusion Customer Relationship Management, Oracle Fusion Financials, Oracle Fusion Human Capital Management, Oracle Fusion Supply Chain Management
Oracle Fusion Incentive Compensation	Incentive Compensation	Oracle Business Intelligence, Common, Oracle Identity Management,Oracle Fusion Customer Relationship Management, Oracle Fusion Financials, Oracle Fusion Human Capital Management, Oracle Fusion Incentive Compensation
Oracle Fusion Financials	Financials	Oracle Business Intelligence, Common, Oracle Identity Management,Oracle Fusion Customer Relationship Management, Oracle Fusion Financials, Oracle Fusion Human Capital Management, Oracle Fusion Project Portfolio Management, Oracle Fusion Supply Chain Management
Oracle Fusion Financials	Fusion Accounting Hub	Oracle Business Intelligence, Common, Oracle Identity Management,Oracle Fusion Customer Relationship Management, Oracle Fusion Financials, Oracle Fusion Human Capital Management
Oracle Fusion Human Capital Management	Compensation Management	Oracle Business Intelligence, Common, Oracle Identity Management,Oracle Fusion Customer Relationship Management, Oracle Fusion Financials, Oracle Fusion Human Capital Management
Oracle Fusion Human Capital Management	Workforce Deployment	Oracle Business Intelligence, Common, Oracle Identity Management,Oracle Fusion Customer Relationship Management, Oracle Fusion Financials, Oracle Fusion Human Capital Management
Oracle Fusion Human Capital Management	Workforce Development	Oracle Business Intelligence, Common, Oracle Identity Management,Oracle Fusion Customer Relationship Management, Oracle Fusion Financials, Oracle Fusion Human Capital Management
Oracle Fusion Procurement	Procurement	Oracle Business Intelligence, Common, Oracle Identity Management,Oracle Fusion Customer Relationship Management, Oracle Fusion Financials, Oracle Fusion Human Capital Management, Oracle Fusion Project Portfolio Management, Oracle Fusion Supply Chain Management

Table 2–2 (Cont.) Product Offering and Dependent Weblogic Server Domains

Oracle Fusion Applications Product Families	Oracle Fusion Applications Product Offering	Provisioned Weblogic Server Domains (Primary + Dependent Domains)
Oracle Fusion Project Portfolio Management	Projects	Oracle Business Intelligence, Common, Oracle Identity Management,Oracle Fusion Customer Relationship Management, Oracle Fusion Financials, Oracle Fusion Human Capital Management, Oracle Fusion Procurement, Oracle Fusion Project Portfolio Management, Oracle Fusion Supply Chain Management
Oracle Fusion Supply Chain Management	Materials Management and Logistics	Oracle Business Intelligence, Common, Oracle Identity Management,Oracle Fusion Customer Relationship Management, Oracle Fusion Financials, Oracle Fusion Human Capital Management, Oracle Fusion Supply Chain Management
Oracle Fusion Supply Chain Management	Order Orchestration	Oracle Business Intelligence, Common, Oracle Identity Management,Oracle Fusion Customer Relationship Management, Oracle Fusion Financials, Oracle Fusion Human Capital Management, Oracle Fusion Supply Chain Management
Oracle Fusion Supply Chain Management	Product Management	Oracle Business Intelligence, Common, Oracle Identity Management,Oracle Fusion Customer Relationship Management, Oracle Fusion Financials, Oracle Fusion Human Capital Management, Oracle Fusion Supply Chain Management

2.1.2 Oracle Fusion Middleware Infrastructure Components

The product families use the following common core framework and infrastructure for Oracle Fusion Applications described in the following table.

Table 2–3 Oracle Fusion Middleware Infrastructure Components

Oracle Fusion Middleware Infrastructure Component	Description
Oracle Fusion Middleware Extensions for Applications (Applications Core)	Provides design time and runtime infrastructure to help standardize complex development patterns for Oracle Fusion Applications. It simplifies the development process of these patterns and provides a consistent user experience. Examples of these patterns include extensibility (Flexfields), hierarchical relationships (Trees), data security, and UI patterns. Applications Core creates simplified methods of implementing these complex requirements by providing robust metadata and comprehensive UI components and services. All of the Applications Core components have been intricately integrated with the rest of the Oracle Fusion Middleware infrastructure so they are available across every layer of the Oracle Fusion Applications platform. Applications Core provides shared libraries referenced by all the Oracle Fusion Applications, a standalone application for application setup and configuration, an Oracle JDeveloper extension to seamlessly integrate our components with the rest of the Oracle Fusion Applications technology stack, PLSQL APIs, C libraries, and common seed data.
Oracle Enterprise Scheduler	Enables you to manage and schedule jobs for Oracle Fusion Applications.
Oracle Enterprise Crawl and Search Framework (ECSF)	Oracle Enterprise Crawl and Search Framework (ECSF) enables Oracle Fusion Applications Search for performing full-text searches securely and simultaneously against multiple logical business objects. Any application that connects to multiple data sources or manages a significant amount of unstructured (non-database) information—or both—needs advanced search capabilities so that application users can easily locate and take action on data that is relevant to them.

2.1.3 Oracle Fusion Middleware Components

A complete installation of Oracle Fusion Applications includes several Oracle and third party products. The majority of installed products form the core of the Oracle Fusion Applications environment, and are installed regardless of the offerings selected during provisioning. Some products are installed only when selecting particular product offerings, while others must be installed manually following provisioning.

Oracle Fusion Middleware includes the components described in the following table.

Except where otherwise stated, all products are installed during Oracle Fusion Applications provisioning and are enabled by default.

> **Note:** Install Oracle Database Server before running Oracle Fusion Applications provisioning.
>
> Before you run the Oracle Identity Management Provisioning Wizard, install Oracle JRockit JDK and Oracle Database Server and run the Oracle Fusion Middleware RCU.

Table 2–4 Oracle Fusion Middleware Components

Oracle Fusion Middleware Components	Description
Oracle Access Manager	Provides the core functionality of Web Single Sign On (SSO), authentication, authorization, centralized policy administration and agent management, real-time session management, and auditing. Installed by Oracle Identity Management provisioning.
Oracle Application Development Framework	Provides an end-to-end application framework that builds on Java Platform, Enterprise Edition (Java EE) standards and open-source technologies to simplify and accelerate implementing service-oriented applications.
Oracle BI Enterprise Edition and Oracle Business Intelligence Applications	Oracle Business Intelligence provides a complete, integrated solution of analytics and reporting for Oracle Fusion Applications. Oracle Business Intelligence Applications is installed **manually** post-provisioning, and is **not** enabled by default. The Oracle Fusion Applications installation and provisioning process installs the Oracle BI Applications software components in the Business Intelligence Oracle home but does no further setup. To finish setting up Oracle BI Applications, you must follow the instructions in the "Setting Up Oracle Business Intelligence Applications" chapter of the *Oracle Business Intelligence Applications Installation Guide*.
Oracle Database Server and Client	The Oracle Database contains the schemas and tablespaces required for both the Oracle Fusion Applications and for your applications. Oracle Fusion Applications does not support other databases. Oracle Database Server must be installed before running Oracle Fusion Applications provisioning and Oracle Identity Management provisioning.
Oracle Data Integrator	Oracle Data Integrator provides a comprehensive data integration platform that covers bulk data movement requirements for Oracle Fusion Applications.
Oracle Directory Services Manager	Provides a graphical administrative interface for Oracle Internet Directory and Oracle Virtual Directory. Installed by Oracle Identity Management provisioning.
Oracle Global Order Promising	A comprehensive order promising solution that determines, based on the current and projected demands and supplies across a supply chain and on an extended supply chain, when a customer order can be fulfilled. This is installed only when selecting Oracle Supply Chain Management.
Oracle HTTP Server	Provides a web listener for applications and the framework for hosting static and dynamic pages and applications over the web. Based on the proven technology of the Apache HTTP Server, Oracle HTTP Server includes significant enhancements that facilitate load balancing, administration, and configuration. Installed by Oracle Identity Management provisioning.
Oracle Internet Directory	A general-purpose LDAPv3 compliant directory storage, Oracle Internet Directory serves as the central user repository for Oracle Identity Management. Installed by Oracle Identity Management provisioning.

Table 2–4 (Cont.) Oracle Fusion Middleware Components

Oracle Fusion Middleware Components	Description
Oracle Identity Federation	Provides a standalone, self-contained federation server that enables single sign-on and authentication in a multiple-domain identity network. Not enabled by default. Installed by Oracle Identity Management provisioning.
Oracle Identity Management	Provides a shared infrastructure for all applications, enabling developers to incorporate Oracle Identity Management into applications. Installed by Oracle Identity Management provisioning.
Informatica Identity Resolution	Enables companies and government organizations to search and match identity data. This is installed only when selecting Oracle Customer Relationship Management.
Oracle JRockit	Oracle JRockit is installed by Oracle Fusion Applications provisioning. Oracle JRockit JDK must be installed prior to running Oracle Identity Management provisioning.
Oracle SOA Suite	Provides a complete set of service infrastructure components for designing, deploying, and managing composite applications. Oracle SOA Suite enables services to be created, managed, and orchestrated into composite applications and business processes. Composites enable you to easily assemble multiple technology components into one SOA composite application. An important component of Oracle SOA Suite is Oracle WSM Policy Manager. Oracle WSM Policy Manager provides the infrastructure for enforcing global security and auditing policies. By securing various endpoints and setting and propagating identity, it secures applications. Oracle WSM Policy Manager provides a standard mechanism for signing messages, performing encryption, performing authentication, and providing role-based access control. You also can change a policy without having to change the endpoints or clients for this endpoints, providing greater flexibility and security monitoring for your enterprise. The Oracle Business Process Management (Oracle BPM) Suite provides an integrated environment for developing, administering, and using business applications centered around business processes. The Oracle BPM Suite is layered on the Oracle SOA Suite and shares many of the same product components. Installed by Oracle Identity Management provisioning.
Oracle Secure Enterprise Search	Provides a search engine for Oracle Fusion Applications Search.
Oracle Virtual Directory	An LDAP-enabled service that provides virtualized abstraction of one or more enterprise data sources into a single directory view. Oracle Virtual Directory provides the ability to integrate LDAP-aware applications into diverse directory environments while minimizing or eliminating the need to change either the infrastructure or the applications. Installed by Oracle Identity Management provisioning.
Oracle WebCenter Content	Provides a comprehensive suite of digital content management tools. These tools can be used across the enterprise to cohesively track, manage, and dispose of content whether written, in digital images, or as email.

Table 2–4 (Cont.) Oracle Fusion Middleware Components

Oracle Fusion Middleware Components	Description
Oracle WebCenter Portal	Enables you to create social applications, enterprise portals, collaborative communities, and composite applications, built on a standards-based, service-oriented architecture. Oracle WebCenter Portal combines dynamic user interface technologies with which to develop rich internet applications, the flexibility and power of an integrated, multichannel portal framework, and a set of horizontal Enterprise 2.0 capabilities delivered as services that provide content, collaboration, presence, and social networking capabilities. Based on these components, Oracle WebCenter Portal also provides an out-of-the-box, enterprise-ready customizable application, WebCenter Spaces, with a configurable work environment that enables individuals and groups to work and collaborate more effectively.
WebGate for Oracle Access Manager	Acts as a communicator plug-in that accepts users requests through Oracle HTTP Server and communicates with Oracle Access Manager. Installed by Oracle Identity Management provisioning.
Oracle WebLogic Communication Services	Provides click-to-dial functionality for applications primarily through contextual actions. Contextual actions provide related information and actions to users within the immediate context of the object instances upon which they act.
Oracle WebLogic Server	Supports the deployment of mission-critical applications in a robust, secure, highly available, and scalable environment. Oracle WebLogic Server is an ideal foundation for building applications based on service-oriented architecture (SOA). Installed by Oracle Identity Management provisioning.
Oracle Web Tier	Includes components that interact with end users at the outermost tier of application grid infrastructure, typically through HTTP requests and responses. Hosts web pages and provides security and high performance along with built-in clustering, load balancing, and failover features

2.1.3.1 Products Installed to the Desktop

In addition to the server-side products installed by the provisioning tools, Oracle Fusion Applications uses the following products that are installed on the desktop.

- Microsoft Office Integration Plugin
- Oracle ADF Integration
- Oracle BI Enterprise Edition plus client
- Oracle Data Integrator Studio
- Oracle Hyperion Financial Reporting Studio
- Oracle Hyperion Smart View
- Oracle JDeveloper

2.1.3.2 Other Related Products

The following Oracle and third-party products are sometimes used to interact directly with Oracle Fusion Applications.

- **Oracle Primavera Enterprise Project Portfolio Management**: Used for the Oracle Fusion Applications Projects product offering.

- **Microsoft Active Directory**: Used to integrate with Oracle Identity Management to provide identity information to Oracle Fusion Applications.
- **Other Applications**: Additional applications such as Oracle eBusiness Suite, Oracle PeopleSoft Human Capital Management, and Oracle Siebel Customer Relationship Management can be configured to integrate with Oracle Fusion Applications.

2.1.4 Oracle Database

The Oracle Database contains the schemas and tablespaces required for both the Oracle Fusion Applications and for your applications. Oracle Fusion Applications does not support other databases.

Oracle Fusion Applications encryption APIs mask data such as credit card numbers in application user interface fields. For encryption and masking beyond that, Transparent Data Encryption (TDE) and Oracle Database Vault (ODV) are certified but optional with Oracle Fusion Applications.

TDE and ODV provide information life cycle protections, such as the following:

- Data access restrictions on database administrators and other privileged users
- Sensitive data at rest in database files and file backups
- Sensitive data in transit
- Sensitive attributes in non-production databases

ODV establishes limitations on the power of privileged users to access sensitive data through segregation of duties policies on DBA roles and by securely consolidating application data in the database. These limitations prevent DBAs and other privileged users from overriding the protections placed on sensitive data by the Virtual Private Database (VPD). Oracle Fusion Applications deploys with the ODV enabled when it is installed.

TDE prevents access to personally identifiable information in the file system or on backups or disk. TDE protects confidential data, such as credit card and social security numbers. TDE encrypts sensitive table data stored in data files at the tablespace level.

2.1.5 Oracle Fusion Applications Management Tools

The following management tools are provided to manage Oracle Fusion Applications:

- Oracle Enterprise Manager Fusion Applications Control
- Oracle Enterprise Manager Cloud Control
- Oracle Enterprise Manager Database Control

Oracle Enterprise Manager Fusion Applications Control

Oracle Enterprise Manager Fusion Applications Control (Fusion Applications Control) enables you to manage a single product family in an Oracle WebLogic Server domain for the Oracle Fusion Applications environment, including the products, applications, and Oracle Fusion Middleware components. As a part of management, you can monitor the runtime performance metrics for the various Oracle Fusion Applications and Oracle Fusion Middleware components.

Oracle Enterprise Manager Cloud Control

Oracle Enterprise Manager Cloud Control (Cloud Control) enables you to monitor and manage the complete IT infrastructure for Oracle Fusion Applications from a single

console. You can monitor all the product families, Oracle Fusion Middleware components, and the Oracle Database. For example, you can monitor all the Oracle WebLogic Server domains for all the product families from one console.

Oracle Enterprise Manager Database Control

Oracle Enterprise Manager Database Control (Database Control) enables you to manage the Oracle Database.

Using Database Control, you can perform administrative tasks such as creating schema objects (tables, views, indexes, and so on), managing user security, managing database memory and storage, backing up and recovering your database, and importing and exporting data. You can also view performance and status information about your database.

2.2 Oracle Fusion Applications Topologies

Both Oracle Identity Management and Oracle Fusion Applications provisioning offer several topology options which allow you to tailor the Oracle Fusion Applications environment, including server allocation, networking, and availability.

There are numerous possible topological permutations, but most topologies fall into a few categories with small variations (such as the use of a demilitarized zone, shared servers, or reverse proxy). These categories are:

- **Basic topology**. This is the simplest type of topology possible directly out-of-the-box.
- **Enterprise topology**. This type of topology is ideal for testing environments where high availability is not necessary.
- **Enterprise topology with high availability**. This type of topology is ideal for Oracle Fusion Applications production environments.

The diagrams in each topology example show logical units, rather than individual servers, representing components of the Oracle Fusion Applications installation. Each unit can be installed to its own server, or multiple units can share a single server, depending on the needs of your enterprise.

2.2.1 Topology Tiers

The Oracle Fusion Applications topologies use a tier-based model that is logically grouped into three tiers: the database tier, middle tier (split into directory and application tiers in Oracle Identity Management), and web tier.

This tier-based model is useful when mapping the Oracle Fusion Applications topology to the type of environment you want to create, fitting the topology to your corporate network location policies, and, consequently, determining where the components should reside in the network.

For example:

- Your company may have a firewall-protected subnet reserved for all production databases. Typically, this is where the databases are deployed, and the database tier resides.
- Your company may have a demilitarized zone (DMZ) where all externally-accessible web servers reside. Typically, this is where the web tier resides, and the web tier components such as the Oracle HTTP Servers and Webgate for Oracle Access Manager are deployed.

- Your company may have a policy that specifies that application-specific HTTP servers may not reside in the DMZ. In such cases, the web tier should be deployed to the internal network along with the mid tier, with a reverse proxy in the DMZ that forwards all external requests to the web tier in the internal network.

Topology tiers are also related to high availability requirements. For a highly available Oracle Fusion Applications environment, each tier must be handled and scaled out independently.

2.2.1.1 Database Tier

In an Oracle Fusion Applications environment, the database tier includes all the databases used for both Oracle Fusion Applications and Oracle Identity Management. For more information about the databases that are part of the Oracle Fusion Applications environment, see Section 2.4.1, "Database Instances and Other Processes."

2.2.1.2 Middle Tier

The middle tier includes all the components between the database tier and the web tier. Components in the middle tier include Oracle WebLogic Servers and the applications deployed on the servers, among other things.

Middle tier components are not accessible directly by end users. Access to the applications in the middle tier is achieved through the web tier, which is ideal for environments where complete isolation between end users and the application is required.

The middle tier consumes information provided from all other tiers as well as itself:

1. The middle tier accesses data stored in any of the Oracle Fusion Applications or Oracle Identity Management databases on the database tier via JDBC or SQL*Net.
2. The middle tier directly accesses the Oracle Identity Management directory tier via LDAP for identity, policy, and credential data.
3. Certain middle tier applications and components communicate amongst themselves using direct calls via protocols such as T3, HTTP, and TCP sockets.
4. For HTTP requests, certain middle tier applications and components communicate amongst each other through calls to the web tier, which then forwards the request to other components in the middle tier.

For Oracle Identity Management, the middle tier is split into two tiers: the directory tier and application tier.

2.2.1.2.1 Oracle Identity Management Directory Tier The Oracle Identity Management directory tier is the deployment tier where all the LDAP services reside. This tier includes products such as Oracle Internet Directory and Oracle Virtual Directory. The directory tier is managed by directory administrators providing enterprise LDAP service support.

The Directory Tier stores two types of information:

- Identity information: Information about users and groups.
- Oracle Platform Security Services (OPSS): Information about security policies and configuration.

Although the topology diagrams do not show LDAP directories other than Oracle Internet Directory, you can use Microsoft Active Directory to store identity information. However, you must always store policy information in Oracle Internet

Directory. You can store identity information in Oracle Internet Directory or another directory.

If you store identity details in a directory other than Oracle Internet Directory, Oracle Virtual Directory is used to present that information to the application and middle tiers.

2.2.1.2.2 Oracle Identity Management Application Tier The Oracle Identity Management application tier is the place where Oracle Identity Management Java EE applications are deployed. The main Java EE components deployed to this tier include Oracle Identity Manager, Oracle Identity Federation, Oracle Directory Services Manager, and Oracle Enterprise Manager Fusion Middleware Control.

The Oracle Identity Management applications on the application tier interact with the directory tier for enterprise identity information and, in some cases, for application metadata. Oracle Enterprise Manager Fusion Middleware Control and Oracle Directory Services Manager provide allow you to manage and administer the components in the application and directory tiers.

2.2.1.3 Web Tier

The web tier contains the Oracle HTTP Servers as well as Webgate for Oracle Access Manager. It is the only tier that can be accessed by end users in Oracle Fusion Applications, and forwards end-user HTTP requests to the applications and components running in the middle tier.

In Oracle Fusion Applications, the web tier can have a load balancer or reverse proxy as a front end. The load balancer or reverse proxy handle all HTTP requests meant for the web tier.

The web tier can be placed in the DMZ if desired, providing end-user access to the services from the middle tier on that side of the firewall.

2.2.2 Network Components

The enterprise and enterprise with high availability topologies involve the use of a load balancer or reverse proxy.

- **Reverse proxy**: The reverse proxy stands between the Oracle Fusion Applications web tier and HTTP clients (end users and external applications). The main purpose of a reverse proxy is to act as a gateway to Oracle Fusion Applications, particularly for network configurations in which clients are using a different subnet from Oracle Fusion Applications. Reverse proxies are recommended for environments using the enterprise topology.
- **Load balancer**: The load balancer is the intermediary between the Oracle Fusion Applications environment and both internal and external clients, where internal clients are Oracle Fusion Applications components and external applications include end users and external applications. The load balancer distributes HTTP requests among servers in the web tier, and TCP requests among the LDAP servers hosting the identity store, policy store, and Oracle Universal Content Management. The load balancer also acts as a gateway for external clients to the Oracle Fusion Applications environment, much like the reverse proxy.

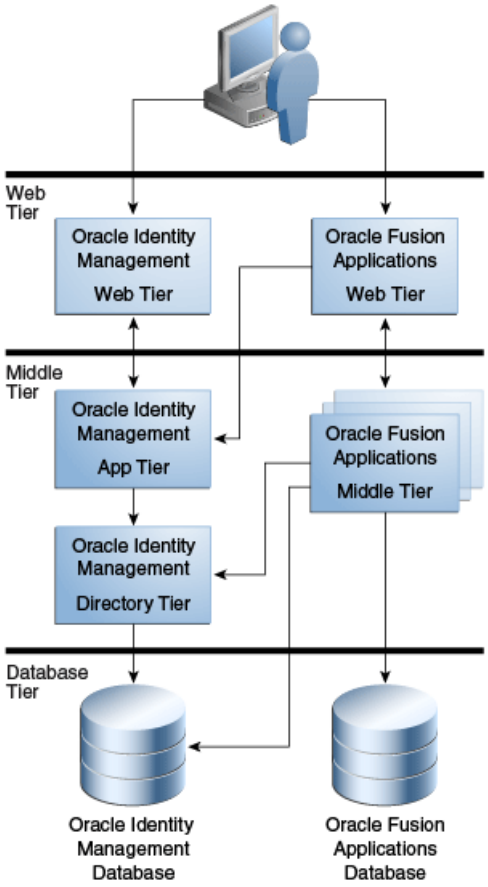
From the perspective of provisioning, the configuration for a load balancer or reverse proxy is essentially the same. The following table summarizes the differences between using a reverse proxy and a load balancer in the context of Oracle Fusion Applications.

Table 2–5 Load Balancer or Reverse Proxy

Functionality	Load Balancer	Reverse Proxy
Acts as an HTTP gateway to Oracle Fusion Applications.	Yes	Yes
Provides high availability through load balancing.	Yes	No
Used for external HTTP traffic.	Yes	Yes
Used for internal HTTP traffic.	Yes	Yes or no
Used for LDAP traffic.	Yes	No
Used for TCP traffic to Oracle WebCenter Content (UCM).	Yes	No

2.2.3 Basic Topology

Figure 2–2 Oracle Fusion Applications Basic Topology



The basic topology is the most rudimentary of possible Oracle Fusion Applications environments, making it a good choice for development or demonstration or proof of concept purposes. It is also the easiest to install, with minimal hardware requirements. In fact, you can install all the components to the same server, given sufficiently robust hardware. Alternatively, you can install Oracle Fusion Applications domains to more than one machine so as to better support Oracle Fusion Applications memory

requirements. No additional network components are required as all communication is server-to-server.

The features of an Oracle Fusion Applications environment with a basic topology are shown in the following table.

Table 2–6 Features of the Basic Topology

Feature	Used in Topology?
Nodes	2 or more
Oracle Identity Management and Oracle Fusion Applications shared node for middle and web tiers	Yes
Oracle Identity Management and Oracle Fusion Applications web tier DMZ setup	No
Reverse proxy or load balancer	No
High availability	No
Expandable post-installation	Limited

Sample configurations of the basic topology are shown in the following table. The following notation is used in the table:

- Oracle Fusion Applications: FA
- Oracle Identity Management: IDM
- Oracle Fusion Applications Database: FA DB
- Oracle Identity Management Database: IDM DB

The asterisk (*) following FA indicates that Oracle Fusion Applications can be split among multiple nodes.

Note:

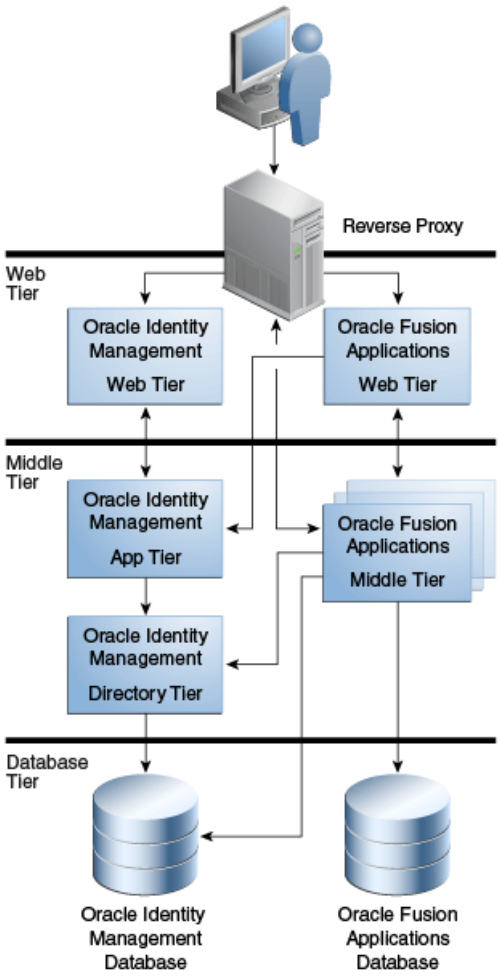
- You **must** install Oracle Identity Management Middle Tier and Oracle Fusion Applications Middle Tier on different hosts. Installing Oracle Identity Management and Oracle Fusion Applications on the same host is not a supported topology.
- You should not share the same database instance for Oracle Identity Management and Oracle Fusion Applications.
- The database instances must also be running on physical host(s).

Table 2–7 Sample Configurations of the Basic Topology

Number of Nodes	Components per Node	Sample Host Names
2	▪ **Node 1**: FA*, FA DB	fahostN.mycompany.com
	▪ **Node 2**: IDM, IDM DB	idmhost.mycompany.com
3	▪ **Node 1**: FA*	fahostN.mycompany.com
	▪ **Node 2**: IDM	idmhost.mycompany.com
	▪ **Node 3**: FA DB, IDM DB	dbhost.mycompany.com
3	▪ **Node 1**: FA*	fahostN.mycompany.com
	▪ **Node 2**: FA DB	fadbhost.mycompany.com
	▪ **Node 3**: IDM, IDM DB	idmhost.mycompany.com
4	▪ **Node 1**: FA*	fahostN.mycompany.com
	▪ **Node 2**: FADB	fadbhost.mycompany.com
	▪ **Node 3**: IDM	idmhost.mycompany.com
	▪ **Node 4**: IDMDB	Idmdbhost.mycompany.com

2.2.4 Enterprise Topology

Figure 2–3 Oracle Fusion Applications Enterprise Topology



The enterprise topology is the most flexible of Oracle Fusion Applications environments, in that it can be expanded following installation. This topology is useful for testing environments in which high availability is not required. The topology features a clear differentiation amongst the web, application, and data tiers. You can install Oracle Fusion Applications domains to more than one machine so as to better support memory requirements. The Oracle Identity Management middle tier can be installed to a maximum of two nodes using the Oracle Identity Management Provisioning Wizard, but additional nodes can be added manually post-install. The use of a reverse proxy is recommended for greater flexibility.

The features of an enterprise topology Oracle Fusion Applications environment are shown in the following table.

Table 2–8 Features of the Enterprise Topology

Feature	Used in Topology?
Nodes	4 or more
Oracle Identity Management and Oracle Fusion Applications shared node for middle and web tiers	No
Oracle Identity Management and Oracle Fusion Applications web tier DMZ setup	Optional
Reverse proxy or load balancer	Recommended
High availability	No
Expandable post-installation	Yes

Sample configurations of the enterprise topology are shown in the following table. The following notation is used in the table:

- Oracle Fusion Applications: FA Web
- Oracle Fusion Applications Middle Tier: FA Mid
- Oracle Identity Management: IDM Mid
- Oracle Identity Management Web Tier: IDM Web
- Oracle Fusion Applications Database: FA DB
- Oracle Identity Management Database: IDM DB

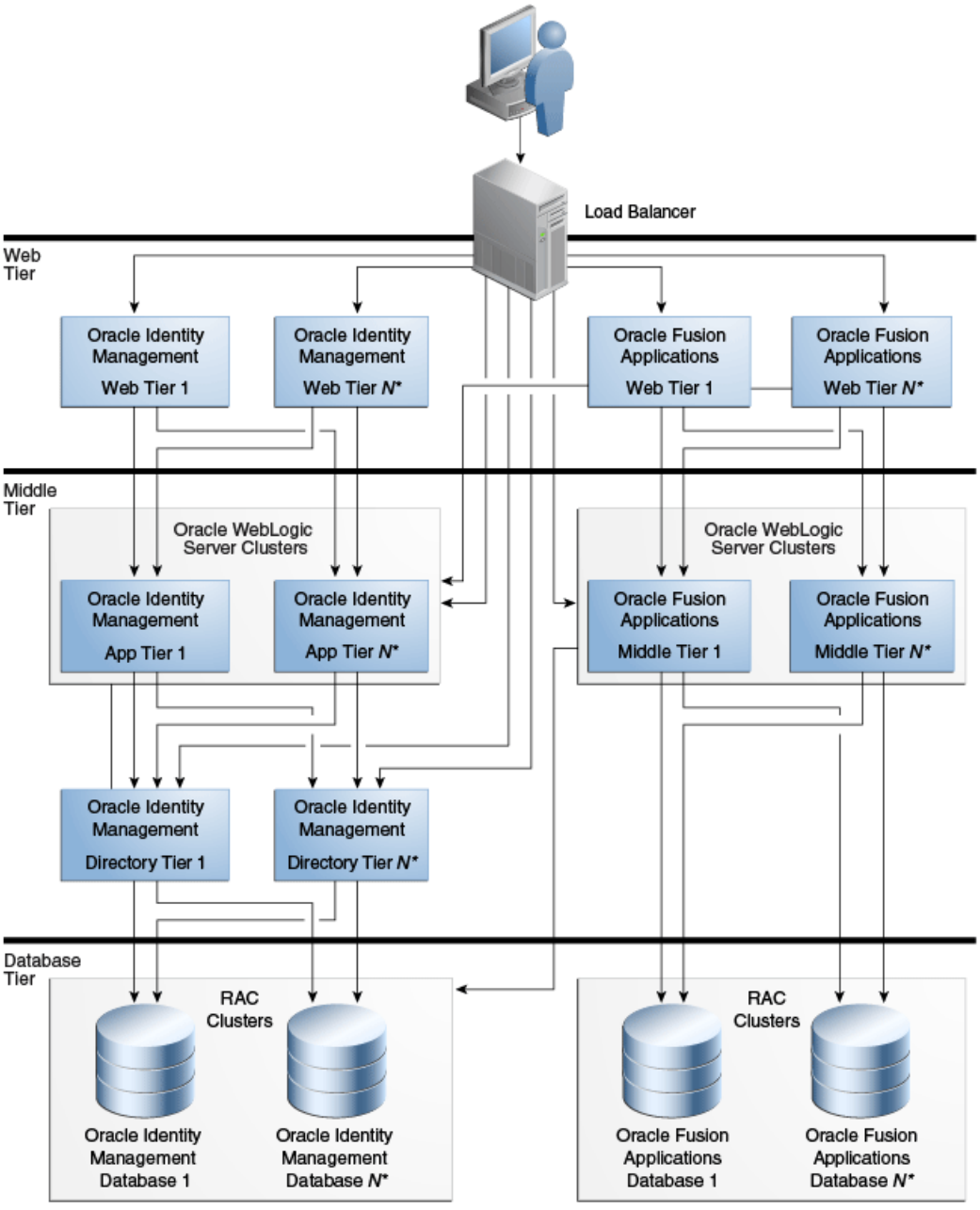
The asterisk (*) following FA Mid indicates that the Oracle Fusion Applications middle tier can be split among multiple nodes. The asterisk (*) following IDM Mid indicates that the Oracle Identity Management middle tier can be split amongst two nodes.

Table 2–9 Sample Configurations of the Enterprise Topology

Number of Nodes	Node Contains	Sample Host Names
4	■ **Node 1**: IDM Web, FA Web	webhost.mycompany.com
	■ **Node 2**: FA Mid*	fahost.mycompany.com
	■ **Node 3**: IDM Mid*	idmhost.mycompany.com
	■ **Node 4**: FA DB, IDM DB	dbhost.mycompany.co
4	■ **Node 1**: IDM Web, FA Web	webhost.mycompany.com
	■ **Node 2**: FA Mid*	fahost.mycompany.com
	■ **Node 3**: IDM Mid*, IDM DB	idmhost.mycompany.com
	■ **Node 4**: FA DB	fadbhost.mycompany.com
5	■ **Node 1**: IDM Web, FA Web	webhost.mycompany.com
	■ **Node 2**: FA Mid*	fahost.mycompany.com
	■ **Node 3**: IDM Mid*	idmhost.mycompany.com
	■ **Node 4**: IDM DB	idmdbhost.mycompany.com
	■ **Node 5**: FA DB	fadbhost.mycompany.com
6	■ **Node 1**: IDM Web	idmwebhost.mycompany.com
	■ **Node 2**: FA Web	fawebhost.mycompany.com
	■ **Node 3**: FA Mid*	fahost.mycompany.com
	■ **Node 4**: IDM Mid*	idmhost.mycompany.com
	■ **Node 5**: IDM DB	idmdbhost.mycompany.com
	■ **Node 6**: FA DB	fadbhost.mycompany.com

2.2.5 Enterprise Topology with High Availability

Figure 2–4 Oracle Fusion Applications Enterprise Topology with High Availability



*The Oracle Fusion Applications Middle Tier can be installed to multiple nodes. The Oracle Identity Management Middle Tier is installed in a single node and can be scaled out to multiple nodes.

The enterprise topology with high availability is the ideal Oracle Fusion Applications topology for production environments. The topology features a clear differentiation amongst the web, application, and data tiers. You can install Oracle Fusion Applications domains to more than one machine so as to better support memory requirements. The Oracle Identity Management middle tier can be installed to a maximum of two nodes using the Oracle Identity Management Provisioning Wizard, but additional nodes can be added manually post-installation. The use of a reverse load balancer is required to manage HTTP and TCP traffic.

The features of an enterprise topology Oracle Fusion Applications environment with high availability are shown in the following table.

Table 2–10 Features of the Enterprise Topology with High Availability

Feature	Used in Topology?
Nodes	8 or more
Oracle Identity Management and Oracle Fusion Applications shared node for middle and web tiers	No
Oracle Identity Management and Oracle Fusion Applications web tier DMZ setup	Optional
Reverse proxy or load balancer	Yes
High availability	Yes
Expandable post-installation	Yes

Sample configurations of the enterprise topology with high availability are shown in the following table. The following notation is used in the table:

- Oracle Fusion Applications: FA Web
- Oracle Fusion Applications Middle Tier: FA Mid
- Oracle Identity Management: IDM Mid
- Oracle Identity Management Web Tier: IDM Web
- Oracle Fusion Applications Database: FA DB
- Oracle Identity Management Database: IDM DB

The asterisk (*) following FA Mid indicates that the Oracle Fusion Applications middle tier can be split among multiple nodes. The asterisk (*) following IDM Mid indicates that the Oracle Identity Management middle tier can be split amongst two nodes.

Table 2–11 Sample Configurations of the Enterprise Topology with High Availability

Number of Nodes	Node Contains	Sample Host Names
8	■ **Nodes 1-2**: IDM Web, FA Web	webhost1.mycompany.com… webhost*N*.mycompany.com
	■ **Nodes 3-4**: FA Mid*	fahost1.mycompany.com… fahost*N*.mycompany.com
	■ **Nodes 5-6**: IDM Mid*	idmhost1.mycompany.com… idmhost*N*.mycompany.com
	■ **Nodes 7-8**: FA DB, IDM DB	dbhost1.mycompany.com… dbhost*N*.mycompany.com

Table 2–11 (Cont.) Sample Configurations of the Enterprise Topology with High Availability

Number of Nodes	Node Contains	Sample Host Names
8	■ **Nodes 1-2**: IDM Web, FA Web ■ **Nodes 3-4**: FA Mid* ■ **Nodes 5-6**: IDM Mid*, IDM DB ■ **Nodes 7-8**: FA DB	webhost1.mycompany.com… webhost*N*.mycompany.com fahost1.mycompany.com… fahost*N*.mycompany.com idmhost1.mycompany.com… idmhost*N*.mycompany.com fadbhost1.mycompany.com… fadbhost*N*.mycompany.com
10	■ **Nodes 1-2**: IDM Web, FA Web ■ **Nodes 3-4**: FA Mid* ■ **Nodes 5-6**: IDM Mid* ■ **Nodes 7-8**: IDM DB ■ **Nodes 9-10**: FA DB	webhost1.mycompany.com… webhost*N*.mycompany.com fahost1.mycompany.com… fahost*N*.mycompany.com idmhost1.mycompany.com… idmhost*N*.mycompany.com idmdbhost1.mycompany.com… idmdbhost*N*.mycompany.com fadbhost1.mycompany.com… fadbhost*N*.mycompany.com
12	■ **Nodes 1-2**: IDM Web ■ **Nodes 3-4**: FA Mid ■ **Nodes 5-6**: FA* ■ **Nodes 7-8**: IDM Mid* ■ **Nodes 9-10**: IDM DB ■ **Nodes 11-12**: FA DB	idmwebhost1.mycompany.com… idmwebhost*N*.mycompany.com fawebhost1.mycompany.com… fawebhost*N*.mycompany.com fahost1.mycompany.com... fahost*N*.mycompany.com idmhost1.mycompany.com… idmhost*N*.mycompany.com idmdbhost1.mycompany.com… idmdbhost*N*.mycompany.com fadbhost1.mycompany.com… fadbhost*N*.mycompany.com

2.3 Oracle Fusion Applications Directory Structure

After the Oracle Fusion Applications environment has been installed, the storage and directory layout will vary depending on the following factors:

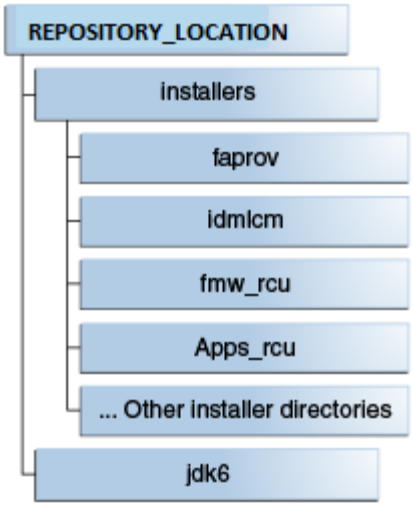
- Paths selected during the provisioning process
- Whether the local configuration option was selected during the provisioning process
- Host names provided during the provisioning process

2.3.1 Installation Repository

The following diagram depicts the directory structure for the installation repository, which is created from the Oracle Fusion Applications install zip files you download. The installation repository should be placed on a shared disk. The installation repository is only required during the installation process. It is no longer needed once the installation is complete.

The root directory for the installation repository is `REPOSITORY_LOCATION`.

Figure 2–5 Directory Structure for the Installation Repository



The directory structure is as follows, as shown in the previous diagram:

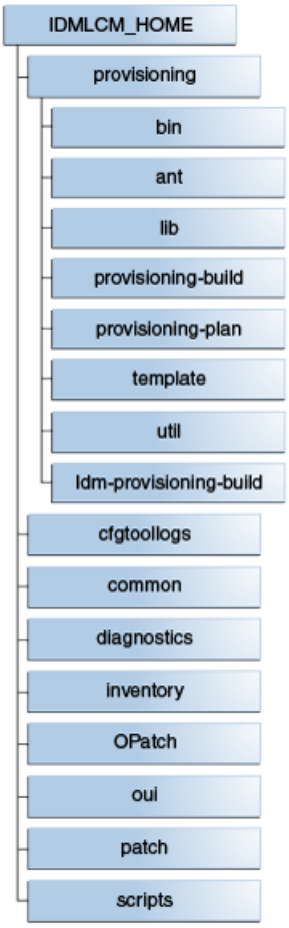
- `REPOSITORY_LOCATION`
- `REPOSITORY_LOCATION/installers`
- `REPOSITORY_LOCATION/installers/faprov`
- `REPOSITORY_LOCATION/installers/idmlcm`
- `REPOSITORY_LOCATION/installers/fmw_rcu`
- `REPOSITORY_LOCATION/installers/apps_rcu`
- `REPOSITORY_LOCATION/jdk6`

2.3.2 Oracle Identity Management Provisioning Framework Directory Structure

The Oracle Identity Management provisioning framework should be installed on a shared disk. The framework will have the directory layout shown in the following figure.

The directory to which the Oracle Identity Management provisioning framework is to be installed is `IDMLCM_HOME`.

Figure 2–6 Oracle Identity Management Provisioning Framework Directory Structure



The directory structure shown in the previous figure is listed as follows:

- `IDMLCM_HOME`
- `IDMLCM_HOME/provisioning`
- `IDMLCM_HOME/provisioning/bin`
- `IDMLCM_HOME/provisioning/ant`
- `IDMLCM_HOME/provisioning/lib`
- `IDMLCM_HOME/provisioning/provisioning-build`
- `IDMLCM_HOME/provisioning/provisioning-plan`
- `IDMLCM_HOME/provisioning/template`
- `IDMLCM_HOME/provisioning/util`
- `IDMLCM_HOME/provisioning/idm-provisioning-build`
- `IDMLCM_HOME/cfgtoollogs`
- `IDMLCM_HOME/common`
- `IDMLCM_HOME/diagnostics`
- `IDMLCM_HOME/inventory`
- `IDMLCM_HOME/Opatch`

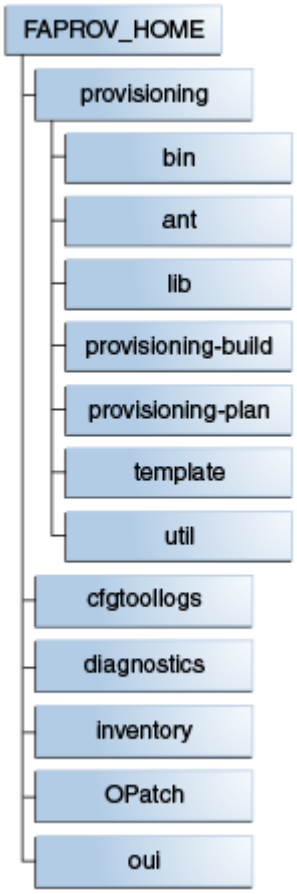
- IDMLCM_HOME/oui
- IDMLCM_HOME/patch
- IDMLCM_HOME/scripts

2.3.3 Oracle Fusion Applications Provisioning Framework Directory Structure

The Oracle Fusion Applications provisioning framework should be installed on a shared disk. The following diagram shows the directory structure of the provisioning framework.

The directory to which the Oracle Fusion Applications provisioning framework is to be installed is FAPROV_HOME.

Figure 2–7 Oracle Fusion Applications Provisioning Framework Directory Structure



The directory structure shown in the previous figure is listed as follows:

- FAPROV_HOME
- FAPROV_HOME/provisioning
- FAPROV_HOME/provisioning/bin
- FAPROV_HOME/provisioning/ant
- FAPROV_HOME/provisioning/lib
- FAPROV_HOME/provisioning/provisioning-build

- FAPROV_HOME/provisioning/provisioning-plan
- FAPROV_HOME/provisioning/template
- FAPROV_HOME/provisioning/util
- FAPROV_HOME/cfgtoollogs
- FAPROV_HOME/diagnostics
- FAPROV_HOME/inventory
- FAPROV_HOME/Opatch
- FAPROV_HOME/oui

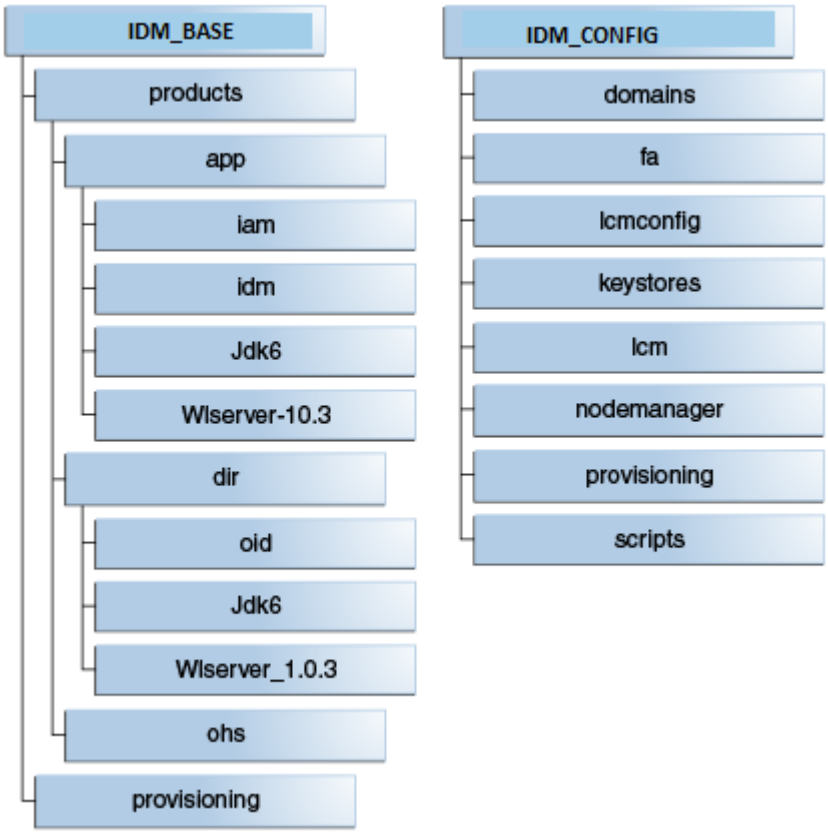
2.3.4 Oracle Identity Management Shared Directory Structure

The Oracle Identity Management directory structure may be placed in shared storage or in a combination of shared and local storage. The following diagram shows the shared directory structure.

The root directory for Oracle Identity Management product binary files is IDM_BASE. The root directory for Oracle Identity Management configuration and instance files is IDM_CONFIG.

The following diagram shows the structure of the shared Oracle Identity Management directories.

Figure 2–8 Oracle Identity Management Shared Directory Structure



The shared directory structure described in the previous diagram is listed here:

Table 2–12 Oracle Identity Management Shared Directory Structure

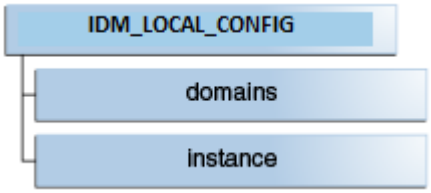
IDM_BASE	IDM_CONFIG
■ IDM_BASE	■ IDM_CONFIG
■ IDM_BASE/products	■ IDM_CONFIG/domains
■ IDM_BASE/products/app	■ IDM_CONFIG/fa
■ IDM_BASE/products/app/iam	■ IDM_CONFIG/lcmconfig
■ IDM_BASE/products/app/idm	■ IDM_CONFIG/keystores
■ IDM_BASE/products/app/jdk6	■ IDM_CONFIG/lcm
■ IDM_BASE/products/app/wlserver-10.3	■ IDM_CONFIG/nodemanager
■ IDM_BASE/products/dir	■ IDM_CONFIG/provisioning
■ IDM_BASE/products/dir/oid	■ IDM_CONFIG/scripts
■ IDM_BASE/products/dir/jdk6	
■ IDM_BASE/products/dir/wlserver_1.0.3	
■ IDM_BASE/products/ohs	
■ IDM_BASE/provisioning	

2.3.5 Oracle Identity Management Local Directory Structure

If you select local domain configuration during Oracle Identity Management provisioning (`INSTALL_LOCALCONFIG_ENABLE=true`), certain Oracle Identity Management configuration directories are stored locally. All servers containing WebLogic Server domains or Oracle Application Server instances will contain this directory.

The local root directory for Oracle Identity Management as defined by the provisioning wizard is `IDM_LOCAL_CONFIG`. The directory structure is shown in the following diagram.

Figure 2–9 Oracle Identity Management Local Directory Structure



The Oracle Identity Management local directory structure shown in the previous diagram is as follows:

- `IDM_LOCAL_CONFIG`
- `IDM_LOCAL_CONFIG/domains`
- `IDM_LOCAL_CONFIG/instances`

2.3.6 Oracle Identity Management DMZ Directory Structure

If you select the DMZ option during Oracle Identity Management provisioning (`WEBTIER_DMZINSTALL_ENABLE=true`), the web tier Oracle Fusion Middleware home as well as the OHS instance directory are stored locally to the DMZ. The directory path

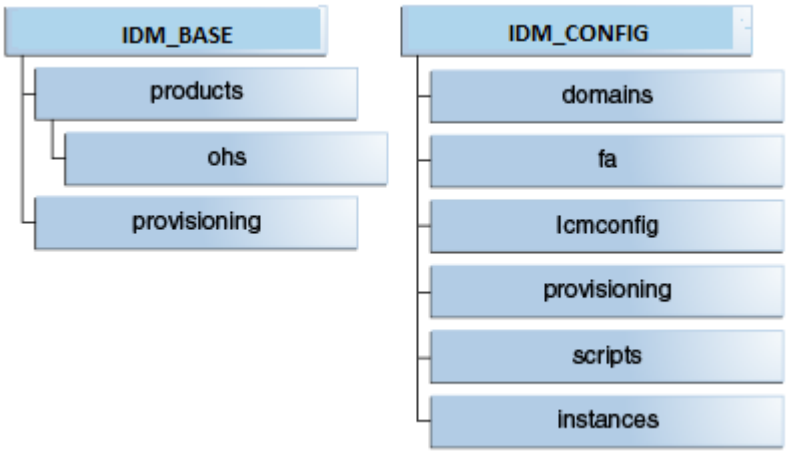
used is the same as that for the shared storage, being IDM_BASE for the Fusion Middleware home and IDM_CONFIG for the configuration directory.

The root directory in the local configuration as defined by the provisioning wizard is IDM_LOCAL_CONFIG.

Additionally, if you select the local domain configuration option during Oracle Identity Management provisioning (INSTALL_LOCALCONFIG_ENABLE=true), certain configuration directories are stored locally under the directory defined for IDM_LOCAL_CONFIG.

The following diagram illustrates the Oracle Identity Management DMZ directory structure.

Figure 2–10 Oracle Identity Management DMZ Directory Structure



The directory structure shown in the previous diagram is as follows:

Table 2–13 Oracle Identity Management DMZ Directory Structure

IDM_BASE	IDM_CONFIG
■ IDM_BASE ■ IDM_BASE/products ■ IDM_BASE/products/ohs ■ IDM_BASE/provisioning	■ IDM_CONFIG ■ IDM_CONFIG/domains ■ IDM_CONFIG/fa ■ IDM_CONFIG/lcmconfig ■ IDM_CONFIG/provisioning ■ IDM_CONFIG/scripts ■ IDM_CONFIG/instances

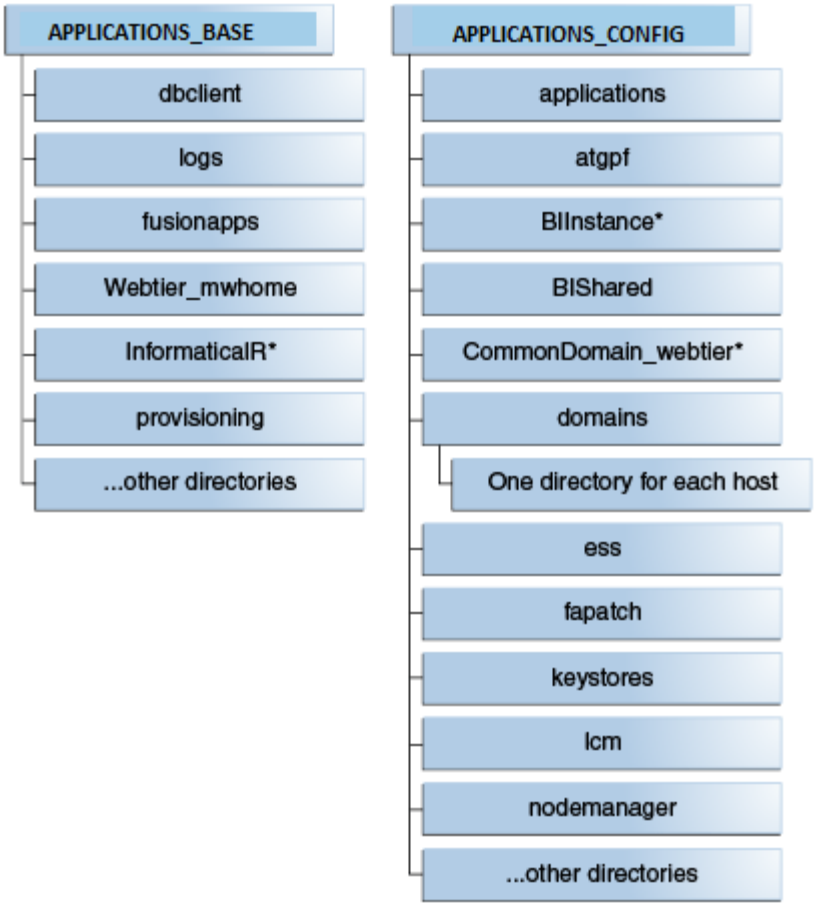
2.3.7 Oracle Fusion Applications Shared Directory Structure

The Oracle Fusion Applications directory structure may be stored in a shared directory or in a combination of shared and local storage.

The root directory for the Oracle Fusion Applications product binary files is *APPLICATIONS_BASE*. The root directory for the Oracle Fusion Applications configuration and instance files is APPLICATIONS_CONFIG.

The following diagram illustrates the Oracle Fusion Applications shared directory structure.

Figure 2–11 Oracle Fusion Applications Shared Directory Structure



The Oracle Fusion Applications shared directory structure shown in the previous diagram is listed as follows.

Table 2–14 Oracle Fusion Applications Shared Directory Structure

APPLICATIONS_BASE	APPLICATIONS_CONFIG
▪ APPLICATIONS_BASE ▪ APPLICATIONS_BASE/dbclient ▪ APPLICATIONS_BASE/logs ▪ APPLICATIONS_BASE/fusionapps ▪ APPLICATIONS_BASE/webtier_mwhome ▪ APPLICATIONS_BASE/InformaticaIR ▪ APPLICATIONS_BASE/provisioning ▪ Other directories	▪ APPLICATIONS_CONFIG ▪ APPLICATIONS_CONFIG/applications ▪ APPLICATIONS_CONFIG/atgpf ▪ APPLICATIONS_CONFIG/BIInstance ▪ APPLICATIONS_CONFIG/BIShared ▪ APPLICATIONS_CONFIG/CommonDomain_webtier ▪ APPLICATIONS_CONFIG/domains ▪ APPLICATIONS_CONFIG/domains/one directory for each host ▪ APPLICATIONS_CONFIG/ess ▪ APPLICATIONS_CONFIG/fapatch ▪ APPLICATIONS_CONFIG/keystores ▪ APPLICATIONS_CONFIG/lcm ▪ APPLICATIONS_CONFIG/nodemanager ▪ Other directories

The `InformaticaIR` directory is only available in environments where Informatica Identity Resolution is installed (for CRM product offerings only).

The `BIIInstance` directory is placed on shared storage only if the local domains configuration option is not selected.

The `CommonDomain_webtier` directory is placed in shared storage only if the DMZ option is not selected.

2.3.7.1 Applications Base Directory

When an environment consists of multiple hosts, a central, shared provisioning installation directory is required so that the location is visible to all provisioned hosts. To achieve this setup, the use of full host names is required. Alias names are not recommended.

The top-level directory for the Oracle Fusion Applications binaries is the applications base. You specify a name for this directory at the time of provisioning. This directory includes two mount points: */net/mount1/appbase* (`APPLICATIONS_BASE`) for components that remain read-only after provisioning, and */net/mount2* (APPLICATIONS_CONFIG) to contain instances that are configurable after provisioning. This structure aids performance issues and accommodates a "lock-down" of binaries after provisioning. It ensures that the configurable components remain available.

The applications base directory must not be set to the system root directory or set to the root directory of a logical drive. Some life cycle management tools compute directory names by backing up one directory level from the applications base directory and then appending the appropriate subdirectory name. These tools will fail if the applications base directory is set to the system root directory or set to the root directory of a logical drive because it is not possible to back up one directory level from the system root directory or from the root directory of a logical drive.

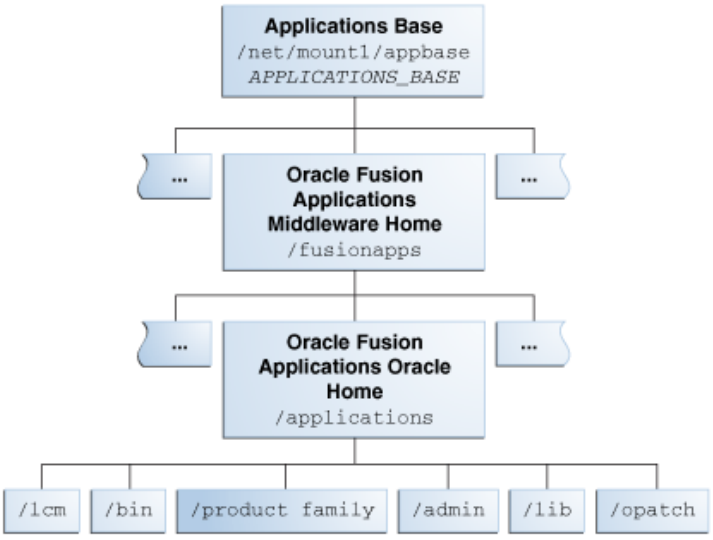
2.3.7.2 Oracle Fusion Applications Oracle Home Directory

In the context of Oracle Fusion Applications directory structures, the term home directory generally refers to a directory that contains one or more Oracle Fusion Middleware homes or Oracle Fusion Applications homes, which groups together related Oracle product offerings.

As the home directory is read-only, you can update it only by using Oracle Fusion Applications life cycle tools, such as Provisioning, RUP Installer, and Patch Manager.

The Oracle Fusion Applications Oracle home directory (*FA_ORACLE_HOME*) is located under the *APPLICATIONS_BASE*/`fusionapps` directory (*net/mount1/appbase*/`fusionapps`). The `/fusionapps` directory is an Oracle Fusion Applications Middleware home (*APPLICATIONS_BASE/fusionapps*). Figure 2–12 shows this directory structure.

Figure 2–12 Oracle Fusion Applications Oracle Home



The Oracle home contains the following subdirectories:

- **/fusionapps/applications/lcm**: The life cycle management directory. Contains the patching framework artifacts in the following subdirectories:
  - **../ad/bin**: Patching framework software and executables, including C artifacts and configuration scripts, that set the environment and start the corresponding utility.
  - **../ad/java**: Java artifacts.
  - **../ad/db/sql**: Database artifacts and SQL files.
  - **../ad/lib**: Application libraries.
  - **../ad/template**: Configuration files or templates delivered and used by the patching framework during configuration activities.
- **/fusionapps/applications/bin**: Executables called by Enterprise Scheduler Service jobs.
- **/fusionapps/applications/*product_family***: Container directory for artifacts specific to a product configuration, for example, `/ORACLE/fusionapps/fin`.
- **/fusionapps/applications/admin**: Patching framework environment properties file (*FUSION_env*.properties), Oracle Fusion Applications AutoPatch, and the patching logs, reports, and administration files. These files are required by Oracle Fusion Applications Patch Manager.
- **/fusionapps/applications/lib**: Applications-specific libraries.
- **/fusionapps/applications/OPatch**: Contains the OPatch utility called by Oracle Fusion Applications Patch Manager when patching middleware artifacts.

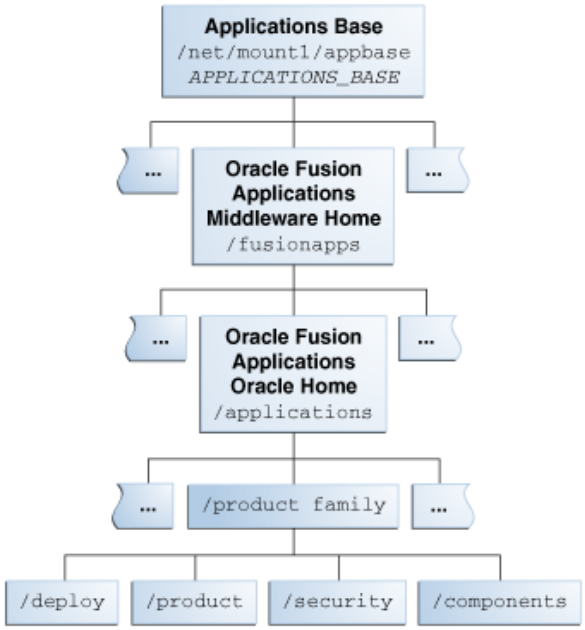
For complete information about patching your applications environment, see the *Oracle Fusion Applications Patching Guide*.

2.3.7.3 Oracle Fusion Applications Product Family Directory

The Oracle Fusion Applications *.../product_family* directory is located under the `FA_ORACLE_HOME` directory. This structure exists for each of the product configurations (product families) deployed in the Oracle Fusion Applications environment during

provisioning. Figure 2–13 shows this directory structure.

Figure 2–13 Oracle Fusion Applications Product Family Directory



The following subdirectories are located under the `.../product_family` directory:

- **/fusionapps/applications/*product_family*/*product***: Product grouping within a product family. For example, `/fusionapps/applications/fin/ar` represents the Account Receivables product in the Financials product family.
  - **/db/plsql/**: PL/SQL packages and bodies for a given product, for example, `.../fin/ar/db/plsql/arp_process_line.pkh`.
  - **/db/sql/**: SQL scripts for a given product. For example, `.../fin/ar/db/sql/ar_ar_rev_rec_typ_type.sql`.
  - **/db/data/*lba*/US/**: Product-specific seed data files, striped by Logical Business Area (LBA). Note that sub-directories could exist in the top-level seed data directory because some LBAs can have sub-LBAs. For example, `.../fin/ar/db/data/FinArCustomers/US/ArlookupTypeSD.xlf`.
- **/fusionapps/applications/*product_family*/deploy**: Container directory for deployable artifacts, composites, Java EE applications (such as Oracle Application Development Framework and Oracle Enterprise Scheduler Service).
- **/fusionapps/applications/*product_family*/security/**: Product family directory containing security-related files.

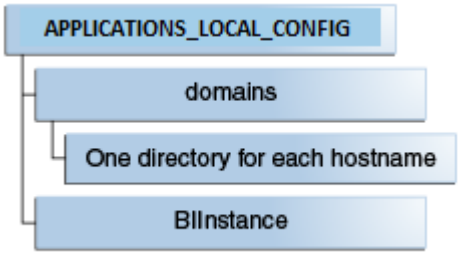
2.3.8 Oracle Fusion Applications Local Directory Structure

If you select the local domain configuration option during Oracle Fusion Applications provisioning (`INSTALL_LOCALCONFIG_ENABLE=true`), certain configuration directories are stored locally. All servers containing domains or Oracle Application Server instances will include this directory.

The local root configuration directory as defined in the provisioning wizard is `IDM_LOCAL_CONFIG`.

The following diagram illustrates the Oracle Fusion Applications shared directory structure.

Figure 2–14 Oracle Fusion Applications Local Directory Structure



The directory structure shown in the previous diagram is listed here.

- `APPLICATIONS_LOCAL_CONFIG`
- `APPLICATIONS_LOCAL_CONFIG/domains`
- `APPLICATIONS_LOCAL_CONFIG/domains/`one directory for each host name
- `APPLICATIONS_LOCAL_CONFIG/BIInstance`

2.3.9 Oracle Fusion Applications DMZ Directory Structure

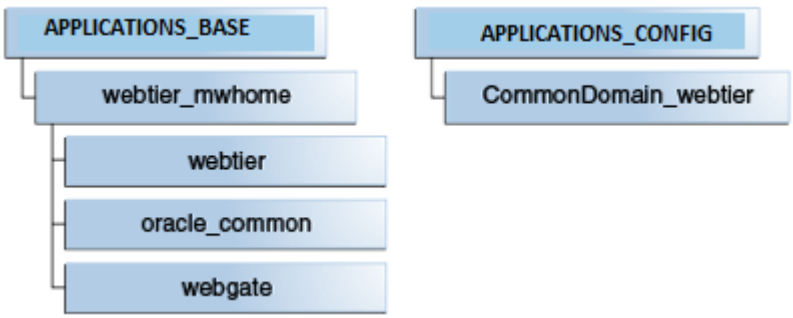
If you select the DMZ option during Oracle Fusion Applications provisioning (`WEBTIER_DMZINSTALL_ENABLE=true`), the web tier Fusion Middleware home and the OHS instance directory are stored locally to the DMZ. The directory path used is the same as that defined for shared storage (`APPLICATIONS_BASE` for the Fusion Middleware home and `APPLICATIONS_CONFIG` for the configuration directory).

The tool local configuration directory as defined in the provisioning wizard is `APPLICATIONS_LOCAL_CONFIG`.

Additionally, if you select the local domain configuration option during Oracle Identity Management provisioning (`INSTALL_LOCALCONFIG_ENABLE=true`), certain configuration directories are stored locally under the directory defined for `APPLICATIONS_LOCAL_CONFIG`.

The following diagram illustrates the Oracle Fusion Applications DMZ directory structure.

Figure 2–15 Oracle Fusion Applications DMZ Directory Structure



The directory structure shown in the previous diagram is listed here.

Table 2–15 Oracle Fusion Applications DMZ Directory Structure

APPLICATIONS_BASE	APPLICATIONS_CONFIG
■ APPLICATIONS_BASE ■ APPLICATIONS_BASE/webtier_mwhome ■ APPLICATIONS_BASE/webtier_mwhome/webtier	■ APPLICATIONS_CONFIG ■ CommonDomain_webtier

2.4 Oracle Fusion Applications Runtime Processes

A running Oracle Fusion Applications environment includes the following runtime processes:

- Databases: These include Oracle Fusion Applications and Oracle Identity Management databases; Oracle Fusion Applications data warehouse.
- Oracle Application Server instances: Run C-based and Java SE components. These include Oracle Internet Directory, Oracle Virtual Directory, Oracle Fusion Applications HTTP server, Oracle Identity Management HTTP server, Oracle Global Order Processing, and Oracle Business Intelligence.
- Oracle WebLogic Server domains: These run Java EE-based components, and include administration and managed servers, as well as the node manager.
- Other executables: For components such as Informatica Identity Resolution.

2.4.1 Database Instances and Other Processes

Both Oracle Identity Management and Oracle Fusion Applications have their own databases, as listed in the following table.

Table 2–16 Database Instances in Oracle Fusion Applications

Provisioned Environment	Database	Sample Schemas	Comments
Oracle Identity Management	Oracle Identity Management Database	FA_OIM FA_OAM FA_SOAINFRA	Contains the schemas for Oracle Identity Management products such as Oracle Identity Management, Oracle Access Manager, and so on.
Oracle Identity Management	Oracle Internet Directory Database	ODS ODSSM	Contains the Oracle Internet Directory schemas. Optional as a separate database, otherwise the Oracle Identity Management database is used.
Oracle Fusion Applications	Transactional Database	FUSION FUSION_RUNTIME	Contains the transactional schemas for Oracle Fusion Applications.
Oracle Fusion Applications	Data warehouse Database	<*prefix*>_DW is the major data warehouse schema, where <*prefix*> is the schema prefix selected when the Oracle Business Intelligence Data warehouse RCU runs.	Contains the schemas for the Oracle Fusion Applications Datawarehouse.

2.4.2 Oracle Application Server Instances

Oracle Application Server instances in the Oracle Fusion Applications environment are listed here.

Application Server Instances in the Provisioned Oracle Identity Management Environment

- Oracle Internet Directory and Oracle Virtual Directory
- Oracle Identity Federation
- Oracle HTTP Server

Application Server Instances in the Oracle Fusion Applications Environment

- Oracle Global Order Promising
- Oracle HTTP Server
- Oracle Business Intelligence

2.4.3 Oracle WebLogic Server Domains

The topology for an applications environment centers around a set of predefined Oracle WebLogic Server domains. The provisioning process creates these domains during the physical installation. It then deploys the product offerings that you select for installation in the associated product family domain. It also deploys common applications for use by all product offerings and their dependent middleware components.

After provisioning is complete, you can scale out Oracle Fusion Middleware components, such as Oracle HTTP Server and Oracle SOA Suite, and product domains, such as Oracle Fusion Customer Relationship Management domain, Oracle Fusion Common domain, Oracle Fusion Human Capital Management domain, and so on.

A WebLogic Server domain is a logically related group of Oracle WebLogic Server resources that is managed as a unit. It consists of an Administration Server and one or more Managed Servers. A managed server hosts components and associated resources that constitute each product configuration. The domains are predefined to ensure that product offerings and their dependencies are always stored in a standardized arrangement.

In each domain, every Managed Server belongs to a cluster. A cluster is a group of Oracle WebLogic Servers that work together to provide scalability and high availability for applications. A cluster appears as a single Oracle WebLogic Server instance. The Managed Server instances that constitute a cluster can run on the same host or be located on different hosts. Applications are deployed to the cluster, which implies deployment to every Managed Server within the cluster.

The WebLogic Server domains run Java EE-based components and include administration and managed servers, as well as the node manager.

The WebLogic Server domains that are part of a Oracle Fusion Applications environment are listed here.

WebLogic Server Domains in the Provisioned Oracle Identity Management Environment

- `IDMDomain`. Always available.

WebLogic Server Domains in the Provisioned Oracle Fusion Applications Environment

- CommonDomain. Always available.
- HCMDomain. Always available.
- CRMDomain. Always available.
- FinancialsDomain. Always available.
- BIDomain. Always available.
- SCMDomain. Available only with the following offerings: Oracle Fusion Customer Relationship Management, Oracle Fusion Financials, and Oracle Fusion Supply Chain Management.
- ProcurementDomain. Available only with the following offerings: Oracle Fusion Financials and Oracle Fusion Supply Chain Management.
- ProjectsDomain. Available only with the following offering: Oracle Fusion Financials.
- ICDomain. Available only with the following offering: Oracle Fusion Incentive Compensation.
- OSNDomain. Available only when Oracle Social Network is configured.

Related Links

- For more information about configuring domains, see "Oracle WebLogic Server Domains Configuration" in *Oracle Fusion Applications Administrator's Guide*.
- For more information about the enterprise deployment of domains and instructions about scale out, see *Chapter 18, "Completing Conditional Common High Availability Post-Installation Tasks for Oracle Fusion Applications"*.

2.5 Accessing Oracle Fusion Applications

End users access Oracle Fusion Applications through a set of URLs defined during the provisioning process (the provisioning wizard calls them external URLs). Depending on whether the topology includes a load balancer or reverse proxy, Oracle Fusion Applications URL endpoints may be at the load balancer or reverse proxy, or directly at the Oracle HTTP Server.

The main end user entry point to Oracle Fusion Applications is generally a URL similar to the following:

```
https://fusionapps-common.mycompany.com/homePage
```

Each product family may have its own host name or port, depending on the web tier and load balancer configuration in the provisioning wizard.

Administrators can access the administration consoles through a set of internal or administrative URLs defined in the provisioning wizard. Administrators can use Oracle Enterprise Manager Fusion Applications Control and Oracle Enterprise Manager Cloud Control Console to manage the Oracle Fusion Applications environment.

As with all URLs in Oracle Fusion Applications, access is subject to authentication through Oracle Access Manager.

For more information about using Fusion Applications Control and Cloud Control Console, see "Getting Started with Administering Oracle Fusion Applications" in the *Oracle Fusion Applications Administrator's Guide*.

2.6 What to Do Next

Now that you have a grasp of the basic process of provisioning, and an idea of the structure and topologies of Oracle Fusion Applications environments, you are ready to plan your deployment. Proceed to the Planning section for more information.

Part II

Planning an Oracle Fusion Applications Installation

Planning is an essential component of installation. This section describes each area that needs to be thought out, and includes a corresponding *Oracle Fusion Applications Installation Workbook* to be completed. The planning phase is divided into the following chapters:

- Chapter 3, "Planning the Topology and Provisioning of Your Installation"
- Chapter 4, "Planning the Configuration of the Components of Your Installation"

3

Planning the Topology and Provisioning of Your Installation

Planning a Oracle Fusion Applications installation is a prerequisite to a successful install, and may involve a variety of users. To plan the installation fully, you may need to collaborate with database administrators, network engineers, and other specialized administrators within your organization. This material also assumes that at least one person is guiding the installation overall and is taking the role of the "Oracle Fusion Applications Administrator."

The planning material is split into two chapters, Chapter 3, "Planning the Topology and Provisioning of Your Installation", and Chapter 4, "Planning the Configuration of the Components of Your Installation". Though the material is divided, all the tasks are important and relate sequentially to each other.

There is also a companion Microsoft Excel spreadsheet – the *Oracle Fusion Applications Installation Workbook* – that you will fill out during the planning phase.

3.1 Introduction

Planning includes the following subjects:

- Section 3.1, "Introduction" where the various sections are outlined and the Workbook is introduced.
- Section 3.2, "Environment: Completing the Environment Tab Entries": Helps you define the basic environment configuration and fill out the first tab of the Workbook.
- Section 3.3, "Provisioning: Planning the Configuration of Your Provisioned Installation": Helps define the licensed offerings and components that you will install using the Provisioning Wizard, and points to a list of post-provisioning tasks to be performed.
- Section 3.4, "Topology: Planning Your Topology": Helps you define the topology to be used and how components will be assigned to each node of the topology.
- Section 4.1, "Network- Virtual Hosts: Planning Network Configuration":Helps you understand networking concepts used by Oracle Fusion Applications as well as prerequisites and how to fulfill them before starting the provisioning process.
- Section 4.2, "Network-Ports: Planning Ports": Shows the default ports and where they can be changed if necessary.
- Section 4.3, "Storage: Planning Storage Configuration": Helps you understand storage requirements and plan for them.

- Section 4.4, "Database: Planning Database Configuration": Explains database usage in Oracle Fusion Applications and helps you plan for the creation of the required databases.
- Section 4.5, "Identity Management: Planning Oracle Identity Management Configuration": Explains key concepts needed to plan for the Oracle Identity Management provisioning and to understand its integration with Oracle Fusion Applications and other components.
- Section 4.6, "SSL and Certificates": Gives tips on completing the SSL and Certificates section of the Workbook.

While all of these areas are equally important, certain areas are more closely related to certain roles, for example, the "Planning the Database" section will normally be used by the database administrator, while the "Planning the Network Configuration" section will normally be of use to network engineers.

3.1.1 Using the Oracle Fusion Applications Installation Workbook

The *Oracle Fusion Applications Installation Workbook* is a companion document to this guide. It is used by the architects, system engineers, and implementers to plan and record all the details for an environment installation (such as server names, URLs, port numbers, installation paths, etc.). The *Oracle Fusion Applications Installation Workbook* is a single input for the entire process, allowing for:

- Separation of tasks between architects, system engineers and implementers
- Comprehensive planning before the implementation
- Validation of planned decisions before actual implementation
- Consistency during implementation
- A record of the environment for future use

A typical use case for the *Oracle Fusion Applications Installation Workbook* is:

- Architect(s) read through the first five chapters of this guide, and fill in the corresponding sections of the *Oracle Fusion Applications Installation Workbook*;
- The *Oracle Fusion Applications Installation Workbook* is validated by other architects and system engineers;
- Architect uses the validated plan to initiate network and system change requests with system engineering departments;
- Implementer or System Integrator uses the *Oracle Fusion Applications Installation Workbook* and the subsequent chapters of this guide as input/instructions to perform the installation and configuration tasks.

3.1.1.1 Oracle Fusion Applications Installation Workbook Structure

The *Oracle Fusion Applications Installation Workbook* is divided into the tabs listed below. Each section of Chapter 3 and Chapter 4 contains a corresponding *Oracle Fusion Applications Installation Workbook* reference section, to guide you in filling out the worksheets step-by-step.

- Environment (Section 3.2)
- Provisioning (Section 3.3)
- Topology (Section 3.4)
- Network - Virtual Hosts (Section 4.1)

- Network - Ports (Section 4.2)
- Storage (Section 4.3)
- Databases (Section 4.4)
- Identity Management (Section 4.5)
- SSL (Section 4.6)

3.1.2 Planning for Platform-Specific Considerations

There are specific platform requirements for desktop tools, the Repository Creation Assistant, OAM modes, the Business Intelligence Applications tool, and print servers.

3.1.2.1 Desktop Tools

Windows only:

- Smart View
- ADF Desktop integration/ADFdi
- Hyperion Financial Reporting Studio
- Financial Reporting Center
- MS Project integrations
- Financials requires print servers on Windows for ODC / OFR

It is also necessary to have network sharing between Windows and non-Windows platforms, in order to use the Windows-only applications.

Power-users may need to set up a Windows Remote Desktop Connection.

3.1.2.2 Repository Creation Assistant (RCU)

Windows or Linux only

The Repository Creation Assistant (RCU) can run against databases on any platform. However, the RCU is only available on the Linux and Windows platforms. This means if you are installing Oracle Fusion Applications on another platform, plan to make a Linux or Windows host available specifically to run the RCU.

3.1.2.3 OAM Modes Supported

OAM modes support for Oracle Fusion Applications depends on the platform being used. For AIX, only **Open** mode is supported at install time. For all other platforms, only **Simple** mode is supported. For more information, see Section 4.5.4, "Oracle Access Manager Transfer Mode".

3.1.2.4 BI Administration Tool

The BI Administration tool is required to manage the Business Intelligence repository and must be used to update database details for Business Intelligence connections. This tool is only available on the Windows platform. Plan to make at least one Windows host available to use this tool.

3.1.2.5 Print Servers

Oracle Financials requires print servers on Windows in order to use Oracle Data Capture/Oracle Forms Recognition.

3.2 Environment: Completing the Environment Tab Entries

The Environment tab includes basic Environment Info, Email settings, and Web Proxy information tables. The basic Info table requires understanding of the topologies described in Section 3.2.1 and Section 3.2.2.

3.2.1 Oracle Identity Management Topologies

The Oracle Identity Management Provisioning Wizard supports three topology types for Oracle Identity Management. These topologies are related to the type of environment being created (e.g. development, test, production) and the desired availability (HA, non-HA). They also play a role in defining which type of identity store will be used (OID or OVD). In the table below, the "Corresponding Sample Topolog[ies]" are described in Section 2.2.

Oracle Identity Management Topology Type	Corresponding Sample Topology	Notes
Single Host	Basic	Recommended for dev/demo environments only Installs all tiers (Directory, Identity and Access, Web) on the same host No LBR required Uses OID as the Identity Store
EDG Topology	Enterprise Non-HA	Recommended for enterprise environments where high-availability is not required. Provides the option to install the 3 tiers on up to 3 different hosts. LBR required Uses OVD as the Identity Store
EDG Topology + Configure second application instances	Enterprise HA	Recommended for enterprise environments with high availability requirements. Provides the option to install the 3 tiers on up to 6 different hosts (with 2 hosts per tier - primary and secondary). LBR required Uses OVD as the Identity Store

3.2.2 Oracle Fusion Applications Topologies

The Oracle Fusion Applications Provisioning Wizard supports three topology types as well, but unlike the Oracle Identity Management topologies, Oracle Fusion Applications topologies are not necessarily related to the type of environment being created (development, test, production) and none of them will provide high availability out of the box. (High availability for Oracle Fusion Applications components must be done manually, as a post-install step). Instead, these topologies define how the various Oracle Fusion Applications components will be split across servers, so the main driver for this decision should be server hardware capacity (memory and processing power).

Additionally, these topologies apply only to the Mid Tier. The Web Tier can use a separate host or, if desired, share the same host with the Mid Tier.

Oracle Fusion Applications Topology Type	Notes
One host for all domains	Recommended for environments where a single server can handle the memory and CPU requirements for all Oracle Fusion Applications mid tier components.
One host per domain	Recommended for environments where a single server cannot handle the memory and CPU requirements for all Oracle Fusion Applications mid tier components, so splitting the domains across different hosts is necessary. This topology allows you to assign entire domains to specific hosts, and different domains can share the same host if desired.
One host per application and Middleware component	Recommended for environments where a single server cannot handle the memory and CPU requirements for all Oracle Fusion Applications mid tier components, so splitting the domains across different hosts is necessary. This topology allows you to assign each individual component (WebLogic AdminServer or Managed Server) to a specific host, allowing for maximum flexibility in component assignment.

3.2.3 Completing the Environment Info Table

This area is informational and used to orient all the people who will interact with this Workbook about the current installation environment.

Table 3–1 Environment

Name	Required	Description
Company Name	No	My Company
Environment Type	Yes	Enter the operating systems used for Oracle Fusion Applications, Oracle Identity Management, and the database(s).
Oracle Fusion Applications Version	Yes	Enter the Oracle Fusion Applications version number you are installing, as well as the Oracle Identity Management version number. Each is important for patching.
Install Type	No	Entries such as "dev", "qa" or "prod" help others understand the use case for this particular installation.
Domain Name	Yes	`www.mycompany.com`
Topology Type for Oracle Fusion Applications	Yes	Enter which type of provisioning-wizard based installation you will run for Oracle Fusion Applications: One host, One host per domain, or One host per application and Middleware component. See Section 3.2.1 for details.
Topology Type for Oracle Identity Management	Yes	Enter the corresponding type of Oracle Identity Management installation you will run: Single Host, EDG (Enterprise), or EDG with added nodes. See Section 3.2.1 for details.

3.2.4 Completing the Email Server Table

During both Oracle Fusion Applications and Oracle Identity Management Provisioning, you are prompted to enter email server information. Oracle Fusion Applications sends emails to end-users and administrators for notification (business processes, Identity Management) and, if CRM is installed, also for marketing purposes. An e-mail server is required to send out these messages and normally the corporate e-mail server is used for this purpose

If you will be using corporate email, fill in the appropriate part of the Oracle Fusion Applications using the table below for guidance.

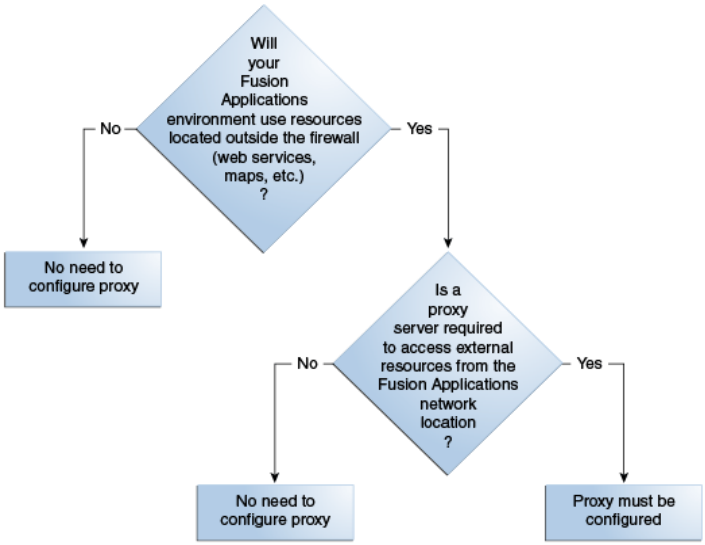
Table 3–2 Environment: Email

Name	Sample Value	Notes
SMTP Server Host	`mail.mycompany.com`	
SMTP Server Port	25	25 is the standard value; other ports can be used.
SMTP Server Security	open	There are two possibilities: open or authentication required. Applies to Oracle Identity Management Provisioning only.
SMTP Username		This user name is only required if server security is not open and requires authentication. Applies to Oracle Identity Management Provisioning only.

3.2.5 Completing the Web Proxy Table of the Oracle Fusion Applications Installation Workbook

Oracle Fusion Applications supports configuring a web proxy host for use whenever Oracle Fusion Applications must access resources (e.g. web services, maps, etc.) that are located outside the firewall. Verify with your network administrator if a proxy server is needed in order for Oracle Fusion Applications to access external resources; if so, then web proxy information must be provided during Oracle Fusion Applications Provisioning.

Figure 3–1 Web Proxy decision tree



Note that this proxy configuration is server-side and not related to the proxy configuration available in end-user's web browsers.

If you are planning to incorporate an existing web proxy into the Oracle Fusion Applications environment, then enter the details in the Workbook, following the guidelines below.

Table 3–3 Environment: Web Proxy

Name	Sample Value	Description
Proxy Host	`proxy.mycompany.com`	

Table 3–3 (Cont.) Environment: Web Proxy

Name	Sample Value	Description
Proxy Port	80 and 443	standard non-SSL and SSL ports are the default
Secure Proxy	yes | no	SSL or non-SSL configuration
Proxy Username		Used if secure proxy is enabled

3.3 Provisioning: Planning the Configuration of Your Provisioned Installation

Oracle Fusion Applications is delivered as a suite, but can be adopted modularly. It can be adopted as a single suite, as product offerings (the highest level collection of functionality that you can license and implement), or as solutions sets that work with other Oracle Applications Unlimited product lines.

The offerings were licensed when Oracle Fusion Applications was purchased, and in the Provisioning Wizard you must select which offerings will be installed as part of the complete Oracle Fusion Applications install. The offerings selected will define, among other things:

- The product families and respective WebLogic domains that will be configured
- The applications that will be installed
- The tech stack components that will be installed

3.3.1 Provisioning: Indicate the Oracle Fusion Applications Offerings You Will Install

This table provides helpful reference for all users of the Workbook.

3.3.1.1 Completing the Oracle Fusion Applications Offerings Table

Enter the Oracle Fusion Applications product offerings that were licensed by your enterprise.

Family	Offering	Install? (Y or N)
Oracle Fusion Customer Relationship Management	Marketing	
	Sales	
Oracle Fusion Financials	Financials	
	Procurement	
	Projects	
Oracle Fusion Human Capital Management	Workforce Deployment	
	Workforce Development	
	Compensation Management	
Oracle Fusion Supply Chain Management	Product Management	
	Order Orchestration	
	Material, Management and Logistics	

Family	Offering	Install? (Y or N)
Oracle Fusion Customer Data Hub		
Oracle Fusion Enterprise Contracts		
Oracle Fusion Accounting Hub		
Oracle Fusion Incentive Compensation		

3.3.2 Provisioning: Describe the Oracle Identity Management Components

The Oracle Identity Management installation also includes multiple components, all of which are installed by default. Note that Oracle Identity Federation (OIF) is not automatically configured and its use is optional.

To review the Oracle Identity Management Toplogies, see Section 3.2.1.

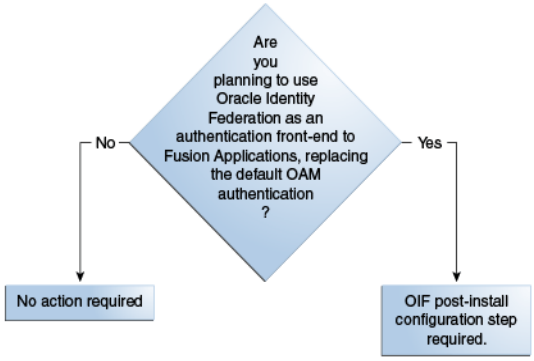
To see a discussion about the Identity Store and whether to use OID or OVD for that purpose, see Section 4.5.1, "Identity Store Planning".

A brief discussion about whether to use OIF is below.

3.3.2.1 OIF

Oracle Identity Federation is installed by default, and can be used for federation. The federation package of standard protocols allows Oracle Identity Management to communicate with an external identity or service provider. See Section 16.10.3, "Configuring Oracle Identity Federation" for details.

Figure 3–2 Oracle Federation Decision Tree



3.3.2.2 Completing the Oracle Identity Management Components Table

By default, all the components will be installed by the Provisioning Wizard. You can annotate your decisions regarding topolgy, Identity Store, and OIF usage in the workbook.

3.3.3 Provisioning: Select the Patches You Want to Apply

Certain patches or bundles may be required for your installation which are not included in the downloaded install files. Check the *Oracle Fusion Applications Release*

Notes for mandatory patches to the Oracle Fusion Applications database, Oracle Identity Management, and Oracle Fusion Applications core. If you plan to install any languages in addition to US English, check the *Oracle Fusion Applications NLS Release Notes* for mandatory patches for languages.

For general information about applying patches to an applications environment, see the *Oracle Fusion Applications Patching Guide*. For database patches, check:

- Oracle Identity Management: Section 7.2.2
- Oracle Fusion Applications: Section 8.2.2.4

3.3.4 Provisioning: Select the Post-Installation Tasks You Want to Perform

The **Post-Install Tasks** table lists all of the mandatory and conditional post-installation activities. These are described in Part VII, "Completing Oracle Fusion Applications Post-Installation Tasks".

Conditional tasks are performed only if your environment meets the criteria defined for those tasks. Cross-refer to the table in(Part VII) to determine whether conditional post-install tasks apply in your case, and enter your decisions as appropriate in the Workbook.

3.3.4.1 Select Languages

If you plan to install any languages in addition to US English, select the languages to install from the following list of supported languages.

- Arabic (ar / AR)
- Chinese (Simplified) (zh_CN / ZHS)
- (Chinese (Traditional) (zh_TW / ZHT)
- Czech (cs / CS)
- Danish (da / DK)
- Dutch (nl / NL)
- Finnish (fi / SF)
- French (fr / F)
- French (Canadian) (fr_CA / FRC)
- German (de / D)
- Hebrew (iw / IW)
- Hungarian (hu / HU)
- Italian (it / I)
- Japanese (ja / JA)
- Korean (ko / KO)
- Norwegian (no / N)
- Polish (pl / PL)
- Portuguese (Brazilian) (pt_BR / PTB)
- Russian (ru / RU)
- Spanish (es / E)

- Swedish (sv / S)
- Turkish (tr / TR)

3.4 Topology: Planning Your Topology

"Topology planning" refers to the tasks related to:

- Determining how many and what type of servers are going to be used for the environment
- Defining their logical location in the network
- Defining which Oracle Fusion Applications component(s) will run on each server
- Deciding how to handle the Demilitarized Zone (DMZ) is part of network and topology planning. A special section is devoted to this topic when completing the Topology tables in the Workbook.

While the number of nodes, their characteristics, and even component allocation are likely to have already been defined during the sizing/licensing phase, this is the moment in the planning phase where you will review them and make any remaining topology decisions or adjustments.

Remember that if you choose to clone a topology in order to maintain a test or staging backup, the two environments must match from the beginning. It is not possible to move from a "Basic" topology, used for development, to an "Enterprise" topology for production, using cloning tools.

Therefore, in this case we recommend that topology decisions consider not only the immediate environment needs, but also future changes to this environment, as well as other environments that will be created through cloning.

3.4.1 Reviewing Component and Server Allocation

Component assignment to specific servers will normally have already been done during the sizing phase of the project, but this is a good time to review those decisions since, once installed, Oracle Identity Management and Oracle Fusion Applications components cannot usually be moved to other servers.

When reviewing component allocation, consider the following:

- CPU capacity
- Amount of memory available on the server vs. what is required by the assigned components
- Network location (for example: DMZ)
- Access to shared storage
- Scale-out nodes should have the same characteristics as the corresponding primary node

3.4.2 Completing the Topology Tab of the Oracle Fusion Applications Installation Workbook

Follow the explanations for each column name to fill in the **Topology** table:

- **Nodes:** Typically, an installation consists of a minimum of three nodes: one for the transactional database, one for Oracle Identity Management, and one for Oracle Fusion Applications. (This would be the "Basic" topology.) If this were your

situation, you would list each component next to Node numbers 1-3, entering the Real Host Name. If you have chosen multiple hosts for Oracle Fusion Applications, and/or used additional Oracle Identity Management or database hosts, then assign each of them to an additional node number.

The node number is simply used as a reference number, for user ease, when filling in the Workbook.

- **Real Host Name:** This is the name assigned in the operating system. The network administrator who sets up the server should provide this information. (DMZ information may be applicable to the Oracle Identity Management Web Tier (line 25) and/or the Oracle Fusion Applications Web Tier (line 35) of the Component Assignment table.
- **Abstract Host Name:** If the DNS hostname used to address the host is different from the hostname defined at the operating system, add it to this column as the abstract hostname. The abstract hostname column can also be used if you prefer to configure Oracle Fusion Applications with hostnames defined in the hosts file of the operating system (allowing the use of more generic names like `fadbhost` or `idmwebhost`) instead of the actual hostnames
- **IP Address**: Get this information from the network administrator. This column is informational only and is not used during the install process.
- **Operating System**: Use this column to specify the operating system of the host. Get this information from the network administrator. This column is informational only and is not used during the install process.
- **CPUs**: Enter the CPUs on the table. This column is informational only and is not used during the install process.
- **RAM**: Enter the amount of RAM available in this host. The command to retrieve RAM information depends on the operating system. This column is informational only and is not used during the install process.
- **DMZ**: The network administrator will also know whether the host is located in the DMZ; for more information about that decision, see Section 3.4.3.

When the Topology table is complete, you define which components will reside on each host. Remember that most of this was specified during the sizing phase.
To fill in the **Component Assignment** table:

- Check the Node numbers you assigned to each host in the Topology table. For example, if you used the 3-node setup, you could have made the following assignments:
  Oracle Fusion Applications and Oracle Identity Management database = Node 1
  Oracle Identity Managementmid tier and web tier = Node 2
  Oracle Fusion Applications mid tier and web tier = Node 3

- Now you can fill out the Component Assignment table by listing the appropriate node for each component. In the Basic 3-node example we are using, that would mean:
  - **FADB** and **IDMBDB**: You would add the number **1** to the " **Node #**" column for the rows that contain the components FA DB and IDM DB.
  - **OIDDB** and **FADW** (Data Warehouse): Since you would not be installing a separate OID Database or a Data Warehouse, you would leave the **Node #** column for those components blank or add N/A.

- **IDM Directory**, **IDM Identity and Access**, and **IDM Web Tier** : You would add the number **2** to the " **Node #**" column for the rows that contain the Oracle Identity Management mid tier and web tier components (IDM Directory, IDM Identity and Access, and IDM Web Tier).
- All remaining **FA-** components: You would add the number **3** to the " **Node #**" column for the rows that contain the Oracle Fusion Applications mid tier and web tier components (all FA domains and the FA Web Tier).

  Adapt this example to match your own environment, using the **HA/Scale-Out Node** column if needed.

3.4.3 Topology: Understanding DMZ Requirements

Oracle Fusion Applications Provisioning has the option automatically to configure the Oracle Fusion Applications Web Tier for deployment on a Demilitarized Zone (DMZ). However, in some cases it is more advantageous to handle the DMZ and security in alternate ways. For example, if your enterprise already has a load balancer in the DMZ, it is not necessary to duplicate that function by installing the Oracle Fusion Applications Web Tier there.

Auto-deploying the Web Tier on a DMZ implies that:

- The Web Tier Middleware Home (binary files) and the OHS instance (including WebGate) will be installed on separate storage from the shared Oracle Fusion Applications/ Oracle Identity Management storage.
- The Web Tier must be installed on a separate server.
- During Provisioning, the Web Tier install will take place separately from the main install, taking into consideration the fact that the DMZ is isolated in terms of storage, server and network.

When deciding whether to use this option, consider the following:

- **Requirements:** Is access from the outside network required, which would justify providing an entry point into Oracle Fusion Applications on the DMZ?
- **Maintenance:** Is it worth the maintenance for servers residing in the DMZ given the restricted server access and restricted access to storage, which can impact maintenance, patching, debugging, etc.?
- **Other Options:** Do you have existing infrastructure to enable external access (VPN, DMZ Web Servers, DMZ Load Balancers and Reverse Proxies, etc.)? Depending on your requirements, it may be possible to provision Oracle Fusion Applications without the Web Tier on the DMZ, simply using your existing infrastructure on the DMZ to forward requests to the Oracle Fusion Applications Web Tier.
- **Firewall Openings:** Placing the Oracle Fusion Applications Web Tier on the DMZ can have a bigger impact on required firewall openings, compared to placing the Web Tier on the internal network and using a DMZ Web Server/Proxy to forward requests to Oracle Fusion Applications, as the diagrams show.

Figure 3–3 Port Openings Required with Web Tier in the DMZ

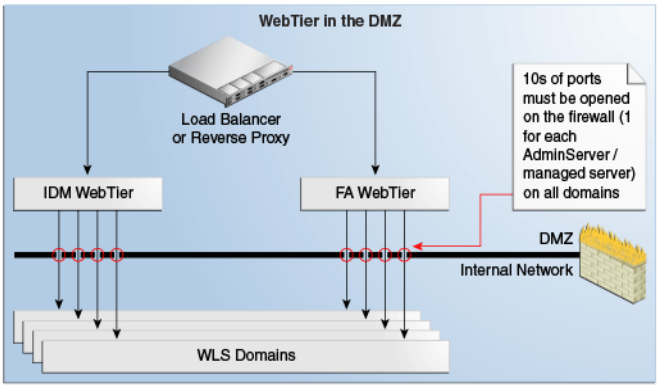
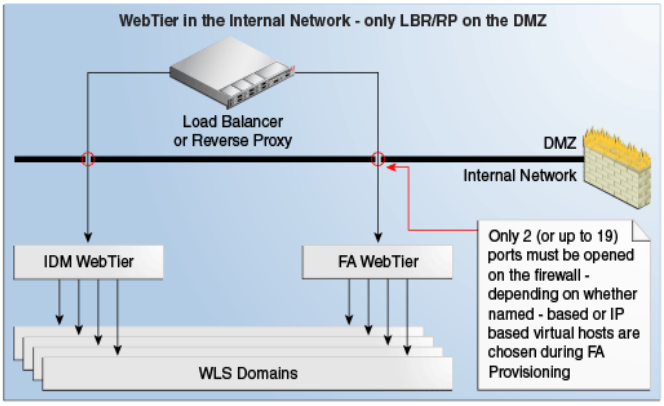


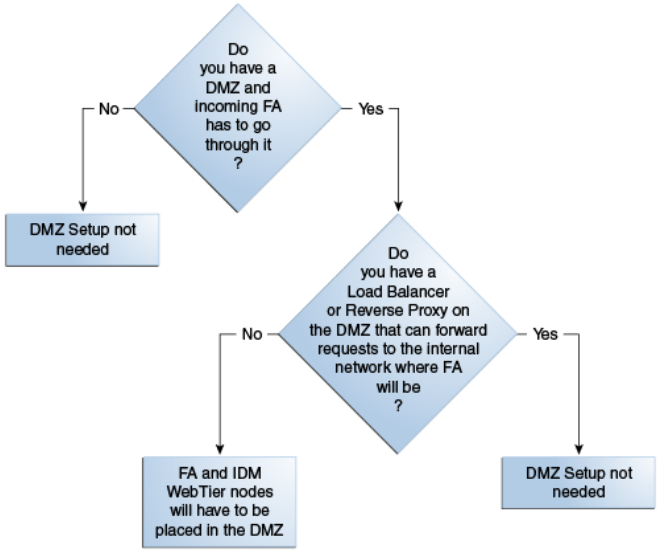
Figure 3–4 Port Openings Required when Web Tier is Not In DMZ



Note that from the Load Balancer/ Reverse Proxy going to the Web Tier, the number of port openings is small and can be minimized by selecting certain options during Provisioning. At a minimum, one port opening for Oracle Identity Management and one port opening for Oracle Fusion Applications will be required.

On the other hand, going from the Web Tier to the Mid Tier, port openings would be required for each managed server that receives requests from the Web Tier. This number cannot be minimized, as Oracle Fusion Applications uses different ports for each managed server.

Figure 3–5 DMZ Decision Tree



3.4.3.1 Completing the DMZ Column in the Topology Table

Decide with your network administrator how to configure components in the DMZ based on the considerations above, and enter Yes or No as appropriate in the DMZ column for each node in the Topology table.

3.5 What to Do Next

Proceed with Chapter 4 planning tasks to complete your plan and your *Oracle Fusion Applications Installation Workbook*.

4

Planning the Configuration of the Components of Your Installation

This chapter contains the following sections, each of which corresponds to a tab in the *Oracle Fusion Applications Installation Workbook*:

- Network- Virtual Hosts: Planning Network Configuration
- Network-Ports: Planning Ports
- Storage: Planning Storage Configuration
- Database: Planning Database Configuration
- Identity Management: Planning Oracle Identity Management Configuration
- SSL and Certificates
- What to Do Next

4.1 Network- Virtual Hosts: Planning Network Configuration

Filling in the **Network-Virtual Hosts** tab of the *Oracle Fusion Applications Installation Workbook* entails understanding and deciding about a range of Oracle Fusion Applications concepts and conventions.

- **Internal vs External URLs:** See Section 4.1.1, "Understanding Internal vs. External URLs", to orient yourself to how Oracle Identity Management and Oracle Fusion Applications provisioning uses these concepts.
- **Naming:** All parts of the network-related decisions involve choosing appropriate names for various endpoints. These will be used throughout the installation, both for internal communication between Oracle Fusion Applications components and externally, to be viewed by users.
  Section 4.1.2, "Naming Conventions in Oracle Fusion Applications", gives important orientation on how to name endpoints throughout the installation.
- **Load Balancer:** Next, you must decide whether your availability and topology requirements demand the use of Load Balancers (LBR) or a Reverse proxy. For an introduction to the use of Load Balancers and Reverse proxy in Oracle Fusion Applications topologies, see Section 2.2.2, "Network Components".

  These decisions are further described in Section 4.1.3, "Planning Load Balancer Requirements"
- **Web Tier/HTTP Servers:** You must also make decisions about the Web Tier. Oracle HTTP Servers (OHS) for Oracle Identity Management and Oracle Fusion

Applications will be installed on the Web Tier. Again you must decide where on the network they will reside and whether they are in the DMZ.

This is described in Section 4.1.4, "Planning HTTP Server Requirements".

Virtual Host Mode: A property of the Web Tier is the Virtual Host Mode. It can be name-based, port-based, or IP-based. These options are described in Section 4.1.4.1, "Defining Web Tier Virtual Host Mode".

- **Virtual IPs (VIPs) for Administration and Managed Servers:** VIPs apply to all Enterprise topologies for Oracle Identity Management. For Oracle Fusion Applications, VIPs apply only to Enterprise-HA topologies. VIP overview information is described in Section 4.1.5, "Defining VIPs for Administration and Managed Servers".
- When each of these subjects has been reviewed and decisions about them have been made, you will be ready for Section 4.1.6, "Completing the Network-Virtual Hosts Tab of the Oracle Fusion Applications Installation Workbook".

4.1.1 Understanding Internal vs. External URLs

Both the Oracle Identity Management and the Oracle Fusion Applications install procedures use the concept of *internal* and *external HTTP endpoints* as part of their service-oriented architecture. External HTTP endpoints are used by end-users to access the system and are used for the login screen, welcome pages, transaction pages, online help, and so on. Internal HTTP endpoints are not meant to be seen by end-users and instead are used for inter-component communication.

This distinction exists for security as well as topology reasons, allowing for maximum flexibility when deploying Oracle Fusion Applications on an enterprise environment. Since internal endpoints are not exposed externally, this provides a layer of security, and since internal traffic can easily be restricted to specific network segments, there is no need for extra security measures such as encryption. External HTTP endpoints allow for maximum topology flexibility: since they are the only external entry points for all Oracle Fusion Applications traffic, they are the only points in the topology that must be directly accessible to the external world; all other components can be located inside a firewall while still providing 100% access to end-users and other applications that integrate with Oracle Fusion Applications.

Both external and internal endpoints can be configured directly at the HTTP Server (in which case internal and external URLs will point at the HTTP Server) or can be configured at a Load Balancer or Reverse Proxy (in which case internal and external URLs will point at the LBR/RP and it in turn must be configured to point at the HTTP Server).

4.1.2 Naming Conventions in Oracle Fusion Applications

These conventions are used when naming URLs/endpoints within Oracle Fusion Applications, Oracle Identity Management, and in any load balancer that may be used.

4.1.2.1 Planning URL Naming Conventions

Naming conventions for network configuration are extremely important, since they will define the URLs that will be used by end-users to access the system, as well as defining all the internal "wiring."

When choosing hostnames for external HTTP endpoints, choose meaningful, easy-to-remember names, as they will be used by end-users.

When choosing hostnames for servers, virtual IP addresses (VIPs), and internal HTTP endpoints, note the following:

- These names will be used for all Oracle Fusion Applications-Oracle Fusion Applications addressing.
- Once chosen, these names cannot be changed!
- It is best to use environment-neutral (abstract) names, rather than names that include clues such as "test" or "prod" or "staging". Since the names are used to maintain internal wiring, they may be deployed on more than one environment (for example, if you clone an installation). Choose environment-neutral names to avoid headaches later.

4.1.3 Planning Load Balancer Requirements

A Load Balancer (LBR) is required for scaled-out enterprise topologies. It is used to balance and route:

- External HTTP traffic from end-users to the Oracle Fusion Applications and Oracle Identity Management Web Tiers
- Internal HTTP traffic from the mid tiers to the Web Tiers (for both Oracle Fusion Applications and Oracle Identity Management)
- Internal LDAP (TCP) traffic from mid tiers to the Identity and Policy Stores (directory tier)
- Internal TCP traffic from the Oracle Fusion Applications mid tier to the Oracle WebCenter Content (UCM) socket listeners

If the topology is not scaled out, an LBR/Reverse proxy is not mandatory, but it is recommended for enterprise topologies with the following characteristics:

- External access requiring that traffic go through a DMZ with the Oracle Fusion Applications Web Tier located in the internal network
- The environment is not currently scaled out but may be in the future

For development environments, an LBR/RP is normally not required or used. In this case, the Provisioning framework can have the LBR option turned off which will set up the Web Tier (OHS) as the HTTP endpoint for Oracle Fusion Applications.

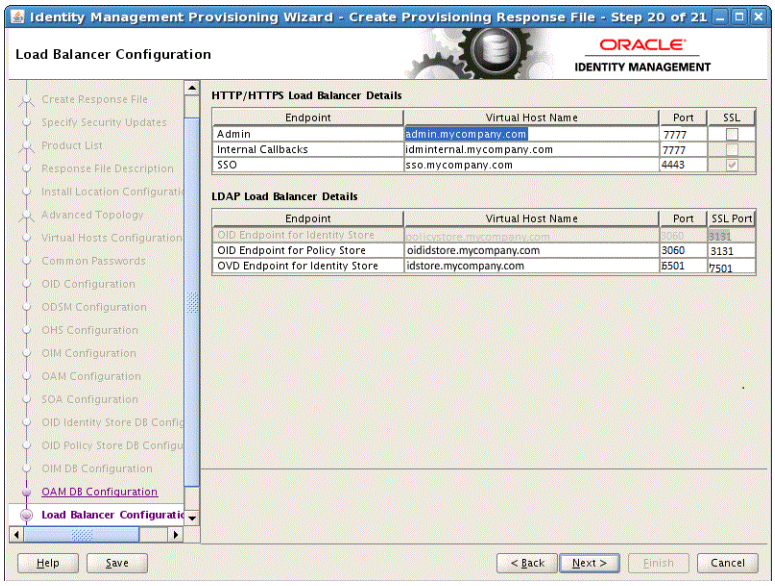
4.1.3.1 SSL Certificate Requirements

Both Oracle Identity Management and Oracle Fusion Applications terminate SSL connections at the LBR. Therefore, it is necessary to set up the appropriate SSL certificates on the LBR prior to starting the provisioning process. More details are provided in Section 4.6, "SSL and Certificates".

4.1.3.2 How the Load Balancer Option Affects the Environment Setup

When Provisioning Oracle Identity Management

When running the Oracle Identity Management Provisioning Tool, the load balancer option not available with the "Single-host" install. The other alternative, "EDG" topology, prompts for three IDM HTTP endpoints and three LDAP endpoints.



The requirements for this screen are described in the table below:

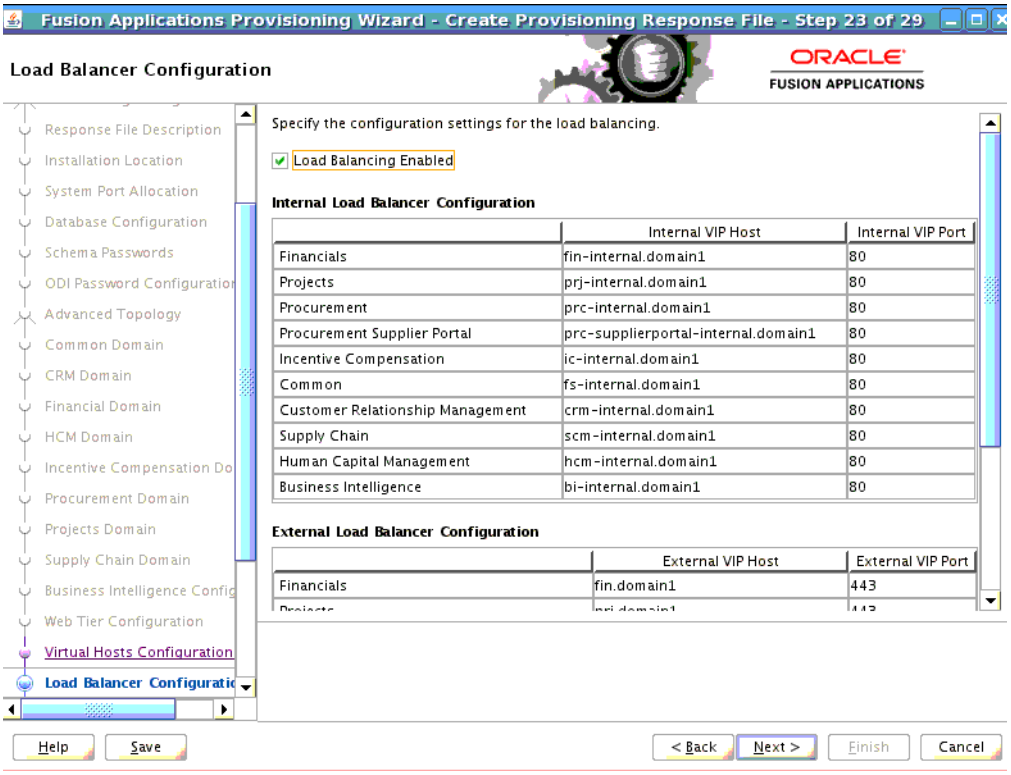
Table 4–1 Load Balancer SSL Requirements

Endpoint Type	SSL?	Description
HTTP/HTTPS Requirements		
Admin	Optional	Defines the host configuration on the Oracle HTTP Server (specifically the ServerName clause on the virtual host configuration `.conf` files)
Internal	Not allowed	Defines the URLs configured internally for the HTTP endpoints
SSO	Required	
LDAP Requirements		
OID Endpoint		LDAP LBR endpoints are only used for the URLs configured internally for the LDAP endpoints.
OVD Endpoint		

All load balancer configuration must be performed by the network administrators; the Oracle Identity Management Provisioning process does not automate that or provide any specific settings for load balancer/reverse proxy configuration.

When Provisioning Oracle Fusion Applications

For Oracle Fusion Applications provisioning, the load balancer option is available for any topology. All load balancer configuration, adding internal and external virtual IP host and port, must be performed by the network administrators before you start provisioning Oracle Fusion Applications. The Oracle Fusion Applications Provisioning process does not install load balancer or provide any specific settings for load balancer/reverse proxy configuration. For more information about planning load balancer requirements, see Section 4.1.3, "Planning Load Balancer Requirements".



If selected, this setting will affect:

- Virtual host configuration on the Oracle HTTP Server (more specifically the ServerName clause in the virtual host configuration `.conf` files)
- The URLs configured internally for the HTTP endpoints.

> **Note:** Whether or not the load balancer is selected has an affect on the SSL configuration at the OHS. This is discussed in Section 4.1.3.1.

4.1.3.3 Network Placement of Load Balancers/Reverse Proxy

If you decide to use a load balancer/reverse proxy, it is important to consider where on the network it should be placed, and whether firewalls exist between it and the Oracle Fusion Applications mid tier and Web Tier.

For example, if a load balancer is placed in the DMZ and is configured for both internal and external Oracle Fusion Applications traffic, this may be undesirable for security reasons. (In this case, internal traffic from the Oracle Fusion Applications and Oracle Identity Management mid tiers will go through the DMZ to get to the respective web tiers.) Additionally, firewall ports may have to be opened for traffic from the internal network to the DMZ, and TCP traffic (for LDAP and UCM) will be going through the DMZ.

In this case, placing an additional load balancer on the internal network is recommended for internal traffic (HTTP and TCP), to prevent it from going through the DMZ.

The following diagrams show both scenarios in more detail:

Figure 4–1 Load Balancer Placed Outside the internal Network

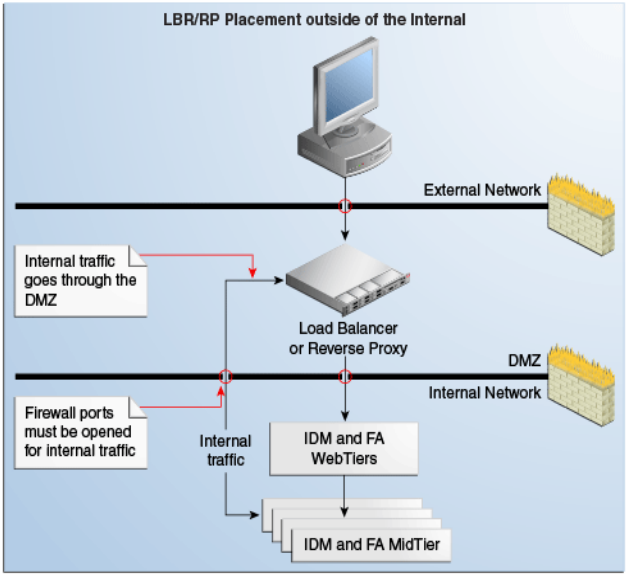
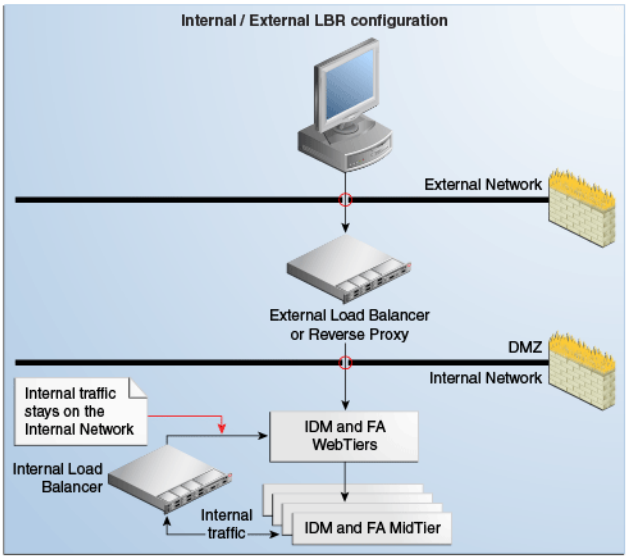
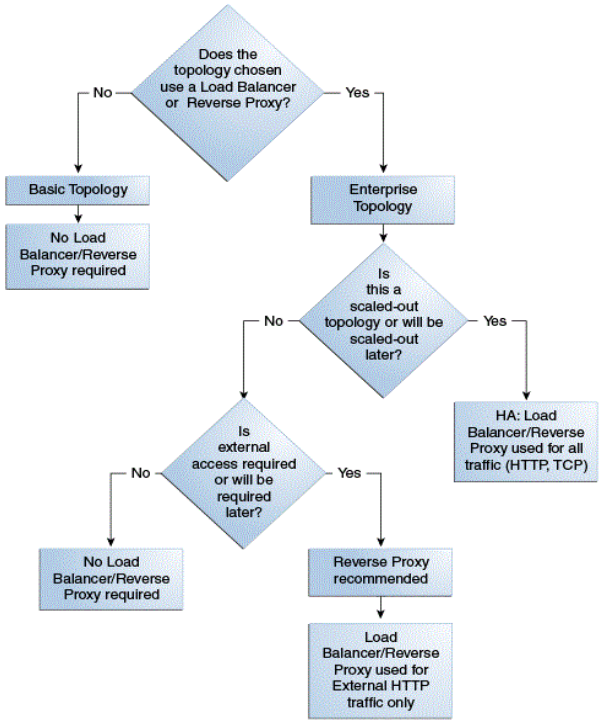


Figure 4–2 Internal/External LBR Configuration



Follow the decision tree to plan the usage and placement of a load balancer, and to fill out the *Oracle Fusion Applications Installation Workbook* appropriately. Enter decisions on the **Environment** tab, **Environment Info** table, *Load Balancer/Reverse proxy* row.

Figure 4–3 Load Balancer/Reverse Proxy Decision Tree



4.1.3.4 Load Balancer Feature Requirements

Several virtual servers and associated ports must be configured on the load balancer for different types of network traffic and monitoring. These should be configured to the appropriate real hosts and ports for the services running. Also, the load balancer should be configured to monitor the real host and ports for availability so that the traffic to these is stopped as soon as possible when a service is down. This ensures that incoming traffic on a given virtual host is not directed to an unavailable service in the other tiers.

If your topology uses a load balancer, it must have the following features:

- **Ability to load-balance traffic to a pool of real servers through a virtual host name:** Clients access services using the virtual host name (instead of using actual host names). The load balancer can then load-balance requests to the servers in the pool.
- **Port translation** configuration
- **Port monitoring** (HTTP and HTTPS)
- **Resource monitoring / port monitoring / process failure detection:** The load balancer must be able to detect service and node failures (through notification or some other means) and to stop directing non-Oracle Web traffic to the failed node. If your external load balancer has the ability to automatically detect failures, you should use it.
- **Ability to Preserve the Client IP Addresses:** The load balancer must have the capability to insert the original client IP address of a request in an `X-Forwarded-For` HTTP header to preserve the Client IP Address.
- **Virtual servers and port configuration:** Ability to configure virtual server names and ports on your external load balancer.

Note that there are also requirements for the virtual server names and ports, as follows:

- The virtual server names must be associated with IP addresses and be part of your DNS. Clients must be able to access the external load balancer through the virtual server names.
- The load balancer should allow configuration of multiple virtual servers, and for each virtual server, the load balancer should allow configuration of **traffic management on more than one port**. For example, for Oracle WebLogic Clusters, the load balancer must be configured with a virtual server and ports for HTTP and HTTPS traffic.

The last list of features are recommended, though not required for every topology:

- It is recommended that you configure the load balancer virtual server to return immediately to the calling client when the back-end services to which it forwards traffic are unavailable. This is preferred over the client disconnecting on its own after a time-out based on the TCP/IP settings on the client machine.
- SSL termination is used in the Oracle Identity Management EDG topology as well as all Oracle Fusion Applications topologies. This is the ability to terminate SSL requests at the load balancer and forward traffic to the back-end real servers using the equivalent non-SSL protocol. (For example, the load balancer must be able to forward HTTPS requests as HTTP.)
- Configure the virtual servers for the Directory Tier in the load balancer with a high value for the connection time-out for TCP connections. This value should be more than the maximum expected time over which no traffic is expected between Oracle Access Manager and the Directory Tier.
- It is recommended that you configure the load balancer to be in fault-tolerant mode.
- SSL acceleration is recommended, but not required. This refers to off-loading the public-key encryption algorithms involved in SSL transactions to a hardware accelerator.
- Have the ability to add `WL-Proxy-SSL: true` to the HTTP Request Header. Some load balancers do this automatically.

4.1.4 Planning HTTP Server Requirements

Both Oracle Identity Management and Oracle Fusion Applications Provisioning will install their own Oracle HTTP Server, which is the primary endpoint for all HTTP traffic, both internal and external. While each provisioning tool may configure its HTTP Server slightly differently, it is important that the planning phase take both into consideration when deciding:

- Naming convention for virtual hosts
- DMZ placement
- Port usage

Note the following default setups:

- Oracle Identity Management Provisioning requires hostnames for only the LBR endpoint. The OHS listeners and name-based virtual hosts are set up with wildcards. Oracle Fusion Applications, however, always requires hostnames for the OHS endpoints even when using an LBR, and its virtual hosts are set up using those hostnames. This has implications when choosing name-based vs. IP or

port-based virtual hosts for Oracle Fusion Applications.

- Both Oracle Identity Management and Oracle Fusion Applications Provisioning terminate SSL connections at the LBR (external HTTP endpoints only). This means that when the LBR option is selected during provisioning, the OHS virtual hosts will not be configured with an SSL listener and therefore the connection between the LBR and OHS will always be non-SSL and SSL certificates must be set up at the LBR.

  On the other hand, if the LBR option is NOT selected, the consequences differ.

  For Oracle Identity Management, only the "Basic" topology allows no LBR. In this case, OHS is configured with no SSL for all internal, external and admin virtual hosts.

  For Oracle Fusion Applications Provisioning, the OHS will be set up with SSL on the external virtual hosts, which will require installing SSL certificates.

4.1.4.1 Defining Web Tier Virtual Host Mode

Oracle Identity Management Provisioning always uses name-based virtual hosts.

Oracle Fusion Applications Provisioning allows you to choose which method you prefer:

- Port-based
- Name-based
- IP-based

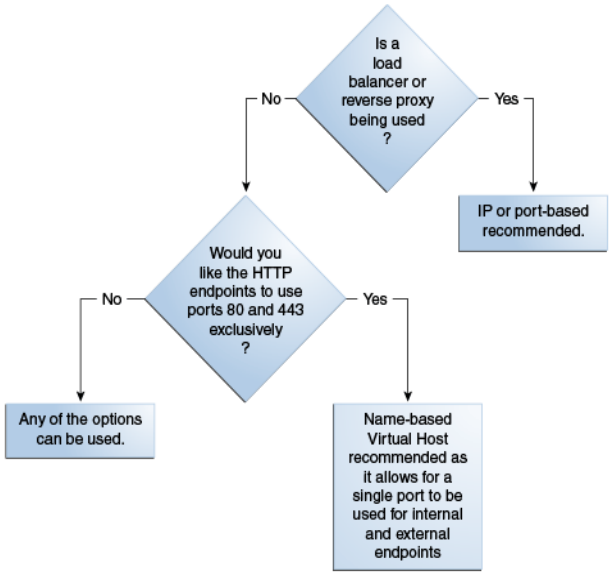
The choice depends on whether a load balancer is used or not, and the hostname/port convention desired for endpoints.

If a load-balancer is used, then IP- or Port-based mode is used.

The following table shows the parameters.

Virtual Host Configuration	Description	# of Ports	# of Host Names
Port-based	Based on the incoming port	2 per domain (one internal and one external)	No virtual hosts will be used
Name-based	Based on the incoming host name	2: one internal (non-SSL) and one external (SSL)	2 per domain (one internal and one external)
IP-based	Based on IP:Port combination	At least 1 and up to 2 per domain (one internal and one external)	At least 1 and up to 2 per domain (one internal and one external)

Figure 4–4 Choosing Virtual Host Mode; Name-, Port- or IP-Based



4.1.5 Defining VIPs for Administration and Managed Servers

A virtual IP address is an unused IP Address which belongs to the same subnet as the host's primary IP address. It is assigned to a host manually and Oracle WebLogic Managed servers are configured to listen on this IP Address. In the event of the failure of the node where the IP address is assigned, the IP address is assigned to another node in the same subnet, so that the new node can take responsibility for running the managed servers assigned to it.

4.1.5.1 Define VIPs for Oracle Identity Management

The following is a list of the Virtual IP addresses required by Oracle Identity Management:

- **IDMDomain AdminServer:** In Enterprise deployments, the WebLogic Administration Server must be able to continue processing requests even if the host on which it resides fails. A virtual IP address should be provisioned in the Application Tier so it can be bound to a network interface on any host in the Application Tier. The WebLogic Administration Server is configured later to listen on this virtual IP address. The virtual IP address fails over along with the Administration Server from IDMHOST1 to IDMHOST2, or vice versa.
- **IDMDomain SOA Server:** One virtual IP address is required for each SOA managed server. This enables the servers to participate in Server migration. Provision a virtual IP address in the Application Tier so it can be bound to a network interface on any host in the Application Tier.
- **IDMDomain OIM Server:** One virtual IP Address is required for each Oracle Identity Manager managed server. This enables the servers to participate in Server migration. Provision a virtual IP address in the Application Tier so it can be bound to a network interface on any host in the Application Tier.

4.1.5.2 Define VIPs for Oracle Fusion Applications

Configure the Administration Server and the Managed Servers to listen on different virtual IPs. Oracle Fusion Applications VIPs are required in Enterprise-HA topologies to configure specific components:

- Virtual IPs for AdminServer are needed for every domain to configure AdminServer in active-passive mode. These VIPs are shared across primary and secondary hosts, depending on where the Administration Server is running.
- Virtual IPs for all Oracle SOA Suite servers in every domain, and Oracle Business Intelligence servers in the Oracle Business Intelligence domain are needed to support server migration. These components are implemented in active-active mode, so these VIPs are needed for primary and secondary hosts.

4.1.6 Completing the Network-Virtual Hosts Tab of the Oracle Fusion Applications Installation Workbook

The Network-Virtual Hosts tab includes the following tables:

- Section 4.1.6.1, "Complete the Web Tier Virtual Host Mode Table"
- Section 4.1.6.2, "Complete the FA Web Tier Virtual Hosts Table"
- Section 4.1.6.3, "Complete the IDM Web Tier Virtual Hosts Table"
- Section 4.1.6.4, "Complete the LDAP Endpoints Table"
- Section 4.1.6.5, "Complete the UCM LBR Endpoint Table"
- Section 4.1.6.6, "Complete the HTTP LBR Endpoints Table"
- Section 4.1.6.7, "Complete the AdminServer Virtual Hosts/VIPs Table"
- Section 4.1.6.8, "Complete the Managed Server Virtual Hosts/VIPs Table"

4.1.6.1 Complete the Web Tier Virtual Host Mode Table

Select the appropriate virtual host mode (name-, port-, or IP-based), as determined in Section 4.1.4.1

4.1.6.2 Complete the FA Web Tier Virtual Hosts Table

How you complete this table depends on the Virtual Host Mode you chose (Section 4.1.4.1. Each row of the table is described in Section 4.1.6.2.1; the mode-based usage is as follows:

Port-Based

- **Internal and External Hostnames:** Will not be used. Leave them blank or mark N/A.
- **Ports:** The *Oracle Fusion Applications Installation Workbook* provides the default ports to be used; they are the same as the defaults presented on the Provisioning Wizard. We recommend keeping the defaults (see Section 4.2.1 for details if needed).

Name-Based

- **Internal and External Hostnames:** Select the external and internal hostnames to be used for the Oracle Fusion Applications Web Tier. The *Oracle Fusion Applications Installation Workbook* provides the defaul hostnames as presented on the Provisioning Wizard. See Section 4.1.2.1, "Planning URL Naming Conventions", for more detail. **Note**: this virtual host mode is not recommend for use with a load

balancer, as indicated in Section 4.1.4.1, "Defining Web Tier Virtual Host Mode".

- **Ports:** In name-based mode, you should not use the "Internal Port" or " External Port" columns. Make them blank or mark them N/A.
  The reason is that in this mode, the default ports defined for the Oracle Fusion Applications HTTP Server are used by the Provisioning Wizard as follows:

  - **Internal Port:** *Oracle Fusion Applications Installation Workbook* - **Network-Ports** tab -> **Fusion Applications Port Numbers** -> *FA Oracle HTTP Server*

  - **External Port:** *Oracle Fusion Applications Installation Workbook* - **Network-Ports** tab -> **Fusion Applications Port Numbers** -> *FA Oracle HTTP Server SSL*.

IP-Based

This mode lets you select both port and hostname and has the defaults as presented on the Provisioning Wizard.

- **Internal and External Hostnames:** Select the external and internal hostnames to be used for the Oracle Fusion Applications Web Tier. See Section 4.1.2.1, "Planning URL Naming Conventions", for more detail.
- Ports: We recommend keeping the default port numbers, as mentioned in Section 4.2.1, "Using Default vs. Custom Port Numbers".

In all three modes, the **IP Address** column should contain the IP address of the host that will run the Oracle Fusion Applications Web Tier. They will normally be all the same.

4.1.6.2.1 FA Web Tier Virtual Hosts Table Rows Defined

A general description of each row is below. How you use them depends on the Virtual Host Mode, above.

- **FA Web Tier Internal Name:** The internal and external names point to the Oracle Fusion Applications Web Tier host or hosts. It can be advantageous/more user-friendly to assign names that indicate their use; for example, the Financials preceded by `fin-ext` (external) or `fin-int` (internal), as shown in the defaults. If you assign a name that differs from the default structure, it will need to be added to the `/etc/hosts` file (or equivalent `/hosts` for Windows).
- **Internal Port:** The default ports are provided by the Provisioning Wizard and are pre-entered in the *Oracle Fusion Applications Installation Workbook*. Change only if necessary for your enterprise. Different ports must be assigned to each product.
- **FA Web Tier External Name:** The internal and external names point to the Oracle Fusion Applications Web Tier host or hosts. It can be advantageous/more user-friendly to assign names that indicate their use; for example, the Financials preceded by `fin-ext` (external) or `fin-int` (internal), as shown in the defaults. If you assign a name that differs from the default structure, it will need to be added to the `/etc/hosts` file (or equivalent `/hosts` for Windows).
- **External Port:** The default ports are provided by the Provisioning Wizard and are pre-entered in the *Oracle Fusion Applications Installation Workbook*. Change only if necessary for your enterprise. Different ports must be assigned to each product.
- **IP Address:** Provide the IP address of the Oracle Fusion Applications Web Tier.

4.1.6.3 Complete the IDM Web Tier Virtual Hosts Table

The Oracle Identity Management Web Tier hosts must share a common port. The IP address points at the Oracle Identity Management Web Tier.

External, Internal and Admin hostnames cannot be chosen. They will default to the hostname defined in the **Topology** tab -> **Topology** table for the component "IDM Web Tier," and will be greyed out on the Provisioning Wizard.

4.1.6.4 Complete the LDAP Endpoints Table

The entries in this table differ depending on whether you chose the "Single Host" or "EDG" topology for Oracle Identity Management. Check your *Oracle Fusion Applications Installation Workbook*: **Environment** tab, *Environment Info* table, IDM Topology Type. To fill in this table, follow these steps:

Determine whether you are using Single-host or EDG topology.

If Single-host, then enter the abstract hostname (or real hostname if not using an abstract one) for the node where you assigned the "IDM Directory" component in the Topology tab. When you run the Oracle Identity Management Provisioning Wizard, these values will be automatically pre-populated and greyed out. They cannot be changed.

If EDG, then you can choose virtual host names for the Policy Store and Identity Store (OVD). These will later be defined either in DNS or `/etc/hosts`. If a load balancer is used, then the virtual host name and port described here will point to the LBR.

The ports are predefined and should only be changed if required by your enterprise.

- **OID Identity Store (OID):** If you are using the Single-host Topology and have OID as your Identity Store, enter the abstract host name and ports. It is the same as the Policy Store and cannot be changed.
- **Policy Store (OID):** Define an abstract host name for the Policy Store. Must be defined either in DNS or `/etc/hosts`. The default port values are already entered and should not be changed unless you are changing the OID port numbers in general.
- **Identity Store (OVD):** Define the abstract host name for the Identity Store and the ports. Otherwise, if you chose to use OID as your Identity Store, use the OID ports.

4.1.6.5 Complete the UCM LBR Endpoint Table

If you are using high availability, then an entry in the load balancer is needed to distribute the load among UCM servers.

- **Hostname:** The load balancer entry here will be configured to distribute traffic among UCM managed servers in the UCM cluster. Enter the load balancer virtual host name used for UCM distribution.
- **Port:** Only change the default port if required by your enterprise. Port must be configured for TCP traffic.

4.1.6.6 Complete the HTTP LBR Endpoints Table

Select the external and internal hostnames that to be used for the HTTP Endpoints at the Load Balancer or Reverse proxy. The *Oracle Fusion Applications Installation Workbook* provides the default hostnames as presented on the Provisioning Wizard. See Section 4.1.2.1, "Planning URL Naming Conventions" for details.

We recommend keeping the default port numbers, as mentioned in Section 4.2.1, "Using Default vs. Custom Port Numbers".

4.1.6.7 Complete the AdminServer Virtual Hosts/VIPs Table

The Oracle Identity Management-related entry is needed for all Enterprise topologies. The Oracle Fusion Applications entries are only needed when planning for Enterprise high availability (HA). You only need to define entries for those products you have licensed.

See Section 4.1.5.1, "Define VIPs for Oracle Identity Management" for general discussion.

- **Virtual Host Name:** For each domain, define a Virtual Hostname. The network administrator will later need to set these up in DNS.
- **Virtual IP Address:** For each domain, define a Virtual IP.

4.1.6.8 Complete the Managed Server Virtual Hosts/VIPs Table

Like the Admin Server entries above, the Oracle Identity Management-related entries are needed for all Enterprise topologies. The Oracle Fusion Applications entries are only needed when planning for Enterprise high availability (HA). You only need to define entries for those products you have licensed. For each managed server in the table, you must define a virtual host name and IP for each scale-out node.

4.2 Network-Ports: Planning Ports

Default ports are provided by Oracle Identity Management and Oracle Fusion Applications Provisioning, and are listed in the *Oracle Fusion Applications Installation Workbook*. The network administrator of your enterprise will determine whether these can be used or should be changed; enter accordingly.

4.2.1 Using Default vs. Custom Port Numbers

The Provisioning tools include default port numbers for all components in their Wizards. While it is possible to change these ports to any other value, keeping the defaults guarantees consistency across different installations/environments and may be helpful when following product documentation, since it uses these default ports in its reference architectures and configuration examples.

When changing port numbers from their defaults, pay special attention to potential conflicts for components running on the same server with the same port. While the installers will verify and warn about any potential port conflicts, ensuring there are no conflicts before installation will help provide a more predictable and smoother installation experience.

4.2.1.1 Completing the Network-Ports Tab of the Oracle Fusion Applications Installation Workbook

The Network-Ports tab in the *Oracle Fusion Applications Installation Workbook* lists all ports that can be changed in the Oracle Identity Management and Oracle Fusion Applications provisioning tools and includes default values. Change the defaults only if required by existing conflicts in your enterprise's network setup.

4.3 Storage: Planning Storage Configuration

Storage planning refers to all planning activities related to:

- Determining how much storage will be needed for Oracle Fusion Applications during installation, runtime, and for upgrade

- Defining the file system directories where the software will be installed
- Defining the type of storage to be used (local, shared), depending on the requirements of both Oracle Fusion Applications and your enterprise.

This section focuses on software installation and initial use only. It does not address long-term capacity planning for the Oracle Fusion Applications environment or space management (e.g. periodic purging of logs).

4.3.1 Recommended Minimum Disk Space

It is recommended that you maintain the minimum amount of free disk space specified in Table 4–2 to accommodate the initial installation, and a reasonable number of incremental backups, daily or weekly thereafter, and subsequent upgrade activities for future releases. If your environment does not meet the minimum requirements, a warning message will be recorded in the provisioning log. You can continue with the installation but may encounter insufficient disk space issues.

In Table 4–2, the Installation/Upgrade Storage column represents the free disk space required for completing installation and upgrade. The Base Storage column is free disk space required to maintain a working application environment which takes into account of storage growth due to transition data, and retention of diagnostic logs for administration and troubleshooting.

Table 4–2 Recommended Minimum Disk Space

Host	Base Storage (GB)	Installation/Upgrade Storage (GB)
Oracle Fusion Applications Web Tier Host	50	50
Oracle Fusion Applications Provisioning Host	500	300
Oracle Fusion Applications Database Host	600	200
Oracle Identity Management Web Tier Host	50	50
Oracle Identity Management Provisioning Host	200	100
Oracle Identity Management Database Host	200	100

4.3.2 Directory Storage Requirements

Table 4–3 outlines space recommendations for various components and directories, several of which are detailed below. It does not include the storage required for storing the Oracle Fusion Applications media packs and the provisioning repository.

- Section 4.3.2.1, "Shared Storage"
- Section 4.3.2.2, "Local Storage (if used)"
- Section 4.3.2.3, "DMZ Local Storage (if used)"
- Section 4.3.2.4, "Database Storage"
- Section 4.3.2.5, "Temporary Files Created During Installation (temp directory)"

Table 4–3 Planning Storage Size

Directory Created	Description	Storage Size Usage Estimate
DB HOME/oradata	Both the Oracle Fusion Applications transaction database and the Oracle Identity Management database(s) may be on one machine or separate machines. On the same machine, they can share a DB Home; otherwise there will be a DB Home on each database machine. DB Home includes database directory files and configuration files. /oradata contains the table spaces and logs.	The Oracle Fusion Applications transaction database DB Home requirement: 50 GB. The Oracle Identity Management DB Home requirement: 50 GB. /oradata for FA: 200 GB /oradata for IDM: 75 GB
IDM_BASE (shared), IDM_CONFIG (shared), IDM_LOCAL_CONFIG (local)	IDM_BASE contains the Oracle Identity Management product directory. It remains relatively unchanged. It must use shared storage and may use local storage additionally.	20 GB
IDMLCM_HOME (shared)	IDMLCM_HOME contains the Oracle Identity Management Configuration directory which stores the configuration files and is modified as a result of the provisioning process. It must use shared storage.	25 GB
FAPROV_HOME (shared)	A directory created just for the Oracle Fusion Applications installing the provisioning framework. Once Oracle Fusion Applications is installed, it can be deleted if there is no further usage after provisioning.	10 GB
APPLICATIONS_BASE (shared), APPLICATIONS_CONFIG (shared), APPLICATIONS_LOCAL_CONFIG (local)	APPLICATIONS_BASE is the top-level directory containing the Oracle Oracle Fusion Applications executable. APPLICATIONS_CONFIG contains the instance details for Oracle Fusion Applications. It must use shared storage and may use local storage (APPLICATIONS_LOCAL_CONFIG) additionally.	120 GB shared
/mnt/hwrepo (shared)	A required directory for Oracle Fusion Human Capital Management (Oracle Fusion HCM) which is checked by the Provisioning Wizard in the pre-verify stage of Oracle Fusion Applications provisioning. It has a large storage requirement if you plan to use the Workforce Reputation Management feature. You can ignore the warning if you do not use Workforce Reputation Management feature.	1 TB
/tmp (local)	For each provisioning host, ensure that there is at least 4 GB free space available for /tmp before installing Oracle Fusion Applications on the provisioning hosts. If the disk space for /tmp is low, you will encounter performance issues. In this case, you should make disk space available or restart the hosts to clean up /tmp.	4 GB/host

4.3.2.1 Shared Storage

Shared storage space must be made available for use by all nodes running Oracle Fusion Applications and Oracle Identity Management. The shared storage space will normally hold:

- The provisioning repository (see Section 4.3.2.1.1)
- All of the Oracle Identity Management and Oracle Fusion Applications software (including their provisioning frameworks). An exception: some of the software will be stored elsewhere if you choose "local Config" during provisioning (see Section 4.3.2.2) or select the DMZ option (see Section 4.3.2.3).
- Temporary backup files (see Section 4.3.2.1.2)
- The hwrepo directory (HCM only; see Section 4.3.2.1.3.)

For more information about the directory structure of the shared storage please refer to Section 2.3

4.3.2.1.1 Installation Files and Provision Repository

The Oracle Fusion Applications software from Oracle eDelivery is downloaded in the form of several .zip files. You extract these into a directory called the provisioning repository (REPOSITORY_LOCATION), which contains the "installers" directory containing all installers required by Oracle Fusion Applications. This repository must reside on shared storage. Space is needed for both the zip files and the extracted repository; you can delete or move the zip files after the repository is created.

For more information, see Section 2.3.1, "Installation Repository".

4.3.2.1.2 Temporary Backup Files

The installation procedures described in this guide prompt you to take temporary backup files at several milestones of the installation process. Plan to make enough space available to store those backups files for the duration of the installation process.

4.3.2.1.3 The hwrepo Directory

If you are provisioning the Oracle Fusion Human Capital Management (Oracle Fusion HCM) application offerings, namely Workforce Development and Workforce Deployment, and planning to use Workforce Reputation Management feature, you must create a directory named `/mnt/hwrepo` (Windows: `C:\mnt\hwrepo`) on a shared disk for the provisioning hosts. If this directory is not set up, you will see a warning message in the provisioning log during the pre-verify phase when you select the offerings for provisioning. You can proceed with provisioning the environment and mount the shared disk after provisioning is complete and before you start using the Workforce Reputation application.

4.3.2.2 Local Storage (if used)

If desired, certain runtime and configuration directories can be stored in local storage instead of shared storage, for both Oracle Identity Management and Oracle Fusion Applications components. See Section 4.3.6, "Local Storage Considerations" for more information on making this decision.

For more information about the directory structure of the local storage, see Section 2.3.

4.3.2.3 DMZ Local Storage (if used)

If desired, the Middleware Home for OHS and Webgate, as well as other configuration files, can be stored separately from the shared storage, for use in a DMZ. See

Section 3.4.3, "Topology: Understanding DMZ Requirements" for information on how to choose whether to use the DMZ option in Oracle Identity Management and Oracle Fusion Applications provisioning wizards. If used, plan space for the DMZ servers.

For more information about the directory structure of the local storage, see Section 2.3.

4.3.2.4 Database Storage

Initial database storage requirements are provided in Table 4–3, but consider short and long-term storage requirements during the planning phase. Storage is needed for both the Oracle database binaries and the data files and other configuration files.

If using Real Application Clusters (RAC) for high-availability, the database storage must be shared among all nodes for each database. Automatic Storage Management (ASM) is the only supported database storage for RAC.

4.3.2.5 Temporary Files Created During Installation (temp directory)

Oracle Fusion Applications uses the system temporary directory to store certain files used during the install, and that space is required throughout the installation process. Since these files may also be used post-installation for patching or upgrade processes, it is recommended to assign that space to the system temp directory permanently.

4.3.3 oraInventory Planning

The oraInventory is the location where the Oracle Universal Installer stores information about all the Oracle software products installed on all `ORACLE_HOMES` and it is essential for lifecycle events such as applying patches, upgrades, and de-installing components. The following components require an oraInventory:

- Oracle Database
- Oracle Identity Management Provisioning tool
- Oracle Identity Management components
- Oracle Fusion Applications Provisioning tool
- Oracle Fusion Applications components
- Oracle HTTP Server (separate oraInventory when installed on a DMZ)

For more information about oraInventory (also called OUI Inventory in some references), see the "Oracle Universal Installer (OUI) Inventory" in the *Oracle Fusion Applications Patching Guide*.

When planning the location of the oraInventory directories, consider the following:

- The oraInventory must be accessible from all the nodes that run software installed against it. Therefore, when Oracle Fusion Applications is installed on multiple nodes, the oraInventory for Oracle Fusion Applications must be located on shared storage. The same applies to the oraInventory for Oracle Identity Management. The database oraInventory locations are usually maintained separately from Oracle Fusion Applications and Oracle Identity Management oraInventory; shared storage is not applicable.
- Having a single oraInventory across all Oracle Fusion Applications components brings the advantage of centralized management and eliminates guesswork when applying patches. By default, the central oraInventory includes a known file (`oraInst.loc`) that provides the location of the central oraInventory to Oracle Fusion Applications lifecycle management utilities such as patching, upgrading, or cloning tools.

For oraInventory planning, please define the inventory location for each of the components below:

- Oracle Identity Management Provisioning Framework
- Oracle Fusion Applications Provisioning Framework
- Oracle Fusion Applications
- Oracle Identity Management
- Oracle Fusion Applications database
- Oracle Identity Management database
- OID database
- Oracle Fusion Applications Data Warehouse database

You should also define whether each inventory will be **central** or **local**:

- **Central:** The `/etc/oraInst.loc` file defines a server-wide location for a single inventory. When this file is present, Oracle installers/provisioning tools will not prompt for an inventory location and will use the one defined in this file instead. This works well if you plan to use the same Inventory path for all components.

  If the `/etc/oraInst.loc` file is not present, the first time you run an installer you will be prompted for a central inventory location and group owner. The installer will create the file automatically in the `/etc` directory, which requires root access. You must manually copy that file to all servers using that software.

- **Local:** No `/etc/oraInst.loc` file should be present. In this case, during install you may have to:

  1. Specify an inventory location and group owner when prompted by an installer, and check the option to make it a local inventory. Be sure to use a path in shared storage so it is visible to all servers running that software. No root access is required in this case. The installer will create the local inventory automatically in the specified location and will add an `oraInst.loc` file pointing to that inventory in the `ORACLE_HOME` of the product.
  2. When the local inventory and oraInst.loc file have been created by the installer, use the option `-invPrtLoc` to specify the oraInst.loc file location when invoking the installers/provisioning tools.

4.3.4 Planning Directory Structure and Naming Conventions

Ensure enough shared storage available and is accessible, and enough local storage is available if using that option. When you run the Provisioning Wizard, in addition to oraInventory, it is necessary to plan for the locations listed in the table below:

Directory Conventions:

- Directory names should not contain spaces
- Directory structure will be maintained across sources and targets, so use environment-neutral directory names and make them unique enough to guarantee this naming will be available on a potential subsequent clone target.
- All the directories must be owned by the installing (operating system) user. By convention, most Oracle software installation are done with the operating system user called "`oracle`".

4.3.5 Shared Storage Considerations

Oracle Fusion Applications and Oracle Identity Management use shared storage to make the binary files, configuration files, and other files available to all its Mid Tier nodes (and Web Tier nodes, if not using the DMZ option). The shared storage should be mounted at the exact same location for each Mid Tier node (and Web Tier nodes, if not using the DMZ option).

Shared storage **must** also be used for the:

- Provisioning repository
- Oracle Identity Management provisioning framework
- Oracle Fusion Applications provisioning framework
- `hwrepo` directory
- Database when using RAC

Shared storage may also be used temporarily during the installation process to hold temporary backup files or other files used during the installation process.

Additional consideration for the shared storage:

- Shared storage can be a Network Attached Storage (NAS) or Storage Area Network (SAN) device.
- NAS storage is only supported on NetApp and zFS.
- It is possible to set up separate volumes of shared storage, one for Oracle Fusion Applications and another for Oracle Identity Management. The Oracle Fusion Applications shared storage does not have to be mounted or visible to the Oracle Identity Management nodes, and vice-versa.
- If provisioning Oracle Identity Management and Oracle Fusion Applications on a single node, it is possible to use a local disk for shared storage, since it must only be visible to one node.
- The shared drive such as, Network File System (NFS) or Common Internet File System (CIFS) must support file locking. For NFS Version 3 and NFS Version 4, the advisory locking must be configured for the NFS mount. This applies to all UNIX platforms.

4.3.6 Local Storage Considerations

Both Oracle Identity Management and Oracle Fusion Applications Provisioning offer the option of using local storage to run Managed Servers and local instances. This storage location is a networked (local) disk on the host, visible only to the processes running on that host, which may offer better performance than shared storage.

When deciding whether or not to use local configuration take the following into account:

- Speed of local storage vs. shared storage
- Disk space available on the local storage
- IT processes (e.g. backup, storage mirroring) that will require additional maintenance due to the added drive location and its accessibility from the local server only.

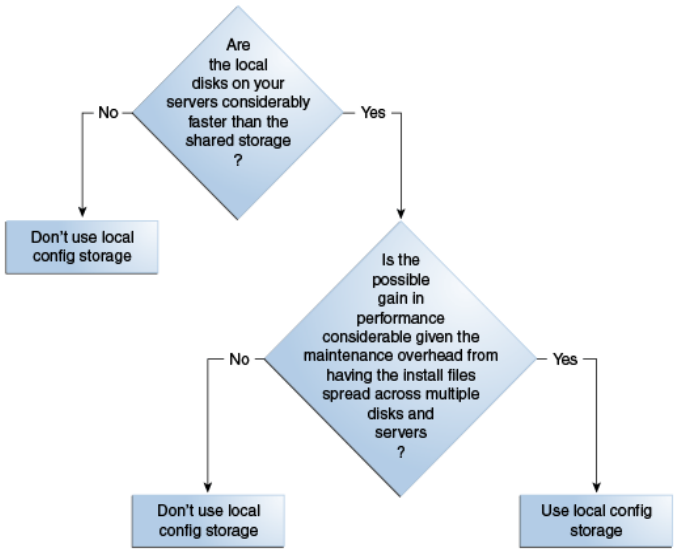
If the Local Config Storage option is used, the following directories will be created:

Installation	Location	Sub-Directories	Includes
Oracle Identity Management	IDM_LOCAL	/instances /domains	All instance configuration files (for OID, OVD, OIF, ODSM, OHS) All managed server files
Oracle Fusion Applications	FA_LOCAL	/applications /BIInstances /domains	BI Instance configuration files UCM configuration files All managed server files

4.3.6.1 Local Config Storage Decision Tree

The decision diagram outlines the key choice points when choosing whether to use the Local Storage Config option available in the Oracle Fusion Applications and Oracle Identity Management Provisioning Wizards.

Figure 4–5 Local Storage Decision Tree



4.3.7 Completing the Storage Tab of the Oracle Fusion Applications Installation Workbook

To complete the **Shared Storage** table:

- **Mount Point:** The file system mount point for the Oracle Fusion Applications or Oracle Identity Management shared storage.
- **NFS Share/Windows Share:** Network location, including server name and path of the shared storage. In UNIX, for example, `<hostname>:/<path>`.
- **NFS Parameters (UNIX only):** NFS parameters as defined in `/etc/fstab`.

To complete the **Install Directories** Table:

- Enter the appropriate install directories, as described in Section 4.3.4.

To complete the **Inventories** Table:

Complete the Inventory path with the desired path for the inventories. See Section 4.3.3, "oraInventory Planning" for details.

To complete the **Temporary Storage** Table:

- **Installer Directory:** When you downloaded the Oracle Fusion Applications package from e-delivery, you receive multiple zip files which, when unzipped create the top-level directory called `Installers`.
- **Temporary Backup Location:** plan space to back up during the provisioning process. When everything is installed and validated, you can delete this.

4.4 Database: Planning Database Configuration

A Oracle Fusion Applications environment will have, at minimum, two databases: one for Oracle Identity Management (IDMDB) and another one for Oracle Fusion Applications transactions (FADB). Since these two databases are subject to different patching and maintenance requirements, it is recommended that they are installed on separate `ORACLE_HOMEs`.

Optionally, a database for the Data Warehouse will also be used if you install Oracle BI Applications (DWDB).

Oracle Identity Management Provisioning also permits a separate dedicated database for OID (OIDDB). This database can be installed on the same `ORACLE_HOME` as the IDMDB.

The following table summarizes the database requirements for Oracle Fusion Applications

Database	Purpose	Mandatory	Separate OACLE_HOME Recommended
FADB	Oracle Fusion Applications transactional database	yes	yes
IDMDB	Oracle Identity Management database	yes	yes
OIDDB	Oracle Identity Management (OID only)	no	no
DWDB	Data Warehouse for Business Intelligence	no	yes

4.4.1 RAC vs. Single Instance Planning

For environments using the Basic or Enterprise (non-HA) topologies, a single-instance database will be used.

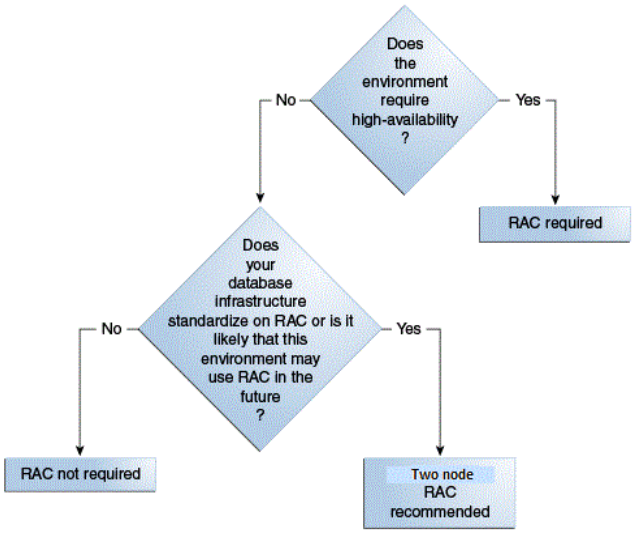
For environments with High Availability requirements, Oracle Fusion Applications supports the use of Oracle Real Application Clusters (RAC).

Note: You must use at least two nodes. RAC single-node functionality is not currently supported.

When you create a provisioning response file using the Oracle Fusion Applications Provisioning Wizard, if you provide only one RAC node information for the Oracle Fusion Applications database, then you will get an error during the install phase. The error is generated due to a limitation in the Oracle Data Integrator (ODI) installer and you must provide at least two RAC nodes. For more information, see Section 14.6.2, "Install Phase Failed with INST-07221: Specified connect string is not in a valid format Error".

For more information on Oracle RAC, see the Oracle database library.

Figure 4–6 RAC or Single-instance Database Decision Tree



4.4.2 Planning for Database Requirements

When determining your database configuration, consider the required instances, the required patching, listener configurations, schema and password requirements, and RCU directories.

> **Note:** Two databases are recommended for Oracle Internet Directory and Oracle Access Manager/Oracle Identity Manager because they are likely to have different configuration requirements. If desired, they can be combined into a single database.

4.4.2.1 Required Instance Parameters

The Oracle Fusion Applications database has specific required instance parameters. Validate Oracle-recommended database instance parameters for the Oracle Fusion Applications and Oracle Identity Management databases against your enterprise corporate guidelines for any potential issues and plan accordingly. For details, see:

Oracle Identity Management: Section 7.2.3, "About Initialization Parameters"

Oracle Fusion Applications: Section 8.2.2.2, "Minimum Configuration Parameters for Oracle Database"

4.4.2.2 Required Database Patches

The Oracle Fusion Applications database has specific patch requirements, which must be applied before starting the provisioning process. To determine your required patches, per corporate guidelines (e.g. CPUs), see:

Oracle Identity Management:
Section 7.2.2.1, "Patch Requirements for Oracle Database 11g (11.1.0.7)", and
Section 7.2.2.2, "Patch Requirements for Oracle Database 11g (11.2.0.2.0)"

Oracle Fusion Applications: Section 8.2.2.4, "Mandatory Oracle Database Patches"

Use these references to check for potential conflicts and plan accordingly. If necessary, request merge patches from Oracle Support.

4.4.2.3 Schema and Password Requirements

All Oracle Identity Management and Oracle Fusion Applications schema names for the Oracle Identity Management database/OID database and Oracle Fusion Applications database are fixed and cannot be modified. They will be created by the Oracle Fusion Middleware RCU (Oracle Identity Management) and Oracle Fusion Applications RCU.

Note that the Oracle Fusion Middleware RCU appears to provide an option to choose a prefix for the schemas, but in this release **the prefix must always be FA.**

Therefore, on the topic of schemas, the only planning required is regarding password selection. Oracle Identity Management and Oracle Fusion Applications Provisioning Wizards give you the option of choosing a different password for each schema, but you can also use the same password for all schemas or groups of schemas as desired.

> **Note:** The Oracle Metadata Services (MDS) Repository is a particular type of repository that contains metadata for some Oracle Fusion Middleware components. It can also include custom Java EE applications developed by your organization.

Table 4–4 lists all the Oracle Fusion Applications schemas created.

Table 4–4 Oracle Fusion Middleware and Oracle Fusion Applications Schema Owners

Component	Schema
Oracle Fusion Applications	FUSION FUSION_DYNAMIC FUSION_RUNTIME FUSION_APM FUSION_AQ FUSION_BI FUSION_DQ FUSION_ODI_STAGE FUSION_SETUP
AS Common Schemas ■ Enterprise Scheduler Service ■ Metadata Services	Includes: ■ FUSION_ORA_ESS ■ CRM_FUSION_MDS_SOA ■ FIN_FUSION_MDS_SOA ■ HCM_FUSION_MDS_SOA ■ OIC_FUSION_MDS_SOA ■ PRC_FUSION_MDS_SOA ■ PRJ_FUSION_MDS_SOA ■ SCM_FUSION_MDS_SOA ■ SETUP_FUSION_MDS_SOA ■ FUSION_MDS ■ FUSION_MDS_ESS ■ FUSION_MDS_SPACES
Secure Enterprise Search	SEARCHSYS
Oracle Data Integrator ■ Master and Work Repository	FUSION_ODI

Table 4–4 (Cont.) Oracle Fusion Middleware and Oracle Fusion Applications Schema

Component	Schema
Enterprise Content Management ■ Oracle Content Server 11*g* - Complete ■ Oracle Imaging and Process Management	Includes: ■ FUSION_OCSERVER11G ■ FUSION_IPM
Oracle Business Intelligence (Platform)	FUSION_BIPLATFORM
Oracle BI Applications Schemas ■ Oracle Transactional BI	Includes: ■ FUSION_OTBI
WebLogic Server Communication Services ■ SIP Infrastructure Location Service ■ Presence ■ SIP Infrastructure Subscriber Data Service	Includes: ■ FUSION_ORASDPLS ■ FUSION_ORASDPXDMS ■ FUSION_ORASDPSDS
SOA and BPM Infrastructure ■ User Messaging Service ■ SOA Infrastructure ■ SOA Infrastructure ■ SOA Infrastructure ■ SOA Infrastructure ■ SOA Infrastructure ■ SOA Infrastructure ■ SOA Infrastructure ■ SOA Infrastructure	Includes: ■ FUSION_ORASDPM ■ CRM_FUSION_SOAINFRA ■ FIN_FUSION_SOAINFRA ■ HCM_FUSION_SOAINFRA ■ OIC_FUSION_SOAINFRA ■ PRC_FUSION_SOAINFRA ■ PRJ_FUSION_SOAINFRA ■ SCM_FUSION_SOAINFRA ■ SETUP_FUSION_SOAINFRA
WebCenter Suite ■ WebCenter Spaces ■ Portlet Producers ■ Activity Graph and Analytics ■ Discussions	Includes: ■ FUSION_WEBCENTER ■ FUSION_PORTLET ■ FUSION_ACTIVITIES ■ FUSION_DISCUSSIONS ■ FUSION_DISCUSSIONS_ CRAWLER
Audit	Includes: ■ FUSION_IAU ■ FUSION_IAU_APPEND ■ FUSION_IAU_VIEWER
Oracle Social Network	Includes: ■ FUSION_SOCIAL ■ FUSION_SOCIAL_VIEWS ■ FUSION_SOCIAL_CEF

Table 4–5 shows all the Oracle Identity Management schemas created:

Table 4–5 Oracle Identity Management Schemas

Component and Database Name	Schema	Service Name
Oracle Internet Directory OIDDB	Includes: ■ ODSSM ■ ODS ■ DIP (Directory Integration Platform)	OIDEDG.mycompany.com

Table 4–5 (Cont.) Oracle Identity Management Schemas

Component and Database Name	Schema	Service Name
Oracle Identity and Access Management IDMDB	Includes: ■ FA_OIM ■ FA_OAM ■ FA_OIF ■ SOA_INFRA ■ FA_MDS ■ FA_ORASDPM ■ FA_OAM ■ FA_IAU	IAMEDG.mycompany.com

4.4.2.4 Oracle Fusion Applications RCU Directories

The Oracle Fusion Applications transactional database requires the creation of several DBA directories, listed in the following table. Directory creation is performed when you run the Oracle Fusion Applications RCU.

To plan for these DBA directories, decide where you will create the corresponding file system directories on the database server and add those locations to the *Oracle Fusion Applications Installation Workbook*. You will be asked to enter the locations when you run the Oracle Fusion Applications RCU.

DBA Directory Name	Purpose	Requirements
APPLCP_FILE_DIR	Used by Oracle Enterprise Scheduler to store the log and output files.	Must be valid on the database server with read-write permissions to the database owner. For Oracle RAC, must point to a location that is shared across all nodes.
APPLLOG_DIR	Location of the PL/SQL log files from Oracle Fusion Applications PL/SQL procedures on the database server.	Ensure that the database owner has read-write privileges.
FUSIONAPPS_PROV_RECOVERY_DIR (RCU OBIEE Backup Directory)	Location of the Oracle Business Intelligence Enterprise Edition dump files. These files are used for enabling a restart action.	Ensure that the database owner has read-write privileges. For Oracle RAC, must point to a location that is shared across all nodes.
FUSIONAPPS_DBINSTALL_DP_DIR	Directory where you will copy the Oracle Fusion Applications database dump files	Ensure that the database owner has read-write privileges. For Oracle RAC, must point to a location that is shared across all nodes.
OTBI_DBINSTALL_DUMP_DIR (RCU OTBI Dump File Directory)	Directory on the database server where Oracle Transactional Business Intelligence dump file is stored.	Ensure that the database owner has read-write privileges. For Oracle RAC, must point to a location that is shared across all nodes.

4.4.2.5 Oracle Identity Management Split Database Configuration

The Oracle Identity Management Provisioning tool allows you to use a dedicated database for OID (OIDDB), which will hold the ODS and ODSSM schemas used by it. With this configuration, only the ODS and ODSSM schemas will be placed on a different database, all other IDM schemas will still be located in the IDMDB.

This configuration can be used if you plan on using the Advanced replication features of the Oracle Database to perform multi-master replication across multiple OID instances. Otherwise, a separate database for OID is not required.

4.4.3 Completing the Database Tab of the Oracle Fusion Applications Installation Workbook

To complete the **Fusion Applications Transactional Database** table:

- **FA DB Service Name:** This is the global database name, such as `fadb.mycompany.com`.
- **FA DB Service Instance:** If you are using RAC, separate the instances with commas in the *Oracle Fusion Applications Installation Workbook* table cell.
- **RCU Directories:** When you start the Repository Creation Utility to populate schemas for Oracle Fusion Applications, it will ask for these directories. Note that they are local to the database server. See Section 8.6, "Running the Oracle Fusion Applications RCU to Create Oracle Fusion Applications Database Objects" for the full context.

To complete the **IDM Database** table:

- **IDM DB Service Name:** This is the global database name, such as `fadb.mycompany.com`.
- **IDM DB Service Instance:** If you are using RAC, separate the instances with commas in the *Oracle Fusion Applications Installation Workbook* table cell.
- **IDM DB Prefix:** This is for running the Oracle Fusion Middleware RCU utility. You must enter FA in the Oracle Identity Management Provisioning Wizard when prompted.

If you are planning to use the OID database or the Oracle Fusion Applications Data Warehouse, enter the same parameters in their respective tables.

4.5 Identity Management: Planning Oracle Identity Management Configuration

The following topics provide concepts needed to plan an Oracle Identity Management installation and to fill out the Identity Management tab in the *Oracle Fusion Applications Installation Workbook*.

- Section 4.5.1, "Identity Store Planning"
- Section 4.5.2, "LDAP Context Planning"
- Section 4.5.3, "Location for Files Generated During Oracle Identity Management Provisioning"
- Section 4.5.4, "Oracle Access Manager Transfer Mode"

4.5.1 Identity Store Planning

Planning your Oracle Identity Management installation requires understanding how Oracle Identity Management handles the OID and OVD Identity Stores.

Understanding OID and OVD

Oracle Fusion Applications supports two types of Identity Store: OID and OVD. With the OID option, identity information is physically stored in OID. OVD on the other hand is a virtual directory and does not store any user/group information. Therefore, when OVD is used as the Identity Store, it is possible to configure it to point to any other user/group store without the need to reconfigure the components in Oracle Fusion Applications or Oracle Identity Management.

Using OVD as the Identity Store has the advantage of flexibility; identity data can still be stored in OID, but OVD provides the ability to switch to a different identity provider later with little impact. (Section 16.10.4, "Configuring Identity Integration with Active Directory", provides instructions on how to configure other sources, such as MS Active Directory, post-provisioning.) **Given this flexibility, OVD will usually be the primary choice for the Identity Store for Oracle Fusion Applications.**

How Topology Affects the OID/OVD Decision

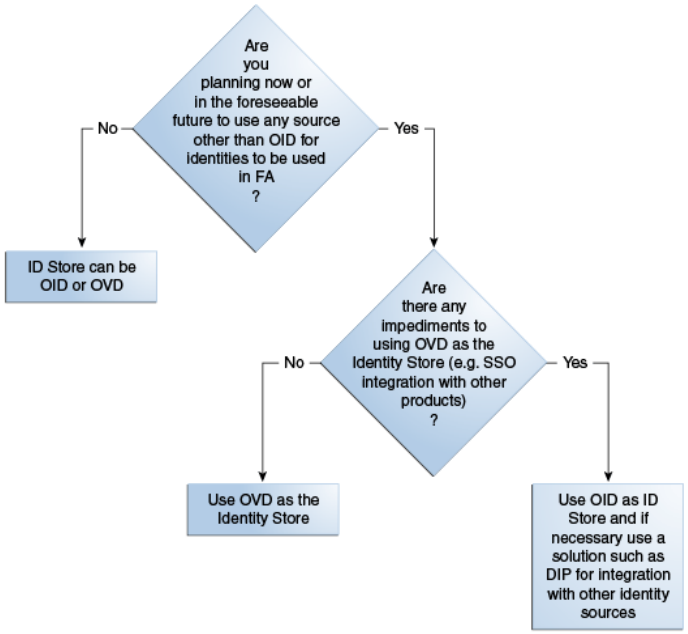
While OVD is installed and configured with an adapter to OID for all three Oracle Identity Management topology types, it is only auto-configured as the Identity Store in the **EDG** topology types. (Note that the EDG topology type will require a load balancer or reverse proxy.)

For the **Single-Host** topology, OID is configured as the Identity Store instead, and that option cannot be user-defined. If you plan to use OVD as the ID Store, you must select the **EDG** (that is, Enterprise) topology for Oracle Identity Management Provisioning.

Additional Considerations when Planning the Identity Store

- Integration with other products for single-sign -on (SSO) may have specific requirements, e.g. Ebusiness Suite integration.
- OID offers additional options if you decide to use OID (without OVD) as the ID Store. One of them is DIP (Directory Integration Platform), which performs synchronization between OID and other directories.

Figure 4–7 Identity Store Decision Tree: OID or OVD?



4.5.2 LDAP Context Planning

LDAP directories are used by Oracle Fusion Applications for storing identities - users and groups (acting as the Identity Store), as well as authorization policies and credentials (acting as the Policy Store/Credential Store).

Oracle Identity Management Provisioning provides the option to choose the context root for the Identity Store, i.e. the starting point in the directory tree for storing user and group information. Normally, the ID Store context root will be based on your domain name, e.g. for a company with domain name "mycompany.com", the ID Store context root chosen will normally be `"dc=mycompany,dc=com"`. Provisioning will then create sub-contexts for Users (`cn=Users`), groups (`cn=Groups`) among others.

For the Policy Store, Oracle Identity Management Provisioning will automatically create contexts for the two policy stores (IDM and FA), under `cn=jpsroot` and `cn=FAPolicies`, respectively. Oracle Identity Management Provisioning does not allow you to change them. During Oracle Fusion Applications Provisioning, you will be asked to provide a context root for the FA Policy Store, and although you are free to choose a different one (Oracle Fusion Applications Provisioning can create it for you if necessary), we recommend using the one previously created by Oracle Identity Management Provisioning.

The table below provides a summary of the LDAP context roots used by Oracle Fusion Applications:

	Default	Directory Type	Can be User-Defined?
Identity Store (Oracle Fusion Applications/Oracle Identity Management) Realm DN	`dc=mycompany,dc=com` (example)	OID or OVD	Yes
IDM Policy Store	`cn=jpsroot`	OID	No.
Fusion Applications Policy Store	`cn=FAPolicies`	OID	Yes

4.5.3 Location for Files Generated During Oracle Identity Management Provisioning

Oracle Identity Management Provisioning automatically generates files to be used during Oracle Fusion Applications Provisioning, providing a more streamlined integration between the two.

Once the Oracle Identity Management Provisioning process finishes, you will find the generated files under `IDM_INSTALL_APPCONFIG_DIR/fa`. These files must be copied to a directory accessible from all Oracle Fusion Applications nodes before Oracle Fusion Applications Provisioning, so planning for this involves simply defining the location where these files will be and adding the information to the *Oracle Fusion Applications Installation Workbook*.

4.5.4 Oracle Access Manager Transfer Mode

Oracle Access Manager (OAM) Transfer Mode refers to the transport security modes for communication between the Oracle Access Manager Server (OAM Server) and the Web gates. While OAM in general supports three different mode options (Open, Simple and Cert), the only available mode for Oracle Fusion Applications Provisioning is "Simple" for all platforms, with the exception of AIX (where only Open mode is supported).

The table below provides a summary of OAM Transfer Modes and availability in Oracle Fusion Applications Provisioning. A single mode must be selected for the entire installation (including Oracle Identity Management) in accordance to the table. In simpler terms: all platforms require Simple mode except for AIX, where Open mode must be selected.

Table 4–6

OAM Mode	Description	Available in Fusion Applications Provisioning
Open	Uses un-encrypted communication	Yes (AIX only)
Simple	Uses encrypted communication through SSL with a public key certificate issued by Oracle	Yes (all platforms except AIX)
Cert	Uses encrypted communication through SSL with a public key certificate issued by a trusted third-party certificate authority.	No

4.5.5 Considering Oracle Internet Directory Password Policies

By default, Oracle Internet Directory passwords expire in 120 days. Users who do not reset their passwords before expiration can no longer authenticate to Oracle Internet Directory. Note that this includes administrative users, such as `oamadmin`, and the Oracle Identity Management environment cannot work properly unless these users can authenticate. See the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* for information about changing Oracle Internet Directory password policies.

4.5.6 Completing the Identity Management Tab of the Oracle Fusion Applications Installation Workbook

The *Oracle Fusion Applications Installation Workbook* provides sample values to make many of these entries self-explanatory.

4.5.6.1 To complete the LDAP table:

Review Section 4.5.2, "LDAP Context Planning" to obtain the information required for the DN entries in this table.

- **Identity Store Realm DN:** Format described in the table in Section 4.5.2,
- **LDAP User DN:** The User DN is a subtree of the Identity Store Realm DN (above). Naming format is fixed: `cn=Users`
- **LDAP Group DN:** The Group DN is a subtree of the Identity Store Realm DN (above). Naming format is fixed: `cn=Groups`
- **Policy Store JPS root DN:** Un-editable.
- **FA JPS root DN:** Refer to the table in Section 4.5.2 to derive.

4.5.6.2 To Complete the IDM Provisioning Files Table

- **IDM Properties file location:** When Oracle Identity Management Provisioning is complete, a file will be created in the `IDM Shared Configuration Location/fa` directory (as defined on the **Storage** tab, **Install Directories** table). This file must be made available to the Oracle Fusion Applications Provisioning process. If the original location is accessible to the Oracle Fusion Applications Provisioning tool, enter that location in the *Oracle Fusion Applications Installation Workbook*. Otherwise, copy the file to an accessible location and note the new location here.
- **IDM Keystore file location:** Not used in this release.

4.5.6.3 To Complete the OAM Table:

Only one field in this table can be edited, and it is generally not necessary to do even that one.

- **OAM Administrator User name**: It is recommended to keep the default (`OAMAdminUser`) unless explicitly instructed to change this.

4.5.6.4 To Complete the Identity Store/Policy Store Table:

Most of the fields in this table cannot be edited. The exceptions are below:

- **ID Store Type (OID/OVD):** Enter the Identity Store you are using, based on the topology you chose (see Section 4.5.1 for details.).
- **FA Node Manager Username:** Use the default or edit if desired.

4.6 SSL and Certificates

This section describes requirements that apply to the *SSL and Certificates* tab in the *Oracle Fusion Applications Installation Workbook*.

4.6.1 Out-of-the-Box SSL Configuration

Out of the box, the Oracle Identity Management and Oracle Fusion Applications Provisioning frameworks will configure their respective components to use SSL connections between the end users and the load balancer/reverse proxy (or Web Tier if an LBR/RP is not used). This is mandatory and cannot be changed.

Oracle Identity Management Provisioning provides the option to select SSL or non-SSL for the `IDM Admin` HTTP endpoint, as noted in the *Oracle Fusion Applications*

Installation Workbook. Select **yes** if you want that endpoint to be configured for SSL automatically during Oracle Identity Management Provisioning.

If a load balancer is used, the connection between the LBR and the Web Tier will be configured as non-SSL, out of the box. Therefore, the HTTP listener on the Oracle HTTP Server will be non-SSL.

If a load balancer is not used, Oracle Identity Management behaves differently from Oracle Fusion Applications:

- **Oracle Fusion Applications:** The end-user (external) connections will still be SSL, but they will terminate at the Web Tier instead. (FA OHS will be configured to listen to SSL traffic.)
- **Oracle Identity Management:** All external endpoints will be non-SSL. (IDM OHS will be configured to listen to regular HTTP traffic.)

4.6.2 SSL Certificate Requirements

SSL Certificate requirements depend on whether your topology uses a load balancer/reverse proxy or not.

If using an LBR/RP:
Because both Oracle Identity Management and Oracle Fusion Applications terminate SSL connections at the load balancer, it is necessary to set up the appropriate SSL certificates on the load balancer BEFORE starting the provisioning process. The certificates should be created and provisioned to the LBR/RP according to your own policies and procedures, along with the instructions provided by your LBR/RP manufacturer.

If not using an LBR/RP:
SSL will terminate at OHS, which will be configured with a default dummy certificate. As the dummy certificate is not trusted by browsers, end users will get certificate warning messages when they access any external URL.

To avoid this, you must configure OHS to use certificate(s) signed by a trusted certificate authority (CA). This can be an external certificate authority such as Verisign, or an internal certificate authority whose root certificate is trusted by the browser. See Section 16.7, "Configuring Oracle HTTP Server with Custom Certificates" for more information.

4.7 What to Do Next

When the *Oracle Fusion Applications Installation Workbook* is entirely filled out, you are ready to proceed with Chapter 5, "Preparing for an Installation".

Part III

Preparing to Provision Oracle Fusion Applications

This part provides instructions to prepare your environment and install the Oracle Identity Management and Oracle Fusion Applications Provisioning Frameworks.

Part III contains the following chapters:

5 Preparing for an Installation

This chapter describes the prerequisites for provisioning a new applications environment.

This chapter includes the following sections:

5.1 Introduction to Preparing for an Installation

Before creating your new environment, review the actions described in the following sections to help ensure a smooth installation.

5.2 Preparing Storage Components

This section describes the following topics:

5.2.1 Preparing Shared Storage for Oracle Identity Management and Oracle Fusion Applications

Prepare the shared storage for Oracle Identity Management and Oracle Fusion Applications as defined in the *Oracle Fusion Applications Installation Workbook*. Ensure the shared storage has the required space as defined in Section 4.3, "Storage: Planning Storage Configuration" and that they are configured according to the instructions detailed in Section 4.3.5, "Shared Storage Considerations".

Tip: The shared storage property value is available in the *Oracle Fusion Applications Installation Workbook* - Storage tab -> Shared Storage.

5.2.2 Mounting the Shared Storage

Mount the shared storage on each server according to the information defined in the *Oracle Fusion Applications Installation Workbook* - Storage tab -> Shared Storage table. Ensure that the file system is mounted as read-write.

If you are using different shared storage for Oracle Identity Management and Oracle Fusion Applications, follow these steps to mount each shared drive:

- The Oracle Identity Management shared storage should be mounted on the servers running Oracle Identity Management components (see the Topology tab in the *Oracle Fusion Applications Installation Workbook*).
- The Oracle Fusion Applications shared storage should be mounted on the servers running Oracle Fusion Applications components (see the Topology tab in the *Oracle Fusion Applications Installation Workbook*).

5.2.3 Verifying Install Directory Location

Ensure the locations defined for the Install Directories and Temporary Shared Storage are owned by the appropriate user, are read/write and can be created later during install. They may include both shared and local file systems.

For servers located in the DMZ, which normally don't have access to the shared storage, the same base path used for the other servers (as defined in the *Oracle Fusion Applications Installation Workbook*) is applicable.

Tip: The directory location values are available in the *Oracle Fusion Applications Installation Workbook* - Storage tab -> Temporary Shared Storage -> Installers Directory Location.

5.2.4 Verifying the /etc/oraInst.loc File

Ensure there is no `oraInst.loc` file present in the `/etc` directory unless you plan on using a central inventory and would prefer to not have the installer create it for you later (which requires root access). In this case, ensure the `oraInst.loc` file points at the location defined for `oraInventory` in the *Oracle Fusion Applications Installation Workbook*. The `oraInst.loc` file contains the following two lines:

```
inventory_loc=<oraInventory path>

inst_group=<oraInventory owner group>
```

The file must be present and have the correct `oraInventory` and group owner values **for all servers**.

Tip: The planned inventory location values are available in the *Oracle Fusion Applications Installation Workbook* - Storage tab -> Inventories.

5.3 Preparing Servers

This section describes the following topics:

- Preparing the Oracle Identity Management Server

- Preparing the Oracle Fusion Applications Server

5.3.1 Preparing the Oracle Identity Management Server

This chapter describes tasks you must perform before running the Oracle Identity Management Provisioning Wizard. Many of these tasks are platform-specific.

5.3.1.1 Ensure Software Install Location is 45 Characters or Fewer

When planning the Oracle Identity Management deployment, ensure that the **Software Installation Location** directory path is 45 characters or fewer in length. You specify this directory on the Installation and Configuration page when you create the provisioning profile. A longer pathname can cause errors during Oracle Identity Management provisioning. See Section 11.2.4, "Null Error Occurs When WebLogic Patches Are Applied".

5.3.1.2 Configure Kernel Parameters (UNIX)

The kernel parameter and shell limit values shown below are recommended values only. For production database systems, Oracle recommends that you tune these values to optimize the performance of the system. See your operating system documentation for more information about tuning kernel parameters.

Kernel parameters must be set to a minimum of those below on all nodes in the cluster.

The values in the following table are the current Linux recommendations. For more information, refer to *Oracle Fusion Middleware System Requirements and Specifications*.

If you are deploying a database onto the host, you might need to modify additional kernel parameters. Refer to the 11*g* Release 2 *Oracle Grid Infrastructure Installation Guide* for your platform.

Table 5–1 UNIX Kernel Parameters

Parameter	Value
kernel.sem	256 32000 100 142
kernel.shmmax	4294967295

To set these parameters:

1. Log in as `root` and add or amend the entries in the file `/etc/sysctl.conf`.
2. Save the file.
3. Activate the changes by issuing the command:

```
/sbin/sysctl -p
```

5.3.1.3 Configure Kernel Parameters (AIX Only)

You must set the following AIX Kernel parameters before starting Oracle Identity Management Provisioning:

```
no -o tcp_recvspace=262144
no -o tcp_sendspace=262144
no -o udp_recvspace=262144
no -o udp_sendspace=262144
no -o rfc1323=1
no -o sb_max=4194304
/usr/sbin/no -o tcp_timewait=1
```

5.3.1.4 Set the Open File Limit (UNIX)

On all UNIX operating systems, the minimum Open File Limit should be 150000.

> **Note:** The following examples are for Linux operating systems. Consult your operating system documentation to determine the commands to be used on your system.

You can see how many files are open with the following command:

```
/usr/sbin/lsof | wc -l
```

To check your open file limits, use the commands below.

C shell:

```
limit descriptors
```

Bash:

```
ulimit -n
```

5.3.1.5 Set Shell Limits (UNIX)

To change the shell limits, login as `root` and edit the `/etc/security/limits.conf` file.

Add the following lines:

```
* soft  nofile  150000
* hard  nofile  150000
* soft  nproc   16384
* hard  nproc   16384
```

If you are installing on Oracle Linux Server release 6, edit `/etc/security/limits.d/90-nproc.conf` to make sure it has the following line:

```
* soft nproc 16384
```

After editing the file, reboot the machine.

5.3.1.6 Administrator Privileges (Windows)

In order to perform an Oracle Identity Management installation on a Microsoft Windows Vista or newer operating system, you must have Windows Administrator privileges.

Even when you log in as a user with Administrator privileges, Windows does not grant you the administrative role by default. In order to access the Oracle home files and folders, you must run commands as Administrator explicitly.

To run commands as Administrator, use either of the following methods:

1. Find the Command Prompt icon (for example, from the Start menu or from the Desktop), right-click the icon, and select Run as Administrator. Then you can run the executables, such as the WebLogic Server installer, from the command line.

2. Start Windows Explorer, find the executable you want to run (for example, rcu.bat for RCU, config.bat for the Configuration Wizard, or setup.exe for the installer), right-click the executable, and select Run as Administrator.

5.3.1.7 Set Up Required User (Windows)

Proceed as follows:

1. Create a `domain\user` that is part of the Administrators group.
2. Log in as the user that you created.
3. Run `secpol.msc` (security policy). To do this, click **Start > Run**, type `secpol.msc`, and press Enter. Add the `domain\user` that you created to **Log on as service** under the Local Policies, User Rights Assignment option.
4. Reboot the machine.

5.3.1.8 Enable IPV4 and Disabling IPV6 (Windows)

Ensure that IPV4 is enabled and IPV6 is disabled, as follows:

To enable the IPV4 address, execute the command:

```
netsh interface ipv4 install
```

To disable the IPV6 address, execute the command:

```
netsh interface ipv6 uninstall
```

A method for completely disabling IPV6 on a Windows host is documented at:

http://support.microsoft.com/kb/929852

To list all the IP addresses for verification, execute the command:

```
netsh interface ipv4 show ipaddresses
netsh interface ipv6 show ipaddresses
```

5.3.1.9 Install OpenSSL (Windows)

The `openssl` command is not available by default on Microsoft Windows.

You must install OpenSSL on the Windows machine. See:
http://www.openssl.org

The directory containing the binary `openssl` must be in the `PATH` environment variable.

5.3.1.10 Install Loopback Adapter (Windows)

Ensure that you have installed the Microsoft Loopback Adapter.

5.3.1.11 Install Cygwin (Windows)

If you plan to perform Oracle Identity Management Provisioning, or to run any shell script, ensure that you have installed a UNIX emulation package such as Cygwin or MKS Toolkit.

5.3.1.12 Enable Unicode Support

Your operating system configuration can influence the behavior of characters supported by Oracle Fusion Middleware products.

On UNIX operating systems, Oracle highly recommends that you enable Unicode support by setting the `LANG` and `LC_ALL` environment variables to a locale with the UTF-8 character set. This enables the operating system to process any character in Unicode. Oracle SOA Suite technologies, for example, are based on Unicode.

If the operating system is configured to use a non-UTF-8 encoding, Oracle SOA Suite components may function in an unexpected way. For example, a non-ASCII file name might make the file inaccessible and cause an error. Oracle does not support problems caused by operating system constraints.

5.3.1.13 Synchronize Oracle Internet Directory Nodes

Synchronize the time on the individual Oracle Internet Directory nodes using Greenwich Mean Time so that there is a discrepancy of no more than 250 seconds between them.

> **Note:** If OID Monitor detects a time discrepancy of more than 250 seconds between the two nodes, the OID Monitor on the node that is behind stops all servers on its node. To correct this problem, synchronize the time on the node that is behind in time. The OID Monitor automatically detects the change in the system time and starts the Oracle Internet Directory servers on its node.

5.3.2 Preparing the Oracle Fusion Applications Server

Before creating your new environment, review the following actions in this section to help ensure a smooth installation.

- Increase the Open Files Limit
- Define the Local Port Range
- Synchronize the System Clocks
- Synchronize Date Time Stamp
- Set the Kernel Parameter Value
- Unset LIBPATH Variable
- Set the System Time Zone
- Create the hwrepo directory
- Verify Swap Space (UNIX)
- Edit Host Names (UNIX)
- Default Shell (UNIX)
- Install en_US.UTF-8 Locale (UNIX)
- 32-bit Libraries (SUSE Linux Enterprise Server 11)
- Increase Entropy Values (Linux)
- Check for the Required Solaris Patch (Solaris Only)
- Tune the Socket Buffer Size (AIX Only)
- Set the SKIP_SLIBCLEAN Variable (AIX Only)
- Add Variable for SKIP_ROOTPRE to Command Line (AIX Only)
- Improve Provisioning Performance (AIX Only)

- Set Up the Server and the Shared Area Permissions (Windows x64)
- Update Virtual Memory setting to Custom Size (Windows Only)
- Microsoft Windows Resource Locking (Windows Only)

5.3.2.1 Increase the Open Files Limit

Increase the limit of open files to 327679 or higher for the operating system.

For Linux x86-64:

Modify `/etc/security/limits.conf` to read as follows:

- *FUSION_USER_ACCOUNT* `soft nofile 327679`
- *FUSION_USER_ACCOUNT* `hard nofile 327679`

Edit `/etc/ssh/sshd_config` as follows:

1. Set `UsePAM` to `Yes`.
2. Restart `sshd`.
3. Logout (or reboot) and log in again.

Increase the maximum open files limit.

Edit `/proc/sys/fs/file-max` and set it to 6553600. The change becomes effective immediately but does not persist after a reboot. To make the change permanent edit `/etc/sysctl.conf` and set `fs.file-max = 6553600`. This change will not be effective until the `sysctl` command is run or the server is rebooted.

For Oracle Solaris on SPARC (64-bit):

Edit `/etc/system` and set as follows:

```
set rlim_fd_cur=327679
set rlim_fd_max=327679
```

For IBM AIX on POWER Systems (64-bit):

Modify `/etc/security/limits` defaults to read as follows:

```
fsize = -1
core = 2097151
cpu = -1
data = 1024000
rss = 512000
stack = -1
stack_hard = -1
nofiles = 327679
nofiles_hard = 327679
```

Note: Do not set `nofiles` and `nofiles_hard` parameters to -1 on IBM AIX platforms. Setting them to -1 (unlimited) will cause the postconfigure phase to fail with an error message.

Note: If you select any Supply Chain Management offerings, then the host where the Global Order Promising (GOP) server is located has a different requirement for the data segment (data) setting. The data segment for the host running the GOP server should be set to a minimum of 2 GB (2097152) or higher.

This means instead of setting `data = 1024000` in the `/etc/security/limits` file on the host where the GOP server is located, you should set `data = 2097152` (or a larger number).

5.3.2.2 Increase the Max User Processes

For all platforms, typically, you would have max user processes set to 16384:

```
$ulimit -u
16384
```

Increase the maximum user process to 16384 or higher.

For Linux x86-64:

To check the max user processes:

```
$ulimit -u

16384
```

To change the max user processes:

Modify `/etc/security/limits.conf` to read as follows:

```
FUSION_USER_ACCOUNT soft nproc 16384

FUSION_USER_ACCOUNT hard nproc 16384
```

The value of 16384 for max user processes is the recommended starting value for installing Oracle Fusion Applications in a multi-host topology. Depending on the hardware topology for the Oracle Fusion Applications environment that you plan to setup, you may need to use a higher number for max user processes when you allocate more WebLogic domains and managed servers into a fewer number of hosts. Is is recommended that you to go through a proper sizing exercise to determine the configuration.

When a host reaches the limit of the max user processes during provisioning of Oracle Fusion Applications, you may encounter the following error messages while starting additional managed server processes even when the IP address and port number are valid.

Node Manager log:

```
2013-12-28 03:31:57.932 NOTIFICATION [logStatus] STATE=BUILD_
ERROR!TIMESTAMP=2013-12-28 03:31:57
GMT!TARGET=common-apps-startup!CATEGORY=BUILD_
ERROR!DOMAIN=HCMDomain!HOSTNAME=<host>!PRODUCTFAMILY=hcm!PRODUCT
=HCM-Talent!TASK=nodeManagerStartServer!TASKID=hcm.HCM-Talent.BU
ILD_
ERROR.common-apps-startup.nodeManagerStartServer!MESSAGE=Node
Manager Start Server operation could not be carried out. Please
check the log files in the Managed Server directory <file path
to a managed server directory>/logs/ and the NodeManager log at
<APPLICATIONS_CONFIG>/nodemanager/<host>/nodemanager.log to find
out details of the problem.!DETAIL=Process execution failed with
```

```
return code: 1. Check the logs for more
information.!BUILDFILE=<FAPROV_
HOME>/provisioning/provisioning-build/common-lifecycle-build.xml
!LINENUMBER=68!
```

Failed Managed Server log:

```
####<Dec 28, 2013 3:31:39 AM GMT> <Error> <Server> <host>
<TalentManagementServer_1> <DynamicListenThread[Default]> <<WLS
Kernel>> <> <> <1388201499505> <BEA-002606> <Unable to create a
server socket for listening on channel "Default". The address
<ip address> might be incorrect or another process is using port
<port>: java.net.BindException: Address already in use.>
```

```
####<Dec 28, 2013 3:31:39 AM GMT> <Critical> <WebLogicServer>
<host> <TalentManagementServer_1> <Main Thread> <<WLS Kernel>>
<> <> <1388201499517> <BEA-000362> <Server failed. Reason:
Server failed to bind to any usable port. See preceeding log
message for details.>
```

5.3.2.3 Define the Local Port Range

You must define your local port range to ensure that it does not overlap with the ports used by the Java Virtual Machines (JVMs) and other servers. This action avoids port conflicts during server startup. To view and modify `localRange`:

For Linux x86-64:

To view:

```
$cat /proc/sys/net/ipv4/ip_local_port_range
```

To modify:

```
$echo "32768 61000" > /proc/sys/net/ipv4/ip_local_port_range
```

To make the local port range permanent after server restart, add (or update)

the following line in `/etc/sysctl.conf`:

```
net.ipv4.ip_local_port_range = 32768 61000
```

For Oracle Solaris

To view:

```
#/usr/sbin/ndd /dev/tcp tcp_smallest_anon_port tcp_largest_anon_
port
```

To modify:

```
#/usr/sbin/ndd -set /dev/tcp tcp_smallest_anon_port 32768
```

```
#/usr/sbin/ndd -set /dev/tcp tcp_largest_anon_port 61000
```

For IBM AIX on POWER Systems (64-bit):

To view:

```
#/usr/sbin/no -a | fgrep ephemeral
```

To modify:

```
#/usr/sbin/no -o tcp_ephemeral_low=32768 -o tcp_ephemeral_
high=61000
```

Typically, the port range settings would be as follows:

```
$ /usr/sbin/no -a | fgrep ephemeral
     tcp_ephemeral_high = 61000
     tcp_ephemeral_low = 32768
     udp_ephemeral_high = 61000
     udp_ephemeral_low = 32768
```

For more information about setting port values, see "Viewing and Changing Ports for Components" in *Oracle Fusion Applications Administrator's Guide*.

5.3.2.4 Synchronize the System Clocks

All engine and data tier servers (including SIP) must accurately synchronize their system clocks to a common time source, to within one or two milliseconds. Large differences in system clocks can cause severe problems.

5.3.2.5 Synchronize Date Time Stamp

Before provisioning, ensure that the provisioning server and the computer hosting Oracle Access Server have the same date and time stamp settings. The WebGate installation fails with an Oracle Access Manager certificate error if the date and time settings on the provisioning server are different from the Oracle Access Server.

5.3.2.6 Set the Kernel Parameter Value

Before you install the Oracle Database using the Provisioning Wizard, ensure that the value of the kernel parameter shmmax on the database host is greater than the value of the System Global Area (SGA) Memory.

The value of SGA Memory (sga_target) is 9 GB in the default Database Configuration Assistant (DBCA) template for the Starter database. If you are running DBCA using the production DBCA template packaged with Oracle Fusion Applications Provisioning, the value of the SGA Memory is 18 GB. Ensure that `shmmax` > (`shmall * shmmni`) > `SGA Memory`, where `shmmax`, `shmall`, `shmmni` are kernel parameters.

For example, to retrieve the values of these kernel parameters on Linux, use the following command:

```
user@host> /sbin/sysctl -a | grep shm
kernel.shmmni = 4096
kernel.shmall = 3145728
kernel.shmmax = 12884901888
```

To set the value of a kernel parameter:

```
user@host> /sbin/sysctl -w sys.kernel.shmmax=value
```

5.3.2.7 Unset LIBPATH Variable

Before provisioning an Oracle Fusion Applications environment make sure the LIBPATH variable is not set. See Section 13.5.1, "Starting the Wizard and Preparing to Install" for details.

UNIX:

- Use *`env`* or *`echo $LIBPATH`* to check if the variable is set.
- Use *`unsetenv LIBPATH`* to unset the variable.

5.3.2.8 Set the System Time Zone

All server machines must have the same time zone settings as described in the following paragraph:

- The time zone should be the standard time zone for the instance.
- Set the `TZ` environment variable on Linux or an equivalent on other operating systems to have a valid time zone ID. On Windows, double click on the clock in the corner of the desktop, then navigate to time zone to set it.
- Check the time zone setting using the command: `echo $TZ`. The tzselect tool may be handy if you need to change the setting.
- Oracle WebLogic Server and Oracle Database will then derive the default VM and database time zones from the system, respectively, unless otherwise configured. JVMs and the database need to be running in the same time zone.

5.3.2.9 Create the hwrepo directory

If you are provisioning the Oracle Fusion Human Capital Management (Oracle Fusion HCM) application offerings, namely Workforce Development and Workforce Deployment, and planning to use the Workforce Reputation Management feature, you need to perform the following tasks after provisioning is complete:

1. Create a directory named `/mnt/hwrrepo` (Windows: `C:\mnt\hwrrepo`) for the provisioning hosts.
2. Mount a shared disk as needed by the Workforce Reputation (HWR) application.
3. Grant directory permission to the user/group who owns the Oracle Fusion Applications WLS domain(s).This user can start or shut down the Oracle Fusion Applications environment.

   UNIX: Run this shell command as root and replace `<user id>:<group id>` with appropriate user and group identifiers:

   ```
   chown <user id>:<group id> /mnt/hwrrepo
   ```

4. Change read/write permission for the directory `/mnt/hwrrepo` to be globally readable/writable.

   UNIX: Run this shell command as root:

   ```
   chmod 750 /mnt/hwrrepo
   ```

You will see a warning message in the provisioning log during the preverify phase when you select the Workforce Development and Workforce Deployment offerings for provisioning if the directory is not setup. The warning message is a reminder. You can proceed with provisioning the environment and mount the shared disk **after** provisioning is complete and before you start using the Workforce Reputation application.

5.3.2.10 Verify Swap Space (UNIX)

For UNIX platforms, ensure that the provisioning hosts have a miminum of 1 GB of swap space. During the provisioning of an Oracle Fusion Applications environment, a validation test is performed in the preverify phase. An error message is displayed if the provisioning hosts do not have at least 1 GB of swap space. This error must be resolved by increasing the swap space before you can proceed with provisioning the environment.

You will receive a warning if there is at least 1 GB of swap space but less than the larger of 2 GB and 10% of memory allocated to the host. This means if a host has less than 20 GB of memory, then the swap space must be at least 2 GB. If a host has more than 20 GB of memory, then the swap space must be at least 10% of the memory.

The decision on whether to set swap space higher than 10% of the memory is a performance tuning exercise that you can make at a later time. Under certain conditions in some platforms, you may need to increase swap space to 30% of the memory in order to complete provisioning an environment.

5.3.2.11 Edit Host Names (UNIX)

For UNIX platforms, confirm that the host names are correctly formatted in `/etc/hosts`, for each host that is participating in provisioning. Review `/etc/hosts` for each participating host and edit any host entries that do not meet the following recommendations:

1. The format for each host entry should follow this format:

   ```
   IP_address canonical_hostname [aliases]
   ```

   The `canonical_hostname` should be the same as the fully qualified host name. Errors can occur if a short version, or alias, of the host name is specified first in `/etc/hosts`. The usage of aliases is optional and can be left empty. Examples of correct and incorrect entries follow:

   ```
   (Correct) 141.80.151.100 myMachine.company.com  myMachine
   (Incorrect) 141.80.151.100  myMachine  myMachine.company.com
   ```

2. If the machine name is a logical host name and is different from the physical host name specified in `/etc/sysconfig/network`, then the entry for the logical machine should be listed before the entry of the physical host name in `/etc/hosts`. If the machine is always accessed using its logical host name, there is no need to have an entry for the physical host name in /etc/hosts. Examples of entries in the correct order follow:

   ```
   141.80.151.100 myLogicalMachine.company.com  myLogicalMachine
   141.80.151.100 myPhysicalMachine.company.com  myPhysicalMachine
   ```

   If the order of host names is reversed from what is shown in the example, then there may be errors in retrieving the logical host name.

   Note: Do not enter multiple host aliases into a single line in the `/etc/hosts` file. There are some software components which do not process a line with more than 700 characters. You may encounter error messages during provisioning phases, such as "UNABLE TO OPEN CREDENTIAL STOREFAILED TO ADUTPSINITIALIZE" caused by incorrect resolution of the host names. If you have a host that has many aliases, then limit the line to 700 characters and break it down into separate lines. Ensure that each line begins with the IP_address and canonical_hostname, then the aliases.

5.3.2.12 Default Shell (UNIX)

Ensure that `/bin/bash` shell is installed on the hosts before provisioning an Oracle Fusion Applications environment. Ensure that the provisioning hosts have bash shell version 3.2 or higher when you upgrade the environment at a later time.

5.3.2.13 Install en_US.UTF-8 Locale (UNIX)

If you are provisioning on UNIX platforms, ensure that the `en_US.UTF-8` locale is installed on the operating system of the provisioning hosts. Oracle Business Intelligence expects the `en_US.UTF-8` locale in the operating system before

provisioning the Oracle Fusion Applications environment. If the en-US.UTF-8 locale is not installed, you will encounter an error during the provisioning configure phase. The runProvisioning-bi-configure.log displays the following error message:

```
FAILED:Distributing Repository

Error:

<APPLICATIONS_
BASE>/fusionapps/bi/bifoundation/provision/scripts/bidomain/bi-i
nstall.xml:274: exec returned: 1.
```

Inspecting the oraInventory logs, it indicates that the EN_US.UTF-8 locale must be installed on the provisioning host for Oracle Business Intelligence. The error message is:

```
Executing Task: Distributing Repository

[CONFIG]:Distributing Repository

ReEncrypting RPD: [nQSError: 46116] The locale EN_US.UTF-8 needs
to be installed on the machine for the Oracle BI locale setting
english-usa specified in
NQSConfig.INI.javax.management.RuntimeMBeanException:javax.manag
ement.RuntimeMBeanException: Repository File '<APPLICATIONS_
CONFIG>/BIInstance/tmp/OracleBIApps.rpd' does not exist or is
not accessible.
```

If you encounter this error during the configure phase, install the missing locale and then retry the configure phase to complete the task.

5.3.2.14 32-bit Libraries (SUSE Linux Enterprise Server 11)

For SUSE Linux Enterprise Server 11 (Linux x86-64 SLES 11), you must ensure the following 32-bit libraries are available before provisioning a new environment. Otherwise, the user will encounter an error during installation:

- glibc-devel-32bit-2.9-13.2
- libgcc43-4.3.3_20081022
- libstdc++43-4.3.3_20081022-11.18
- gcc-32bit-4.3
- libaio-32bit-0.3.104
- libaio-devel-32bit-0.3.104
- libstdc++43-32bit-4.3.3_20081022
- libstdc++43-devel-32bit-4.3.3_20081022

5.3.2.15 Increase Entropy Values (Linux)

Make sure the hosts have enough entropy values in the provisioning hosts. If this value is less than 1000, increase it to a value to a greater value using the rngd command. Run these commands as the root user for the current session:

To check the entropy value:

```
cat /proc/sys/kernel/random/entropy_avail
```

To increase the entropy value:

```
rngd -r /dev/urandom -o /dev/random
```

To set the `rngd` service to start automatically after rebooting the host, enter the following text into a script, such as, `start.rngd`, and run the script as root user:

```
#! /usr/bin/perl -w
.
# minimum required bytes to be happy with the device
my $want_bytes = 8192;
.
# list of commands to check
my clist = qw(/sbin/rngd /usr/sbin/rngd); S
.
# list of device names to check
my slist = qw(
  /dev/hwrandom /dev/hw_random /dev/hwrng /dev/intel_rng /dev/i810_rng
  /dev/urandom
);
.
.
use Fcntl qw(O_RDONLY);
.
# find the rngd binary
my $command;
.
foreach (clist) {
  -x && ($command = $_) && last;
}
.
# stop if rngd isn't installed
defined $command || die "$0 error: rngd is not installed\n";
.
.
# look for a hw random device
my $source;
my $continue = 1;
$SIG{'ALRM'} = sub { $continue = 0 };
.
foreach my $test (slist) {
  -e $test || next;
.
  alarm 2;
  $continue = 1;
.
  my $bytes = 0;
.
  sysopen FILE, $test, O_RDONLY or next;
  while ($continue) {
    sysread FILE, $_, 4096 or last;
    $bytes += length $_;
  }
  close FILE;
.
  if ($bytes > $want_bytes) {
    $source = $test;
    last;
  }
}
.
.
# use the select command and source
print "starting $command with $source... ";
```

```
system "$command -r $source";
print "done.\n";
.
exit 0;
```

5.3.2.16 Check for the Required Solaris Patch (Solaris Only)

For Oracle Solaris platforms, ensure that the Solaris Operating System patch 144540-01 is installed on the servers. Do this for both Oracle Solaris on SPARC (64-bit) and Oracle Solaris on x86-64 (64-bit) platforms. The Solaris OS patch 144540-01 can be obtained from My Oracle Support.

5.3.2.17 Tune the Socket Buffer Size (AIX Only)

For IBM AIX on POWER Systems (64-bit) platforms, run the following commands as the `root` user:

```
no -o rfc1323=1
```

```
no -o sb_max = 4194304
```

5.3.2.18 Set the SKIP_SLIBCLEAN Variable (AIX Only)

For IBM AIX on POWER Systems (64-bit) platforms, the provisioning install phase installs the Oracle Database client and a database patch update. To prepare your environment for this action, set the SKIP_SLIBCLEAN environment variable as follows:

```
SKIP_SLIBCLEAN = TRUE;export SKIP_SLIBCLEAN;
```

Run `/usr/sbin/slibclean` as `root` and ensure that the value `TRUE` is in uppercase as this value is case sensitive.

5.3.2.19 Add Variable for SKIP_ROOTPRE to Command Line (AIX Only)

When installing a transaction database with the Provisioning Wizard on IBM AIX on POWER Systems (64-bit), you must add the following variable to the command line syntax used to start the wizard:

```
export SKIP_ROOTPRE=TRUE
```

5.3.2.20 Improve Provisioning Performance (AIX Only)

On IBM AIX on POWER Systems (64-bit) systems, the provisioning performance slows down or times out when the Oracle Fusion Applications Provisioning host, the Oracle Database host, and the Oracle Identity Management host are located in different subnets or when these hosts are situated at a distance of more than four network hops.

For provisioning, use the hosts that are located in the same subnet or the hosts that are within a distance of four network hops.

5.3.2.21 Set Up the Server and the Shared Area Permissions (Windows x64)

For Microsoft Windows x64 (64-bit) platforms, complete these steps on each provisioning host:

1. Create a `domain\user` that is part of the Administrators group.
2. Log in as the user that you created.
3. Run `secpol.msc` (security policy) and add the `domain\user` that you created to "Log on as service" under the Local Policies, User Rights Assignment option.

4. Create a folder on a shared disk which will be the Oracle Fusion Applications Home (denote this location as `APPLICATIONS_BASE`). The folder must be accessible to all hosts in the provisioned environment. The name of the folder must not exceed eight characters. For example, create a folder called `appbase` under `\ComputerName` and refer to the folder as `\ComputerName\appbase`. Next, you must share this folder with the Windows domain user who will be provisioning the Oracle Fusion Applications environment and give that user read/write permissions to the shared folder as follows:

    1. In Windows Explorer, right click on the `appbase` folder and select **Properties** from the context menu.
    2. In the **Properties** window, click the **Sharing** tab, then click **Share**.
    3. In the **File Sharing** window enter the domain user name using the format `DomainName\userid`.
    4. Click **Add**. This adds the given domain user name to the list of users whom the folder is shared with.
    5. Select the domain user name that has been added and change the permission level to **Read/Write**.
    6. Click **Share** and then click **Done** to save and close the **File Sharing** window.
    7. Click **Close** to close the **Properties** window.

5. Create a symbolic link to the folder that you created in Step 4. Perform this step on all hosts to be provisioned. For example, at the MS-DOS prompt, type the following:

    `C:\>mklink /d C:\`*`falink`*`\`*`ComputerName`*`\appbase`

    Make note of the location and the name of the symbolic link. Later when you create the provisioning response file, enter C:*`falink`* in the Oracle Fusion Applications Home field.

    > **Note:** For non-Windows platforms, you must enter the full file path in the Provisioning Wizard UI when prompted (for example, Oracle Fusion Applications Home, Applications Configuration Directory, and so on). Using symbolic link paths will cause provisioning failure in the later phases.

6. Confirm that a file or folder can be created through the symbolic link from all hosts in the provisioned environment.

7. If you choose not to use the default location, *APPLICATIONS_BASE*`\instance`, as the Applications Configuration Directory, then repeat Steps 5 and 6 to create another symbolic link to the location of your choice. Later when you create the provisioning response file, enter the newly created symbolic link in the Applications Configuration Directory field. If you choose to use the default location, for example, then enter `C:\falink\instance` in the Applications Configuration Directory field.

5.3.2.22 Update Virtual Memory setting to Custom Size (Windows Only)

Before provisioning, change the Virtual Memory setting to Custom Size in the Advanced System Settings of the Microsoft Windows operation system. The recommended Initial Size is one and one-half times the physical RAM and Maximum Size is three times the physical RAM.

5.3.2.23 Microsoft Windows Resource Locking (Windows Only)

Ensure that no other windows or sessions are open while running provisioning. Do not access any of the files or directories under APPLICATIONS_BASE/instance/, which can create locking of the resources and cause failure.

5.4 Preparing the Network

This section describes the network environment configuration required by Oracle Fusion Applications, more specifically these three areas:

- Name Resolution
- Load Balancers or Reverse Proxy
- Firewall

While name resolution configuration applies to all topologies, the remaining topics (load balancer/reverse proxy and firewall) apply only if any of those are present in your topology.

5.4.1 Configuring Name Resolution

At this point you should configure name resolution for all endpoints in your environment. This includes:

- Web Tier Virtual Hosts (Internal and External), if used
- HTTP LBR Endpoints (Internal and External), if used
- LDAP Endpoints
- Oracle WebCenter Content (UCM) LBR Endpoint, if the environment is highly available
- AdminServer VIPs, if used
- Managed Server VIPs, if used

Name resolution can be done in DNS or in the Hosts file. Each table has a column called Name Resolution which defines if that specific endpoint should be resolved via DNS or Hosts file.

5.4.1.1 Name Resolution for Oracle Fusion Applications Web Tier Virtual Hosts

Use Table 5–2 along with the information in the *Oracle Fusion Applications Installation Workbook* to create the necessary DNS or Hosts entries for name resolution for your environment.

Table 5–2 Name Resolution for Oracle Fusion Applications Web Tier Virtual Hosts

Name resolution for	Name for HTTP Endpoint	Points at IP Address
Oracle Fusion Applications (for each component: Financials, Projects, Procurement, Supplier Portal, IC, Common, CRM, SCM, HCM, BI)	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> FA WebTier Virtual Hosts -> ■ FA WebTier Internal Name (for each component) ■ FA WebTier External Name (for each component)	FA WebTier *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> FA WebTier Virtual Hosts -> IP Endpoint

Table 5–2 (Cont.) Name Resolution for Oracle Fusion Applications Web Tier Virtual

Name resolution for	Name for HTTP Endpoint	Points at IP Address
Oracle Identity Management (IDM and IDM Admin)	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> IDM WebTier Virtual Hosts -> ■ IDM WebTier Internal Name (for each component) ■ IDM WebTier External Name (for each component)	IDM WebTier *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> IDM WebTier Virtual Hosts -> IP Endpoint

5.4.1.2 Name Resolution for HTTP LBR Endpoints

Use Table 5–3 along with the information in the *Oracle Fusion Applications Installation Workbook* to create the necessary DNS or Hosts entries for name resolution for your environment:

Table 5–3 Name Resolution for HTTP LBR Endpoints

Name resolution for	Name for HTTP Endpoint	Points at IP Address
External	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> External Name (for each component)	External Load Balancer / Reverse Proxy *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> External IP Endpoint
Internal	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> Internal Name (for each component)	Internal Load Balancer / Reverse Proxy *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> Internal IP Endpoint

5.4.1.3 Name Resolution for LDAP Endpoints

Use Table 5–4 along with the information in the *Oracle Fusion Applications Installation Workbook* to create the necessary DNS or Hosts entries for name resolution for your environment:

Table 5–4 Name Resolution for LDAP Endpoints

Name resolution for	Name for LDAP Endpoint	Points at IP Address
Policy Store (OID)	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> LDAP Endpoints -> Hostname	Internal Load Balancer, if using one; otherwise OID *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> IP Endpoint

Table 5–4 (Cont.) Name Resolution for LDAP Endpoints

Name resolution for	Name for LDAP Endpoint	Points at IP Address
Identity Store (OVD)	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> Hostname	Internal Load Balancer, if using one; otherwise OVD *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> IP Endpoint

5.4.1.4 Name Resolution for Other Endpoints

Use Table 5–5 along with the information in the *Oracle Fusion Applications Installation Workbook* to create the necessary DNS or Hosts entries for name resolution for your environment:

Table 5–5 Name Resolution for Other Endpoints

Name Resolution for	Name for Endpoint	Points at IP Address
UCM LBR Endpoint	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> UCM LBR Endpoint -> Hostname	Internal Load Balancer, if using one; otherwise not necessary *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> UCM LBR Endpoint -> IP Endpoint
AdminServer Virtual Hosts / VIPs	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> AdminServer Virtual Hosts / VIPs -> Virtual Hostname column (for each component)	Active AdminServer host for each domain *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> AdminServer Virtual Hosts / VIPs -> Virtual IP column (for each component)
Managed Server Virtual Hosts/ VIPs	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> Managed Server Virtual Hosts/ VIPs -> Virtual Hostname column (for each component) (multiple columns for HA)	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> Managed Server Virtual Hosts/ VIPs -> Virtual IP column (for each component) (multiple columns for HA)

5.4.2 Configuring Load Balancers/Reverse Proxy

If your Oracle Fusion Applications Topology includes the use of a Load Balancer or Reverse Proxy, they must be configured appropriately for Oracle Fusion Applications, which has specific requirements for:

- Load balancing settings
- SSL termination

- Mappings

The instructions provided distinguish between internal traffic (to Internal HTTP endpoints and TCP/LDAP endpoints) and external traffic (External HTTP endpoints), so they can be used for topologies with one or two load balancer devices deployed separately on each network (internal and external). For more information about load balancer placement on the network, see Section 4.1.3.3, "Network Placement of Load Balancers/Reverse Proxy".

If the topology has a single load balancer device deployed on a single network, ensure the security implications of this have been fully considered and ensure the relevant firewall ports are opened to allow traffic through it. For more information about how to configure the firewall, see Section 5.4.3, "Configuring Firewalls".

5.4.2.1 Configure Load Balancer/ Reverse Proxy Settings

If a Load Balancer/Reverse proxy is being used, follow the guidelines from Section 4.1.3.4, "Load Balancer Feature Requirements" along with your own requirements to configure their settings.

5.4.2.2 Configure Certificates and SSL

Oracle Fusion Applications configures SSL to terminate at the Load Balancer/Reverse Proxy, so you may also have to configure certificates, as appropriate, on your Load Balancer/Reverse Proxy.

The *Oracle Fusion Applications Installation Workbook*, SSL and Certificates tab contains the SSL Communication table which lists the communication that will be SSL-enabled during installation. In the current release of Oracle Fusion Applications there are two options for SSL termination:

- External HTTP Endpoints (mandatory)
- IDM Admin HTTP Endpoint (optional)

If you are using a Load Balancer, set up certificates appropriately and ensure that SSL termination is configured for the endpoints that will use SSL when executing the next section.

5.4.2.3 Configure Load Balancer/Reverse Proxy Mappings

Once name resolution for endpoints is configured, the Load Balancer or Reverse Proxy mappings must be configured if one is being used. Use Table 5–6 along with the information in the *Oracle Fusion Applications Installation Workbook* to create the necessary Load Balancer/Reverse Proxy mappings:

5.4.2.3.1 External HTTP LBR Endpoints These should be configured at the Load Balancer/Reverse Proxy that provides external access to Oracle Fusion Applications (for end-users and external integrations as shown in Table 5–6).

Table 5–6 External HTTP LBR Endpoints

External LBR Mapping for	Hostname on LBR/RP	Port on LBR/RP	Maps to (Node)	Maps to (Port)
Oracle Fusion Applications (for each component: Financial, Projects, Procurement, Supplier Portal, IC, Common, CRM, SCM, HCM, BI)	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> External Name column (for each component)	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> External Port column (for each component)	*Oracle Fusion Applications Installation Workbook* - Topology tab -> Topology -> All nodes containing the component FA Web Tier	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> FA WebTier Virtual Hosts -> External Port column (for each component)
Oracle Identity Management (IDM)	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> External Name	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> External Port	*Oracle Fusion Applications Installation Workbook* - Topology tab -> Topology -> All nodes containing the component IDM Web Tier	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> IDM WebTier Virtual Hosts -> External Port

5.4.2.3.2 Internal HTTP Endpoints

The default configuration when using the Load Balancer option during Oracle Fusion Applications provisioning is for the source environment to also have internal endpoints at the load balancer. In this case, you must also create appropriate mappings. Note that internal and external Load Balancer/Reverse Proxy(s) may be different.

Table 5–7 Internal HTTP Endpoints

Internal LBR Mapping for	Hostname on LBR/RP	Port on LBR/RP	Maps to (Node)	Maps to (Port)
Oracle Fusion Applications (for each component: Financial, Projects, Procurement, Supplier Portal, IC, Common, CRM, SCM, HCM, BI)	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> Internal Name column (for each component)	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> Internal Port column (for each component)	*Oracle Fusion Applications Installation Workbook* - Topology tab -> Topology -> All nodes containing the component FA Web Tier	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> FA WebTier Virtual Hosts -> Internal Port column (for each component)

Table 5–7 (Cont.) Internal HTTP Endpoints

Internal LBR Mapping for	Hostname on LBR/RP	Port on LBR/RP	Maps to (Node)	Maps to (Port)
Oracle Identity Management (IDM and IDM Admin)	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> Internal Name column (for each component)	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> Internal Port column (for each component)	*Oracle Fusion Applications Installation Workbook* - Topology tab -> Topology -> All nodes containing the component IDM Web Tier	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> IDM WebTier Virtual Hosts -> Internal Port column (for each component)

5.4.2.3.3 TCP/LDAP Endpoints

In a highly-available or scaled-out topology, the load balancer is used to route requests to the various instances of Oracle Internet Directory, Oracle Virtual Directory and WebCenter Content. The communication protocol in this case is TCP (more specifically LDAP for OID and OVD).

Table 5–8 TCP/LDAP Endpoints

TCP LBR Mapping for	Hostname on LBR/RP	Port on LBR/RP	Maps to (Node)	Maps to (Port)
Policy Store (OID)	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> LDAP Endpoints -> Hostname	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> LDAP Endpoints -> Port	*Oracle Fusion Applications Installation Workbook* - Topology tab -> Topology -> All nodes containing the component IDM Identity and Access (or all nodes that contain OID)	*Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Identity Management Port Numbers -> Port Number column for Component OID
Identity Store (OVD)	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> LDAP Endpoints -> Hostname	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> LDAP Endpoints -> Port	*Oracle Fusion Applications Installation Workbook* - Topology tab -> Topology -> All nodes containing the component IDM Identity and Access (or all nodes that contain OVD)	*Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Identity Management Port Numbers -> Port Number column for Component OVD

Table 5–8 (Cont.) TCP/LDAP Endpoints

TCP LBR Mapping for	Hostname on LBR/RP	Port on LBR/RP	Maps to (Node)	Maps to (Port)
UCM (Oracle WebCenter Content)	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> UCM LBR Endpoint -> Hostname	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> UCM LBR Endpoint -> Port	*Oracle Fusion Applications Installation Workbook* - Topology tab -> Topology -> All nodes containing the component FA Common Domain (or all nodes that contain the UCM_ server Managed Server)	UCM port will be defined during Oracle Fusion Applications Provisioning (defaults to 7012 when Oracle Fusion Applications base port has the defaul value 7000)

5.4.3 Configuring Firewalls

If your Oracle Fusion Applications environment will be deployed in a topology where its tiers will be separated by firewalls, you will have to configure the firewall to allow traffic through certain ports in order to install and use the environment.

For more information about different Oracle Fusion Applications topologies and tiers, see Section 2.2, "Oracle Fusion Applications Topologies".

Firewalls are normally found between the following tiers:

- End User and Web Tier (DMZ)
- Web Tier (DMZ) and Mid Tier
- Mid Tier and IDM Directory Tier
- Mid Tier and Database Tier

Table 5–9 lists the expected traffic between the different tiers in Oracle Fusion Applications. Use it with the *Oracle Fusion Applications Installation Workbook* and information about your environment's firewall configuration to determine which ports must be opened.

Table 5–9 Expected Traffic between different tiers in Oracle Fusion Applications

From	To	Ports	Protocol	Notes
End user	External Load Balancer/ Reverse Proxy	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> External Port column (for each component)	HTTP	Applicable if a Load Balancer/ Reverse Proxy is used for external HTTP traffic
End User	FA Web Tier	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> FA WebTier Virtual Hosts: FA WebTier Internal Port column (for each component) FA WebTier External Port column (for each component)	HTTP	Applicable if no Load Balancer/ Reverse Proxy is used

Table 5–9 (Cont.) Expected Traffic between different tiers in Oracle Fusion Applications

From	To	Ports	Protocol	Notes
End User	IDM Web Tier	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> IDM WebTier Virtual Hosts: IDM WebTier Internal Port column (for each component) IDM WebTier External Port column (for each component)	HTTP	Applicable if no Load Balancer/ Reverse Proxy is used
External Load Balancer / Reverse Proxy	FA Web Tier	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> FA WebTier Virtual Hosts: FA WebTier Internal Port column (for each component) FA WebTier External Port column (for each component)	HTTP	Applicable if a Load Balancer/ Reverse Proxy is used for external HTTP traffic
External Load Balancer / Reverse Proxy	IDM Web Tier	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> IDM WebTier Virtual Hosts: IDM WebTier Internal Port column (for each component) IDM WebTier External Port column (for each component)	HTTP	Applicable if a Load Balancer/ Reverse Proxy is used for external HTTP traffic
FA Web Tier	FA Mid Tier	All AdminServer and Managed Server ports in all Oracle Fusion Applications WebLogic Domains	HTTP / TCP(T3)	T3 traffic: OHS registration with the AdminServers
FA Web Tier	IDM Application Tier	*Oracle Fusion Applications Installation Workbook* - Network - Ports tab- > Identity Management Port Numbers -> IDMDomain OAM AAA Server Port	TCP (OAP)	OAP traffic: WebGate to OAM Server
IDM Web Tier	IDM Application Tier	All AdminServer and Managed Server ports in the WebLogic IDMDomain	HTTP / TCP (T3) / TCP (OAP)	T3 traffic: OHS registration with the AdminServers OAP traffic: WebGate to OAM Server

Table 5–9 (Cont.) Expected Traffic between different tiers in Oracle Fusion Applications

From	To	Ports	Protocol	Notes
FA Mid Tier	IDM Web Tier	If not using an Load Balancer/Reverse Proxy for Internal HTTP traffic: *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> IDM WebTier Virtual Hosts -> IDM WebTier Internal Port column (for IDM and IDM Admin) If using a Load Balancer/Reverse Proxy for Internal HTTP traffic: *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> Internal Port column (for IDM and IDM Admin)	HTTP	
FA Mid Tier	IDM Directory Tier	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> LDAP Endpoints -> Port and SSL Port columns for Policy Store (OID) and Identity Store (OVD)	TCP (LDAP)	
FA Mid Tier	FA Mid Tier (via LBR)	UCM port will be defined during Oracle Fusion Applications Provisioning (defaults to 7012 when Oracle Fusion Applications base port is at the default value 7000)	TCP	Applicable only for HA environments where UCM will have a load balancer as frontend
IDM Mid Tier	FA Web Tier	If not using an Load Balancer/Reverse Proxy for Internal HTTP traffic: *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> FA WebTier Virtual Hosts -> FA WebTier Internal Port column (for HCM) If using a Load Balancer/Reverse Proxy for Internal HTTP traffic: *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> Internal Port column (for HCM)	HTTP	For OIM callbacks to HCM
IDM Application Tier	IDM Directory Tier	*Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> LDAP Endpoints -> Port and SSL Port columns for Policy Store (OID) and Identity Store (OVD)	TCP (LDAP)	
FA Mid Tier	FA Database	*Oracle Fusion Applications Installation Workbook* - Database tab -> FA Transactional Database -> Ports for each one of the FA DB Instances	SQL*Net / JDBC	

Table 5–9 (Cont.) Expected Traffic between different tiers in Oracle Fusion Applications

From	To	Ports	Protocol	Notes
FA Mid Tier	IDM Database	*Oracle Fusion Applications Installation Workbook* - Database tab -> IDM Database -> Ports for each one of the IDM DB Instances	SQL*Net / JDBC	
IDM Mid Tier	IDM Database	*Oracle Fusion Applications Installation Workbook* - Database tab -> FA Transactional Database -> Ports for each one of the FA DB Instances	SQL*Net / JDBC	
IDM Mid Tier	OID Database	*Oracle Fusion Applications Installation Workbook* - Database tab -> OID Database -> Ports for each one of the OID DB Instances	SQL*Net / JDBC	Applies only if a separate OID database is used
FA Mid Tier	FA Data Warehouse Database	*Oracle Fusion Applications Installation Workbook* - Database tab -> FA Data Warehouse Database -> Ports for each one of the FA DW DB Instances	SQL*Net / JDBC	Applies only if a Data Warehouse database is used

5.5 Creating the Oracle Fusion Applications Provisioning Repository

The provisioning repository contains all the installers required to provision a new Oracle Fusion Applications environment. You download the repository from the Oracle Fusion Applications Product Media Package to a location of your choice (*`repository_location`*).

The Oracle Identity Management Lifecycle Tools and the Oracle Fusion Applications provisioning wizard are packaged in the same Oracle Fusion Applications Media Packs that you download from Oracle Software Delivery Cloud as detailed in Section 5.5.2, "Download from the Oracle Software Delivery Cloud Portal". Oracle Identity Management is in the `idmlcm` folder and the Oracle Fusion Applications provisioning wizard is in the `faprov` folder. When you install Oracle Identity Management ensure that the provisioning repository is accessible to the Oracle Identity Management hosts.

Note: If you want to set up a demilitarized zone (DMZ) for the web tier in your new environment, see Section 6.4 before you create the repository.

5.5.1 Obtain the Software

Oracle groups its software releases by product area. A **Product Media Pack** refers to those groupings. Each media pack may also include a zipped file containing electronic documentation files or "Quick Install" files, which facilitate the initial installation of the software.

Note: For installations of Oracle Fusion Applications, you must have available the complete set of software contained in the product media pack. You cannot install from individual pieces. Therefore, if you need to install from media that is no longer available on Oracle Software Delivery Cloud, contact My Oracle Support to obtain the complete media pack.

After you have completed the software licensing agreements, you can obtain the Oracle Fusion Applications software using one of these two methods:

- **Oracle Software Delivery Cloud Portal**: Provides you with a readme document that helps you to determine which media you need to fulfill the license you have purchased. You download only the media you need. This is the default delivery method.
- **My Oracle Support**: Provides a complete set of the software in DVD format. You use only the DVDs covered by your software licensing agreement.

Using either method, you can obtain the Oracle Fusion Applications Provisioning repository and gain access to the Oracle Fusion Applications documentation library.

If you are downloading Oracle Fusion Applications 11g Media Pack for the following platforms, then use the following version (and above) of the UnZip / 7-Zip utility to extract the Oracle software to a location of your choice (*REPOSITORY_LOCATION*). UnZip is freeware that is available at: `http://www.info-zip.org`. Oracle has also made copies available for most commonly used platforms at: `https://updates.oracle.com/unzips/unzips.html`.

- Linux x86-64 (64-bit) - Info-ZIP version 6.0
- Oracle Solaris on SPARC (64-bit) - Info-ZIP version 6.0
- Oracle Solaris on x86-64 (64-bit) - Info-ZIP version 6.0
- IBM AIX on POWER Systems (64-bit) - Info-ZIP version 6.10
- Microsoft Windows x64 (64-bit) - 7-Zip version 9.20

5.5.1.1 Xcopy Utility Should Not Be Used To Copy Fusion Application Repositories and APPLTOP on Microsoft Windows

The Microsoft Windows utility Xcopy does not copy long path names. Therefore, do not use Xcopy to copy Oracle Fusion Applications repositories and APPLTOP.

Resolution: Use Robocopy instead of Xcopy.

5.5.2 Download from the Oracle Software Delivery Cloud Portal

Go to `http://edelivery.oracle.com/` and follow these instructions:

1. Complete the Export Validation process by entering basic identification information using the online form.
2. On the Media Pack Search page, specify the product pack and platform to identify the media pack you want to download. If you do not know the name of the product pack, you can search for it using the license list.
3. Choose the appropriate media pack from the search results and download the provisioning repository (in zipped format). You can download the repository to a location of your choice.
4. Extract the contents of all the zipped files to the same target directory. The directory must be on a networked drive or shared disk so that it will be accessible to all the hosts in your new environment. By default, the unzip process places the installers in *`repository_location`*`/installers`.

Note: Create the repository location name so that unzipping the files does not run into the Windows MAX_PATH limitation.

Note: Do not unzip different versions of Oracle Fusion Applications Media Packs into the same location. This will cause errors when you try to provision Oracle Fusion Applications files.

5.5.2.1 Download Language Pack Software

If you use languages other than US English and want to install these languages during the initial installation process, perform the steps in this section.

1. Download the Oracle Fusion Applications NLS 11*g* Release 8 software for each language you want to install. This is available from the NLS DVD media or from Oracle Software Delivery Cloud. The software for 11*g* Release 8 is a zip file that contains a repository of the translated Oracle Fusion Applications files plus the installation utilities that are required for you to install the software.
2. If there are no post-installation patches in the *Oracle Fusion Applications NLS release notes* when you run Language Pack Installer, there is no action required for this step and you have completed the download for language pack software.

   Language Pack Installer can apply mandatory post-installation patches that are required by Oracle Fusion Applications if you download the patches from My Oracle Support before you start the installation. Note that this feature relates only to patches that are documented in the Oracle Fusion Applications NLS release notes and that are specifically required for the language pack you are installing.

   Perform the following steps to download the patches:

   a. Create a directory named `11.1.8.0.0_post_repo_patches` in the parent directory of your *`APPLICATIONS_BASE`* directory. For example, if *`APPLICATIONS_BASE`* is `/u01/APPTOP`, the patch directory is `/u01/11.1.8.0.0_post_repo_patches`.

   b. Copy `PostRepoPatchDirs.zip` from the *`REPOSITORY_LOCATION`*`/installerspreinstall` directory to the `11.1.8.0.0_post_repo_patches` directory.

   c. Unzip `PostRepoPatchDirs.zip` in the `11.1.8.0.0_post_repo_patches` directory to create the directory structure for the patches you download.

   d. Review the `README.txt` file that was created when you unzipped *`REPOSITORY_LOCATION`*`/installers/pre_install/PostRepoPatchDirs.zip`, to learn how the subdirectories under the `11.1.8.0.0_post_repo_patches` directory map to the corresponding components, such as Oracle Fusion Middleware, database client, and database server components.

   Note: If you choose to download the patches to a different directory, you must use the `-DpatchDownloadLocation` option when you start Language Pack Installer. See Section 16.17.3, "Install a Language" for more information.

   e. Refer to*Oracle Fusion Applications NLS release notes* to find the patches to be downloaded from My Oracle Support.

   f. Download and unzip the patches into the appropriate subdirectory under the `11.1.8.0.0_post_repo_patches` directory, based on the mapping information in the `README.txt` file described in Step d. A failure could result

if you do not download a patch to the correct directory. Note that when you download the Oracle Fusion Applications patches, you must create a patch plan by running the script in Step g.

g. Run this step to create a patch plan. This step assumes that you have downloaded the patches as described in Step f.

The perl script, `adGenerateFAPatchPlan.pl`, reads the patch metadata from the downloaded patches to generate the patch plan file, `FAPatchPlan.xml`. To run this script, use the Perl executable from *APPLICATIONS_BASE*`/dbclient/perl/bin` for UNIX platforms and *APPLICATIONS_BASE*`\dbclient\perl\5.8.3\bin\MSWin32-x64-multi-thread` for Windows.

Use the following command syntax to create the patch plan file:

```
UNIX:
setenv PERL5LIB $APPLICATIONS_BASE/dbclient/perl/lib/5.8.3:$APPLICATIONS_
BASE/dbclient/perl/lib/site_perl/5.8.3/:
$APPLICATIONS_BASE/dbclient/perl/lib/site_perl

$APPLICATIONS_BASE/dbclient/perl/bin/perl
$APPLICATIONS_
BASE/fusionapps/applications/lcm/ad/bin/adGenerateFAPatchPlan.pl patches_
download_location

Windows:
SET PERL5LIB=%APPLICATIONS_BASE%\dbclient\perl\5.8.3;%APPLICATIONS_
BASE%\dbclient\perl\site\5.8.3\;
%APPLICATIONS_BASE%\dbclient\perl\site

%APPLICATIONS_BASE%\dbclient\perl\5.8.3\bin\MSWin32-x64-multi-thread\perl
%APPLICATIONS_
BASE%\fusionapps\applications\lcm\ad\bin\adGenerateFAPatchPlan.pl patches_
download_location
```

5.5.3 Obtain DVDs from My Oracle Support

You can order a complete set of the software in DVD format by contacting My Oracle Support. You can use only the DVDs covered by your software licensing agreement.

5.5.4 Verify Required Operating System Packages and Libraries

Oracle Fusion Applications require specific operating system packages and libraries in the hosts where the software is installed. During the preverify phase of provisioning an Oracle Fusion Applications environment as detailed in Chapter 13, "Provisioning a New Oracle Fusion Applications Environment", the Provisioning Wizard and the provisioning command line verifies if the hosts have the required packages, libraries, and other requirements such as swap space, free space, and kernel parameters. Any issues during the check are reported in the provisioning log. If you want to perform the manual checks ahead of time, follow these steps after you create the provisioning repository.

For Database Host

1. Navigate to *REPOSITORY_LOCATION*`/installer/database/Disk1`.
2. Run the command:

   UNIX: `./runInstaller -executePrereqs -silent`

Windows: `setup.exe -executePrereqs -silent -jreLoc REPOSITORY_LOCATION\jdk6`

3. Review the output located at: `oraInventory/logs/installAction<timestamp>.log`. For example, `oraInventory/logs/installActionyyyy-mm-dd_hh-mm-ssPM.log`.

Other Oracle Fusion Applications Hosts

1. Navigate to *REPOSITORY_LOCATION*`/installer/<product>/Disk1`, where <product> represents:
   - atgf
   - biappsshiphome
   - bishiphome
   - dbclient
   - ecm_bucket2
   - fusionapps
   - odi
   - soa
   - wc
   - webgate
   - webtier

   Optionally, you can also include the following products:
   - bhd
   - gop
2. Run the command:

   UNIX: `./runInstaller -sv -jreLoc REPOSITORY_LOCATION/jdk6`

   Windows: `setup.exe -sv -jreLoc REPOSITORY_LOCATION\jdk6`
3. Review the output located at: `oraInventory/logs/install<timestamp>.out`. For example, `oraInventory/logs/installyyyy-mm-dd_hh-mm-ssAM.out`.
4. Repeat Step 1 to Step 3 for all products listed in Step 1.

Example 5–1 Sample Output

If any of the stated library (or package) is not found, you should obtain and install the library (or package) in order to continue after the preverify phase of the provisioning process.

Note: The list of libraries and version are example values and you should refer to the actual output from your environment for the correct values.

```
$$$$$DEBUG>>>>Packages
Checking for binutils-2.17.50.0.6; found binutils-2.17.50.0.6-20.el5_8.3-x86_64.
Passed
Checking for compat-libstdc++-33-3.2.3-x86_64; found
compat-libstdc++-33-3.2.3-61-x86_64.    Passed
Checking for compat-libstdc++-33-3.2.3-i386; found
```

```
compat-libstdc++-33-3.2.3-61-i386.    Passed
Checking for elfutils-libelf-0.125; found elfutils-libelf-0.137-3.el5-x86_64.
Passed
Checking for elfutils-libelf-devel-0.125; found
elfutils-libelf-devel-0.137-3.el5-x86_64.    Passed
Checking for gcc-4.1.1; found gcc-4.1.2-54.el5-x86_64.    Passed
Checking for gcc-c++-4.1.1; found gcc-c++-4.1.2-54.el5-x86_64.    Passed
Checking for glibc-2.5-12-x86_64; found glibc-2.5-107.el5_9.5-x86_64.    Passed
Checking for glibc-2.5-12-i686; found glibc-2.5-107.el5_9.5-i686.    Passed
Checking for glibc-common-2.5; found glibc-common-2.5-107.el5_9.5-x86_64.
Passed
Checking for glibc-devel-2.5-x86_64; found glibc-devel-2.5-107.el5_9.5-x86_64.
Passed
Checking for glibc-devel-2.5-12-i386; Not found.    Failed <<<<
Checking for libaio-0.3.106-x86_64; found libaio-0.3.106-5-x86_64.    Passed
Checking for libaio-0.3.106-i386; found libaio-0.3.106-5-i386.    Passed
Checking for libaio-devel-0.3.106; found libaio-devel-0.3.106-5-i386.    Passed
Checking for libgcc-4.1.1-x86_64; found libgcc-4.1.2-54.el5-x86_64.    Passed
Checking for libgcc-4.1.1-i386; found libgcc-4.1.2-54.el5-i386.    Passed
Checking for libstdc++-4.1.1-x86_64; found libstdc++-4.1.2-54.el5-x86_64.
Passed
Checking for libstdc++-4.1.1-i386; found libstdc++-4.1.2-54.el5-i386.    Passed
Checking for libstdc++-devel-4.1.1; found libstdc++-devel-4.1.2-54.el5-x86_64.
Passed
Checking for make-3.81; found make-1:3.81-3.el5-x86_64.    Passed
Checking for sysstat-7.0.0; found sysstat-7.0.2-12.0.1.el5-x86_64.    Passed
Check complete. The overall result of this check is: Failed <<<<

Check Name:Kernel
Check Description:This is a prerequisite condition to test whether the minimum
required kernel parameters are configured.
Checking for VERSION=2.6.18; found VERSION=2.6.18-348.4.1.0.1.el5.    Passed
Checking for hardnofiles=4096; found hardnofiles=327679.    Passed
Checking for softnofiles=4096; found softnofiles=327679.    Passed
Check complete. The overall result of this check is: Passed
Kernel Check: Success.
Checking for VERSION=2.6.18; found VERSION=2.6.18-348.4.1.0.1.el5.    Passed
Checking for hardnofiles=4096; found hardnofiles=327679.    Passed
Checking for softnofiles=4096; found softnofiles=327679.    Passed
Check complete. The overall result of this check is: Passed

Check Name:GLIBC
Check Description:This is a prerequisite condition to check whether the
recommended glibc version is available on the system
Expected result: ATLEAST=2.5-12
Actual Result: 2.5-107.el5_9.5
Check complete. The overall result of this check is: Passed
GLIBC Check: Success.
Expected result: ATLEAST=2.5-12
Actual Result: 2.5-107.el5_9.5
Check complete. The overall result of this check is: Passed
```

5.6 What to Do Next

You must install the Oracle Identity Management Lifecycle Tools and the Oracle Fusion Applications Provisioning Framework. Go to Chapter 6 to get started.

6

Installing the Oracle Identity Management and Oracle Fusion Applications Provisioning Frameworks

This chapter describes how to install the Oracle Identity Management and Oracle Fusion Applications provisioning frameworks.

This chapter includes the following sections:

6.1 Introduction to Oracle Identity Management and Oracle Fusion Applications Provisioning Frameworks

The Oracle Identity Management Provisioning Framework which consists of the Oracle Identity Management Provisioning Wizard and related tools was developed to automate Oracle Identity Management Provisioning and reduce the time required to configure Oracle Identity Management for Oracle Fusion Applications.

The Oracle Fusion Applications Provisioning installer (faprov) is delivered with the other installers in the provisioning repository. The purpose of faprov is to create the Oracle Fusion Applications Provisioning framework consisting of the Provisioning Wizard, Provisioning Command-line interface and Provisioning-related files and utilities.

6.2 Installing the Oracle Identity Management Provisioning Tools

The Oracle Identity Management Provisioning tools share a repository with the Oracle Fusion Applications Provisioning tools.

The software required by Oracle Identity Management is located in the Oracle Fusion Applications repository. If you have not already done so then you need to create an Oracle Fusion Applications provisioning repository as described in Section 5.5, "Creating the Oracle Fusion Applications Provisioning Repository".

6.2.1 Verify Java and Ant

Ensure that your Provisioning Repository contains Java and Ant. Java should reside in a directory called `jdk6`. Ant should reside in a directory called `ant`. The paths should be:

UNIX:

```
REPOSITORY_LOCATION/jdk6
IDMLCM_HOME/provisioning/ant
```

Windows:

```
REPOSITORY_LOCATION\jdk6
IDMLCM_HOME\provisioning\ant
```

For more information about the contents of the provisioning framework, See Table 6–2.

6.2.2 Oracle Identity Management Provisioning Framework Installation Checklist

Before initiating the Oracle Identity Management Provisioning Framework installation, verify the following checklist:

- Necessary infrastructure
  - Access to the server console is provided for the OS User (VNC recommended).
  - The provisioning repository or Oracle Database installer are available and accessible from the node where you install the Oracle Identity Management Provisioning Framework.
- Prerequisites for the host where you will install the Oracle Identity Management Provisioning Framework.

6.2.3 Installing the Oracle Identity Management Lifecycle Tools

The Oracle Identity Management Provisioning Wizard is a component of the Oracle Identity Management Lifecycle Tools, which also includes the Oracle Identity Management Patching Framework. You must install the tools by running an installer, which is located in the provisioning repository.

In a multi-host environment, the Oracle Identity Management Lifecycle Tools must be visible to each host in the topology.

The installation script for the Oracle Identity Management Lifecycle Tools resides in the directory:

```
REPOSITORY_LOCATION/installers/idmlcm/idmlcm/Disk1
```

where *REPOSITORY_LOCATION* is the Oracle Fusion Applications provisioning repository, as described in Section 5.5, "Creating the Oracle Fusion Applications Provisioning Repository".

To begin installing the tools, change to that directory and start the script.

UNIX:

```
cd REPOSITORY_LOCATION/installers/idmlcm/idmlcm/Disk1
./runInstaller -jreLoc REPOSITORY_LOCATION/jdk6
```

Windows:

```
cd REPOSITORY_LOCATION\installers\idmlcm\idmlcm\Disk1
setup.exe -jreLoc REPOSITORY_LOCATION\jdk6
```

Then proceed as follows:

1. On the Welcome page, click **Next**.
2. If you are running on a UNIX platform, and you have not previously installed an Oracle product on this host, you might be presented with the Specify Inventory Directory page, which prompts you for the location of the **Inventory Directory**. This directory is used to keep track of all Oracle products installed on this host. If you see this page, proceed as follows:

   In the **Operating System Group ID** field, select the group whose members you want to grant access to the inventory directory. All members of this group can install products on this host. Click **OK** to continue.

   The **Inventory Location Confirmation** dialog prompts you to run the *inventory_directory*/createCentralInventory.sh script as root to create the /etc/oraInst.loc file. This file is a pointer to the central inventory and must be present for silent installations. It contains two lines:

   ```
   inventory_loc=path_to_central_inventory

   inst_group=install_group
   ```

   The standard location for this file is /etc/oraInst.loc, but it can be created anywhere. If you create it in a directory other than /etc, you must include the -invPtrLoc argument and enter the location of the inventory when you run the Identity ManagementProvisioningWizard or the runIDMProvisioning script.

   If you do not have root access on this host but want to continue with the provisioning, select **Continue installation with local inventory**.

   Click **OK** to continue.
3. On the Prerequisite Checks page, verify that checks complete successfully, then click **Next**.
4. On the Specify Install Location page, enter the following information:

   a. **Oracle Middleware Home** - This is the parent directory of the directory where the Oracle Identity Management Provisioning Wizard will be installed. In a multi-host Oracle Identity Management environment, this must be on shared storage. for example:

      ```
      /u01/tools
      ```

   b. **Oracle Home Directory** - This is a subdirectory of the Oracle Middleware Home directory where the wizard will be installed. For example:

      ```
      idmlcm
      ```

      In the current guide, this subdirectory is referred to as *IDMLCM_HOME*.

   Click **Next**.
5. On the Installation Summary page, click **Install**.
6. On the Installation Progress page, click **Next**.
7. On the Installation Complete page, click **Finish**.

6.3 Installing the Oracle Fusion Applications Provisioning Framework

The Oracle Fusion Applications Provisioning installer (faprov) is delivered with the other installers in the provisioning repository. The purpose of faprov is to create the

Oracle Fusion Applications Provisioning framework, which contains the following components:

- **Provisioning Wizard**: A question-and-answer interview that guides you through the process of installing a database, creating or updating a response file, and provisioning or deinstalling an Oracle Fusion Applications environment.

  Note:

  - Run the Provisioning Wizard on the primordial host to create a provisioning response file. If you run the Provisioning Wizard on a non-primordial host to create a provisioning response file, the validation assumes that the host is the primordial host. Ensure that you interpret the validation errors correctly as they may not be applicable to the non-primordial host.
  - When provisioning a new environment, you should only run the Provisioning Wizard on the primordial host and the Provisioning Command-line Interface on non-primordial hosts.

- **Provisioning Command-Line Interface (CLI)**: Used for starting the wizard and running installation phases on the Primary host, Secondary host, and DMZ host (when present).
- **Provisioning-related files and utilities**: The ANT utilities, binary files, library files, templates, locations of saved response files and provisioning build scripts, and other provisioning utilities required for performing provisioning tasks.

Because the provisioning installer is a customized version of the Oracle Universal Installer (OUI), its behavior closely resembles that of the OUI.

6.3.1 Oracle Fusion Applications Provisioning Framework Installation Checklist

Before initiating the Oracle Fusion Applications provisioning framework installation, verify the following checklist:

- Necessary infrastructure
  - Access to the server console is provided for the OS User (VNC recommended).
  - The provisioning repository or Oracle Database installer are available and accessible from the node where you install the Oracle Fusion Applications provisioning framework.
- Prerequisites for the host where you will install the Oracle Fusion Applications provisioning framework.

6.3.2 Run the Provisioning Framework Installer

To install the provisioning framework, locate the directory `REPOSITORY_LOCATION/installers/faprov/Disk1` and run the script, `runInstaller` or `setup.exe`, depending on your hardware platform. Note that `REPOSITORY_LOCATION` is the directory where you created the provisioning repository.

Note: You should not run the scripts, `runInstaller` or `setup.exe`, located in `REPOSITORY_LOCATION/installers/fusionapps/Disk1`. These scripts are used and run by the Provisioning Wizard and Provisioning Command-line Interface when needed. They are not meant for installing the provisioning framework.

1. Use this command to start OUI from the command line to install the Provisioning Wizard. Ensure that you replace `REPOSITORY_LOCATION` with the full file path to the provisioning repository:

   UNIX: `runInstaller -jreLoc REPOSITORY_LOCATION/jdk6`

   Note: If you did not specify `-jreLoc REPOSITORY_LOCATION/jdk6` in the command line, you can enter the file path on the command prompt.

   Windows: `setup.exe  -jreLoc REPOSITORY_LOCATION\jdk6`

   Note: Ensure you are using the 8-character file path format for `REPOSITORY_LOCATION`.

6.3.3 Provisioning Installer Screens and Instructions

Table 6–1 lists the steps for running the provisioning framework installer.

Table 6–1 Provisioning Framework Installation Screen Flow

Screen	Description and Action Required
Specify Inventory Directory (UNIX)	If this is your first Oracle installation on this host, you must specify the location of the **Central Inventory Directory**. It is used by the installer to keep track of all Oracle products installed on this host. The default location for this file varies by platform. **Tip: This value is available in the** *Oracle Fusion Applications Installation Workbook* **- Storage tab -> Inventories -> FA Provisioning Framework**. In the **Operating System Group Name** field, select the group whose members will be granted access to the inventory directory. All members of this group can install products on this host. Click **OK** to continue. **Tip: This value is available in the** *Oracle Fusion Applications Installation Workbook* **- Storage tab -> Shared Storage -> FA Shared -> OS Group Owner**. The **Inventory Location Confirmation** dialog prompts you to run the *inventory_directory*`/createCentralInventory.sh` script as `root` to create the `/etc/oraInst.loc` file. This file is a pointer to the central inventory and must be present for silent installations. It contains two lines: `inventory_loc=`*`path_to_central_inventory`* `inst_group=`*`install_group`* The standard location for this file is `/etc/oraInst.loc`, but it can be created anywhere. Note that the default for Linux and AIX platforms is `/etc/oraInst.loc` and for Solaris and HP, it is `/var/opt/oracle/oraInst.loc`. If you create it in a directory other than `/etc`, you must include the `-invPtrLoc` argument and enter the location of the inventory when you run the `provisioningWizard` or the `runProvisioning` script. If you do not have `root` access on this host but want to continue with the installation, select **Continue installation with local inventory**. Click **OK** to continue.
Welcome	No action is necessary on this read-only screen. Click **Next** to continue.
Prerequisite Checks	Analyzes the host computer to ensure that specific operating system prerequisites have been met. If any prerequisite check fails, the screen displays a short error message at the bottom. Fix the issue that caused the error and click **Retry**. To ignore the error or warning message, click **Continue**. Click **Abort** to stop the prerequisite check process for all components. Click **Next** to continue.
Installation Location	In the **Location** field, specify where you want to install the provisioning framework. This is the location where the Provisioning Wizard and the start command for provisioning are installed. This location is denoted as *FAPROV_HOME*. You can choose any location if it is on a shared disk in a location that is accessible to all hosts in your new environment. **Tip: This value is available in the** *Oracle Fusion Applications Installation Workbook* **- Storage tab -> Install Directories -> FA Provisioning Framework Location**. The installation process creates a logical directory called the Oracle home. This location is where software binaries will be stored. No runtime process can write to this directory. The directory must initially be empty. If you are performing the installation on a Windows operating system, ensure that the directory paths are valid and do not contain a double backslash (`\\`). Click **Next** to continue.

Table 6–1 (Cont.) Provisioning Framework Installation Screen Flow

Screen	Description and Action Required
Installation Summary	Summarizes the selections that you have made during this installation session. To change this configuration before installing, select one of the screens from the left navigation pane or click **Back** to return to a previous screen. When you are satisfied with the details, click **Save** to create a text file (response file) to use if you choose to perform the same installation later. Click **Install** to begin installing this configuration.
Installation Progress	The progress indicator shows the percentage of the installation that is complete, and indicates the location of the installation log file. Click **Next** when the progress indicator shows 100 percent.
Installation Complete	Summarizes the installation just completed. To save the details to a text file, click **Save** and indicate a directory where you want to save the file. Click **Finish** to dismiss the screen and exit the installer.

6.3.4 Provisioning Framework Components

Table 6–2 shows the components in the *FAPROV_HOME*/provisioning directory.

Table 6–2 Contents of the Provisioning Framework

Component Type	Component Name	General Use
ANT	ant	Java processes for installing binaries, configuring domains and subsystems (JDBD and SOA composites), deploying applications, and domain startup
Binary files	bin	Executable files, compiled programs, system files, spreadsheets, compressed files, and graphic (image) files
Library files	lib	Previously defined functions that have related functionality or are commonly used, stored in object code format
Location of saved response files	provisioning-response file	Location for completed or partially completed response files
Location of provisioning build scripts	provisioning-build	Location for build scripts that are available when called for during the provisioning of an environment
Location of templates	template	Start parameters, single sign-on configuration, and database templates
Location of utility files	util	Other provisioning utilities

6.4 Setting Up a Demilitarized Zone (DMZ) for the Web Tier

The web tier contains Oracle HTTP Server, which can be installed on the same shared file system (inside the firewall) as the other components, or exist on a host in a DMZ. If you install the web tier in a DMZ, the web tier host cannot be the same as any other host deployed, regardless of domain.

Installing the web tier in a DMZ enables you to impose more restrictions on communication within the portion of the system that is within the firewall, including the following:

- The DMZ host cannot access the shared storage that is accessible by the hosts within the firewall (in the *APPLICATIONS_BASE* area where the Middleware homes are installed or the shared area).
- The DMZ host may not be able to communicate with the CommonDomain AdminServer through the firewall. If this is the case, web tier running on the DMZ

is **non-managed**; that is, it is not associated with the CommonDomain running inside the firewall.

However, the *APPLICATIONS_BASE* (Oracle Fusion Applications) or *IDM_BASE* (Oracle Identity Management) file path and the directory structure under it remain the same on the DMZ host as for the other hosts that exist inside the firewall.

To set up and configure your web tier on a DMZ host, go to http://edelivery.oracle.com/ and follow these directions:

Note: On a DMZ host, you should not have any symlink or mount points that point to a repository or *APPLICATIONS_BASE* residing inside the firewall, that is, the repository and *APPLICATIONS_BASE* should be accessible from the DMZ host.

---

1. Copy the provisioning repository zipped files to a location on the web tier host to be designated as a demilitarized zone.
2. Run the provisioning framework installers for Oracle Identity Management and Oracle Fusion Applications as described in Section 6.2 and Section 6.3 on the DMZ host. Alternatively, you can copy the provisioning framework (`IDMLCM_HOME` or `FAPROV_HOME`) to the DMZ host.
3. When you create the response file for this environment, indicate this web tier configuration by selecting the **Install Web Tier in DMZ** checkbox. See Section 12.3 for details.
4. When the preverify phase is successful on the primordial host, place a copy of the response file and the generated provisioning plan (`<APPLICATIONS_BASE>/provisioning/plan/provisioning.plan`) on the DMZ host.

6.5 What to Do Next

You must install the Oracle Identity Management and Oracle Fusion Applications database. See Chapter 7 for complete information.

Consider installing Oracle Enterprise Governance, Risk and Compliance (GRC) with Oracle Fusion Applications. Although not required, GRC can serve as part of the user provisioning flow to ensure that proper controls for security exist. For more information, see the Oracle Fusion Applications security guides and also see the *Oracle Application Access Controls Governer Implementation Guide.*

Part IV

Installing the Databases

This part provides instructions to install databases and troubleshoot database installations for Identity Management and Oracle Fusion Applications.

Part IV contains the following chapters:

7

Installing Databases for Oracle Identity Management

This chapter describes how to install and configure the Oracle Identity Management database repositories.

7.1 Introduction to Installing Databases for Oracle Identity Management

The Oracle Identity Management components in the enterprise deployment use database repositories. This chapter describes how to perform the following steps:

- Verify the database requirements as described in Section 4.4.2, "Planning for Database Requirements".
- Verify all decisions that have been made regarding the database and documented in the *Oracle Fusion Applications Installation Workbook*. For more information, see Section 4.4.2, "Planning for Database Requirements".

> **Note:** You may have one or two Oracle Identity Management databases, based on the decision made during the planning phase and documented in the *Oracle Fusion Applications Installation Workbook* - Database tab -> IDM Database -> IDM DB Type. For more information, see Section 4.4.2.5, "Oracle Identity Management Split Database Configuration". The prerequisites in this chapter apply to both databases unless stated otherwise.

- Install and configure the Oracle database repositories. See Section 7.4, "Installing Oracle Database or Oracle Real Application Clusters."

- Create the required Oracle schemas in the database using the Oracle Fusion Middleware Repository Creation Utility (Oracle Fusion Middleware RCU). See Section 7.6, "Running the Oracle Fusion Middleware RCU for Oracle Identity Management."

7.2 Prerequisites for Installing Databases for Oracle Identity Management

An overview of databases and their schemas is in Section 4.4.2, "Planning for Database Requirements". All details in the sections below apply to those databases.

Before loading the metadata repository into your databases, check that they meet the requirements described in these subsections:

- Section 7.2.1, "Database Versions Supported"
- Section 7.2.2, "Patching the Oracle Database"
- Section 7.2.3, "About Initialization Parameters"

7.2.1 Database Versions Supported

To check if your database is certified or to see all certified databases, refer to the "Certified Databases" section in the Certification Document:

`http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html`

To determine the version of your installed Oracle Database, execute the following query at the SQL prompt:

```
select version from sys.product_component_version where product like 'Oracle%';
```

7.2.2 Patching the Oracle Database

Patches are required for some versions of Oracle Database.

7.2.2.1 Patch Requirements for Oracle Database 11g (11.1.0.7)

Table 7–1 lists patches required for Oracle Identity Manager configurations that use Oracle Database 11*g* (11.1.0.7). Before you configure Oracle Identity Manager 11*g*, be sure to apply the patches to your Oracle Database 11*g* (11.1.0.7) database.

Table 7–1 Required Patches for Oracle Database 11g (11.1.0.7)

Platform	Patch Number and Description on My Oracle Support
Linux	7614692: BULK FEATURE WITH 'SAVE EXCEPTIONS' DOES NOT WORK IN ORACLE 11G
	7000281: DIFFERENCE IN FORALL STATEMENT BEHAVIOR IN 11G
	8327137: WRONG RESULTS WITH INLINE VIEW AND AGGREGATION FUNCTION
	8617824: MERGE LABEL REQUEST ON TOP OF 11.1.0.7 FOR BUGS 7628358 7598314

7.2.2.2 Patch Requirements for Oracle Database 11g (11.2.0.2.0)

If you are using Oracle Database 11*g* (11.2.0.2.0), make sure that you download and install the appropriate version (based on the platform) for the RDBMS Patch Number 10259620. This is a prerequisite for installing the Oracle Identity Manager schemas.

Table 7–2 lists the patches required for Oracle Identity Manager configurations that use Oracle Database 11*g* Release 2 (11.2.0.2.0). Make sure that you download and install the following patches before creating Oracle Identity Manager schemas.

Table 7–2 Required Patches for Oracle Database 11g (11.2.0.2.0)

Platform	Patch Number and Description on My Oracle Support
Linux x86 (32-bit) Linux x86 (64-bit)	RDBMS Interim Patch#10259620.

If this patch is not applied, then problems might occur in user and role search and manager lookup. In addition, search results might return empty result.

Note:

- Apply this patch in ONLINE mode. Refer to the readme.txt file bundled with the patch for the steps to be followed.
- In some environments, the RDBMS Interim Patch has been unable to resolve the issue, but the published workaround works. Refer to the metalink note "Wrong Results on 11.2.0.2 with Function-Based Index and OR Expansion due to fix for Bug:8352378 [Metalink Note ID 1264550.1]" for the workaround. This note can be followed to set the parameters accordingly with the only exception that they need to be altered at the Database Instance level by using ALTER SYSTEM SET <param>=<value> scope=<memory> or <both>.

7.2.3 About Initialization Parameters

The databases must have the following minimum initialization parameters defined:

Table 7–3 Minimum Initialization Parameters for Oracle RAC Databases

Parameter	Value
aq_tm_processes	1
dml_locks	200
job_queue_processes	10
open_cursors	1500
session_max_open_files	50
sessions	500
processes	500
sga_target	512M
pga_aggregate_target	100M
sga_max_size	4G
session_cached_cursors	500

If the database is being used for Oracle Internet Directory, it must have the following minimum initialization parameters defined:

Table 7–4 Minimum Initialization Parameters for Oracle RAC Oracle Internet Directory Databases

Parameter	Value
aq_tm_processes	1
dml_locks	200
job_queue_processes	10
open_cursors	800
session_max_open_files	50
sessions	500
processes	2500
sga_target	4G
pga_aggregate_target	2G
sga_max_size	4G
session_cached_cursors	500
_b_tree_bitmap_plans	FALSE
parallel_max_servers[1]	1

[1] Only required for Oracle Internet Directory Databases where the Oracle RAC system has more than 32 CPUs.

Note: For guidelines on setting up optimum parameters for the Database, see *Oracle Fusion Applications Performance and Tuning Guide*.

7.3 Oracle Identity Management Database Installation Checklist

Before initiating the Oracle Identity Management database installation, verify the following checklist:

- Necessary infrastructure
  - Access to the database server console is provided for the database OS User as well as root/pseudo access (VNC recommended).
  - The provisioning repository or Oracle database installers are available and accessible from the database nodes.
- Prerequisites for the database server
  - General Oracle database prerequisites have been satisfied.
- Planning
  - *Oracle Fusion Applications Installation Workbook* - Databases tab -> Identity Management Database and OID Database tables have information that will be used for the database installation.

7.4 Installing Oracle Database or Oracle Real Application Clusters

Install and configure the database repository as follows:

Oracle Clusterware

- For 10*g* Release 2 (10.2), see the *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide* for your platform, listed in "Related Documents".
- For 11*g* Release 1 (11.1), see *Oracle Clusterware Installation Guide*.

Automatic Storage Management

- For 10*g* Release 2 (10.2), see *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide* for your platform, listed in "Related Documents".
- For 11*g* Release 1 (11.1), see *Oracle Clusterware Installation Guide*.
- When you run the installer, select the **Configure Automatic Storage Management** option in the **Select Configuration** screen to create a separate Automatic Storage Management home.

Oracle Real Application Clusters

- For 10*g* Release 2 (10.2), see *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide* for your platform.
- For 11*g* Release 1 (11.1), see *Oracle Real Application Clusters Installation Guide*.

Oracle Real Application Clusters Database

Create a Real Applications Clusters Database with the following characteristics:

- Database must be in archive log mode to facilitate backup and recovery.
- Optionally, enable the Flashback database.
- Create UNDO tablespace of sufficient size to handle any rollback requirements during the Oracle Identity Manager reconciliation process.
- Database is created with ALT32UTF8 character set.

7.5 Preparing the Oracle Identity Management Database for the Oracle Fusion Middleware RCU

To prepare the Oracle Database, follow the instructions in the section "RCU Requirements for Oracle Databases" in the *Oracle Fusion Middleware System Requirements and Specifications*.

On UNIX, execute the following commands to create XATRANS Views:

```
cd $ORACLE_HOME/rdbms/admin
sqlplus / as sysdba
@xaview.sql
```

On Windows, the commands are:

```
cd %ORACLE_HOME%\rdbms\admin
sqlplus / as sysdba
@xaview.sql
```

Ensure that the view v$pending_xatrans$ is created. This can be achieved by running the following SQL commands:

```
DROP VIEW v$xatrans$;
DROP VIEW v$pending_xatrans$;
```

```
CREATE VIEW v$pending_xatrans$ AS
(SELECT global_tran_fmt, global_foreign_id, branch_id
FROM   sys.pending_trans$ tran, sys.pending_sessions$ sess
WHERE  tran.local_tran_id = sess.local_tran_id
AND    tran.state != 'collecting'
AND    BITAND(TO_NUMBER(tran.session_vector), POWER(2, (sess.session_id - 1))) =
sess.session_id)
/


CREATE VIEW v$xatrans$ AS
 (((SELECT k2gtifmt, k2gtitid_ext, k2gtibid
FROM x$k2gte2
WHERE  k2gterct=k2gtdpct)
MINUS
SELECT global_tran_fmt, global_foreign_id, branch_id
 FROM   v$pending_xatrans$)
UNION
SELECT global_tran_fmt, global_foreign_id, branch_id
 FROM   v$pending_xatrans$)
 /
```

7.6 Running the Oracle Fusion Middleware RCU for Oracle Identity Management

Unzip the Oracle Fusion Middleware RCU zip file
Linux: *REPOSITORY_LOCATION*/installers/fmw_rcu/linux/rcuHome.zip

or

Windows: *REPOSITORY_LOCATION*/installers/fmw_rcu/windows/rcuHome.zip

to: *REPOSITORY_LOCATION*/installers/rcu

where *REPOSITORY_LOCATION* is the Oracle Fusion Applications provisioning repository, as described in "Section 5.5, "Creating the Oracle Fusion Applications Provisioning Repository".

Use the Oracle Identity Management version of RCU, which now exists in that directory.

The Oracle Fusion Middleware RCU needs to be set up for the following components: ODS, OIF, OIM, OAM. You must use FA as the prefix for the schema names.

Optionally, you can use two database instances for Oracle Identity Management. If you do this, install ODS in one database instance and other components in the second database instance

You must select a single password for all the schema while running the RCU.

Note: The Oracle Fusion Middleware RCU is available only on Windows and Linux platforms. For other platforms, such as Solaris and AIX, you must install and run the Oracle Fusion Middleware RCU from a Windows or Linux machine.

You run the Oracle Fusion Middleware RCU to create the collection of schemas used by Oracle Identity Management and Management Services.

1. Start the Oracle Fusion Middleware RCU by issuing this command:

   FMW_RCU_HOME/bin/rcu &

2. On the Welcome screen, click **Next**.
3. On the Create Repository screen, select the **Create** operation to load component schemas into a database. Then click **Next**.
4. On the Database Connection Details screen, provide the information required to connect to an existing database. For example:

   Database Type: `Oracle Database`

   - **Host Name:** Enter one of the Oracle RAC nodes. Enter the VIP address of one of the RAC database nodes or the database SCAN address, for example: `DB-SCAN.mycompany.com`
   - **Port:** The port number for the database listener *(DB_LSNR_PORT)*. For example: `1521`
   - **Service Name:** The service name of the database. For example `OIDEDG.mycompany.com`.
   - **Username:** `sys`
   - **Password:** The sys user password
   - **Role:** `SYSDBA`

   Click **Next**.
5. On the Check Prerequisites screen, click `OK` after the prerequisites have been validated.
6. On the Select Components screen, provide the following values:

   Create a New Prefix: Enter a prefix to be added to the database schemas, for example, enter `FA`.

   > **Note:** All schemas except for the ODS schema are required to have a prefix. In this release, the Oracle Fusion Middleware RCU prefix must be `FA`.

   Components: Select the schemas shown in the following table:

Product	Oracle Fusion Middleware RCU Option	Service Name	Comments
Oracle Internet Directory	Identity Management–Oracle Internet Directory	*Oracle Fusion Applications Installation Workbook* - Database tab -> IDM DB -> Service name (if not using a separate OID DB) OID DB -> Service Name (if using a separate OID DB)	

Product	Oracle Fusion Middleware RCU Option	Service Name	Comments
Oracle Access Manager	Identity Management–Oracle Access Manager	*Oracle Fusion Applications Installation Workbook* - Database tab -> IDMDB -> Service name	Audit Services will also be selected.
Oracle Identity Manager	Identity Management–Oracle Identity Manager	*Oracle Fusion Applications Installation Workbook* - Database tab -> IDMDB -> Service name	Metadata Services, SOA infrastructure, and User Messaging will also be selected.
Oracle Identity Federation	Identity Management–Oracle Identity Federation	*Oracle Fusion Applications Installation Workbook* - Database tab -> IDMDB -> Service name	

Click **Next**.

Notes: If your topology requires more than one database, the following important considerations apply:

- Be sure to install the correct schemas in the correct database.
- You might have to run the Oracle Fusion Middleware RCU more than once to create all the schemas for a given topology.
- The tables in Section 4.4.2, "Planning for Database Requirements" provide the recommended mapping between the schemas and their corresponding databases. Refer to Table 4–5, " Oracle Identity Management Schemas" to ensure that the correct details are entered in this screen.

7. On the Check Prerequisites screen, click **OK** after the prerequisites have been validated.
8. On the Schema Passwords screen, enter the passwords for the schemas. You can choose to use either the same password for all the schemas or different passwords for each of the schemas. Oracle recommends choosing different passwords for different schema's to enhance security

   Click **Next**.
9. On the Map Tablespaces screen, accept the defaults and click **Next**.
10. On the confirmation screen, click **OK** to allow the creation of the tablespaces.
11. On the Creating tablespaces screen, click OK to acknowledge creation of the tablespaces.
12. On the Summary screen, the summary and verify that the details provided are accurate. Click **Create** to start the schema creation process.
13. On the Completion summary screen, verify that the schemas were created.

    Click **Close** to exit.

7.7 Validating the Oracle Identity Management Database Installation

To verify if the Oracle Identity Management database installation has been completed successfully, check the following:

- The database is up and running on all nodes.
- The database listener is up and running.
- The database installation includes the required components.
- Use SQL*Plus or another tool to check that the system user is able to connect to the database remotely.
- Run `opatch -lsinventory` on the database to verify that patches have been applied according to the document for the specific platform.
- Manual patch Post-Installation steps have been performed for all the patches.
- The password policy has been defined and the passwords defined for the Oracle Identity Management database schemas are in line with the policy.

7.8 What to Do Next

When you have completed the Oracle Identity Management database installation, see Chapter 8 for complete information to install the Oracle Fusion Applications transaction database.

8

Installing Oracle Fusion Applications Transaction Database

This chapter describes how to install and configure a transaction database for use with an Oracle Fusion Applications environment. It also describes the Oracle Fusion Applications Repository Creation Utility (Oracle Fusion Applications RCU), which creates a repository for applications schemas and tablespaces and loads seed data into the database.

This chapter includes the following sections:

8.1 Introduction to Installing Oracle Fusion Applications Transaction Databases

A **transaction database** holds the business transactions generated as you use your Oracle Fusion Applications products offerings. This chapter includes overview information related to installing Oracle Database. The Provisioning Wizard installs 11.2.0.3 database. If you manually install the database, you must install Oracle Database 11.2.0.3.

Note: To provision Oracle Fusion Applications for 11*g* Release 8 (11.1.8), you must use Oracle Database 11.2.0.3. This release of Oracle Fusion Applications is certified with Oracle Database 11.2.0.4.0 and Oracle Real Application Clusters 11.2.0.4.0.

You can upgrade the database to 11.2.0.4 after provisioning the Oracle Fusion Applications environment.

8.1.1 Process Overview

You must install Oracle Database Enterprise Edition on a physical host before you create a response file. The database must be created using the database template that is shipped with Oracle Fusion Applications software. The template contains the database structure and features, but is not seeded. It is generic for use across platforms.

For a small-scale, single-node database, you can use the **Install an Applications Transaction Database** option in the Provisioning Wizard to install a single-node instance of Oracle Database Enterprise Edition. Or, you can install the database manually (interactively) if you are creating a production-scale, multiple-node database. Oracle Fusion Applications also supports Oracle Real Application Clusters (Oracle RAC).

To finish any database installation, you must use the Oracle Fusion Applications RCU to perform the following actions:

- Create Oracle Fusion Middleware schema and tablespace users and define the tables, views, and other artifacts that the schema user owns.
- Create empty tablespaces for Oracle Fusion Applications components and the schema owners. The owners do not own any tables or data initially.
- Import default seed data values for the schema users using Oracle Data Pump files.

See Section 8.6, "Running the Oracle Fusion Applications RCU to Create Oracle Fusion Applications Database Objects" for details about running the Oracle Fusion Applications RCU.

8.1.2 Oracle Data Pump

Oracle Data Pump provides high-speed, parallel, bulk data and metadata movement of Oracle Database contents. The Data Pump dump files (.dmp) that contain the table definitions are delivered as part of the provisioning framework installation to make them available to the Oracle Fusion Applications RCU.

When using Oracle Data Pump to import data and metadata for an Oracle RAC installation, note that the directory that holds the dump files must be accessible from all Oracle RAC nodes. In addition, keep the following considerations in mind:

- To use Data Pump or external tables in an Oracle RAC configuration, you must ensure that the directory object path is on a cluster-wide file system.

  The directory object must point to shared physical storage that is visible to, and accessible from, all instances where Data Pump and/or external table processes may run.
- The default Data Pump behavior is that worker processes can run on any instance in an Oracle RAC configuration. Therefore, workers on those Oracle RAC instances must have physical access to the location defined by the directory object, such as shared storage media.
- Under certain circumstances, Data Pump uses parallel query slaves to load or unload data. In an Oracle RAC environment, Data Pump does not control where these slaves run, and they may run on other instances in the Oracle RAC, regardless of what is specified for `CLUSTER` and `SERVICE_NAME` for the Data Pump job. Controls for parallel query operations are independent of Data Pump. When parallel query slaves run on other instances as part of a Data Pump job, they also require access to the physical storage of the dump file set.

8.1.3 Single-Node Versus Multiple-Node Databases

A single-node instance of Oracle Database Enterprise Edition is typically used for medium-sized installations, or for training and demonstrations. The Provisioning Wizard database installation interview collects details such as the database listener port and the location of the database home, the database software, the database files, the database password, and the global name of the database. The wizard performs prerequisite validation checks, reports the status of the checks, and summarizes the actions to be performed during the database installation.

Oracle Real Application Clusters (Oracle RAC) enables multiple database instances, linked by an interconnect, to share access to Oracle Database. This configuration enables you to increase the scale of your applications environment. This type of database is typically used for production environments.

For information about Oracle RAC, see "Oracle RAC Database Configuration for Oracle Fusion Applications Repositories" in *Oracle Fusion Applications Administrator's Guide*.

8.2 Oracle Fusion Applications Transaction Database Requirements

This section describes the requirements for Oracle Fusion Applications transaction databases.

8.2.1 Prerequisites for Database Installation

You must read and understand the information in the following sections and perform any tasks outlined there before you begin a database installation.

8.2.1.1 General Oracle Database Prerequisites

General Oracle database prerequisites must be satisfied before you can proceed with the database installation for Oracle Fusion Applications. See the Oracle Database Installation Guide for the required prerequisites and pre-installation tasks. Use the guide that corresponds to the platform you will be running the database on http://www.oracle.com/pls/db112/portal.portal_db?selected=11.

8.2.1.2 Specific Oracle Fusion Applications Prerequisites

The following prerequisites are specific to Oracle Fusion Applications:

- You must have created the provisioning repository, see Section 5.5, "Creating the Oracle Fusion Applications Provisioning Repository".
- You should not share the same database instance for Oracle Identity Management and Oracle Fusion Applications. Oracle Fusion Applications should be in a separate database instance.
- The database instance must also be running on a physical host.
- Even if performing a manual database installation, you must install the Oracle Fusion Applications provisioning framework (see Section 6.3, "Installing the Oracle Fusion Applications Provisioning Framework") to obtain the DBCA template needed for the database creation.
- If performing a manual install, the appropriate DBCA template from the Provisioning Framework must be copied to the database host.
- Ensure there is enough free disk space for Oracle Fusion Applications database tablespaces.

- Designate a Linux or Windows server for the Oracle Fusion Applications RCU if installing Oracle Fusion Applications on another platform.

  The Oracle Fusion Applications RCU is supported only on Linux x86-64 and Microsoft Windows x64 (64-bit) platforms. However it can run from any host that can access the database, it does not have to run from the database server itself. So if the database is installed on other platforms, you must start the Oracle Fusion Applications RCU from the supported Linux x86-64 and Microsoft Windows x64 (64-bit) platforms to connect to your database.

- Download database software and patches separately if the database platform is different from the Fusion Applications platform.

  If the database platform is different from the platform Oracle Fusion Applications and Oracle Identity Management will be running on, the Provisioning Framework and the Oracle Database installer and patches that ship as part of the Oracle Fusion Applications installers cannot be used and it is recommended to download the Oracle Database software and patches for that specific platform and perform the database install manually.

8.2.2 Oracle Fusion Applications Database Requirements

You must read and understand the information in the following sections and perform any tasks outlined there during or after a database installation, before running the Oracle Fusion Applications RCU.

For more information about database installation requirements, see the "Certification" section in the *Oracle Fusion Applications release notes*. The Provisioning Wizard performs prerequisite validation checks to ensure that those requirements are met.

Note: Before you install Oracle database using the Oracle Fusion Applications Provisioning Wizard, you must shut down all Oracle and Oracle-related services on the database host. Failure to do so will result in database installation errors.

8.2.2.1 Components

Oracle Fusion Applications requires Oracle Database Enterprise Edition or Oracle Real Application Clusters Database. If you are installing Oracle Database Enterprise Edition installer manually (not using the provisioning Wizard), the installation requires the enabling of specific components, several of which are selected by default:

- Oracle Partitioning (default)
- Oracle Data Mining RDBMS Files (default)

To verify that your system meets all minimum requirements associated with the database, see *Oracle Database Installation Guide* for your platform for details.

8.2.2.2 Minimum Configuration Parameters for Oracle Database

Table 8–1 shows the commonly recommended initialization parameters.

Table 8–1 Recommended Initialization Parameters

Expected Database Size	Parameter Name	DB Default Value	Recommended Value for Oracle Fusion Applications
Small and large	`audit_trail`	DB	NONE

Table 8–1 (Cont.) Recommended Initialization Parameters

Expected Database Size	Parameter Name	DB Default Value	Recommended Value for Oracle Fusion Applications
	plsql_code_type	INTERPRETED	NATIVE
	nls_sort	Derived from NLS_LANGUAGE	BINARY
	`open_cursors`	50	500
	`session_cached_cursors`	50	500
	`_b_tree_bitmap_plans`	TRUE	FALSE
	db_securefile	PERMITTED	ALWAYS
	disk_asynch_io	TRUE	TRUE
	filesystemio_options	Platform Dependent ("none" for Linux)	Use default value ("none" for Linux)
	Note: When you use the Provisioning Wizard to install the database using the dbca template, the default values for the disk_asynch_io and filesystemio_options parameters are as follows: disk_asynch_io is set to TRUE filesystemio_options will be set to the default value based on the platform where the database is installed. It could be either "none", "setall", "asynch", or "diskio". To verify that the filesystemio_options parameter is using the default value, run the following query: "`select isdefault from v$parameter where name='filesystemio_options`". If it returns TRUE, the default value is set. If you change the parameter value from the original default value to another value and then change it back to the original default value, the default value will still remain FALSE. The following Warning messages will be displayed based on the values set: If disk_asynch_io is set to FALSE and filesystemio_options is set to the default value, a Warning message will be displayed recommending setting the value for disk_asynch_io to TRUE. If disk_asynch_io is set to FALSE and filesystemio_options is not set to the default value, a Warning message will be displayed recommending setting the value for disk_asynch_io to TRUE for the best performance optimization.		
	SYSTEM	1900	1900
	SYSAUX	1100	1100
Starter - Single-node, small	`sga_target`	0	9 GB
	`pga_aggregate_target`	0	4 GB
	_fix_control	5483301:ON,6708183:OFF	5483301:OFF,6708183:ON
	processes	100	5000
	undo tablespace	0	6 GB; autoextend ON
	temp tablespace	0	6 GB; autoextend ON
	redo log	0	Three 2 GB Groups
	SYSTEM	1900	1900
	SYSAUX	1100	1100
	_ACTIVE_SESSION_LEGACY_BEHAVIOR	FALSE	TRUE
Single-node, large	`sga_target`	0	18 GB

Table 8–1 (Cont.) Recommended Initialization Parameters

Expected Database Size	Parameter Name	DB Default Value	Recommended Value for Oracle Fusion Applications
	pga_aggregate_target	0	8 GB
	_fix_control	5483301:ON,6708183:OFF	5483301:OFF,6708183:ON
	processes	100	5000
	undo tablespace	0	12 GB; autoextend ON
	temp tablespace	0	9 GB; autoextend ON
	redo log	0	Three 2 GB Groups
	SYSTEM	1900	1900
	SYSAUX	1100	1100
	_ACTIVE_SESSION_ LEGACY_BEHAVIOR	FALSE	TRUE
2-node Oracle RAC, large	sga_target	0	18 GB
	pga_aggregate_target	0	8 GB
	_fix_control	5483301:ON,6708183:OFF	5483301:OFF,6708183:ON
	processes	100	5000
	undo tablespace	0	12 GB; autoextend ON
	temp tablespace	0	9 GB; autoextend ON
	redo log	0	Three 2 GB Groups per instance
	SYSTEM	1900	1900
	SYSAUX	1100	1100
	_ACTIVE_SESSION_ LEGACY_BEHAVIOR	FALSE	TRUE

For more information about setting the kernel parameter value, see Section 5.3.2.6.

8.2.2.3 Tuning Oracle Database

For more information about tuning Oracle database, see "Chapter 3, Tuning the Database" in the *Oracle Fusion Applications Performance and Tuning Guide*.

8.2.2.4 Mandatory Oracle Database Patches

Table 8–2 lists the mandatory Oracle Database (Enterprise Edition and RAC) patches required for Oracle Fusion Applications. The list is organized by operating system platforms. Patches listed as **generic** are required for all operating system platforms. For each platform, there is one patch for Opatch, one patch for Patch Set Updates (PSU), and zero or many one-off patches.

- If you install Oracle Database using the Provisioning Wizard, these patches are automatically applied.
- If you install Oracle Database manually, you must apply the mandatory database patches by following the instructions detailed in Section 8.4.2.5.

Note: For both scenarios described above, ensure that you complete the following steps before running the Oracle Fusion Applications RCU:

- Complete the manual postinstallation tasks detailed in the patch readme file (Section 8.4.1.5).
- Refer to Oracle Database patch details listed in the "Additional Patches for the Tech Stack" section of the latest Oracle Fusion Applications release notes for any additional patches required for the current release.

Table 8–2 Mandatory Oracle Database Patches

Operating System	Patches
generic	One-off patches: p12317925_112030_Generic.zip p13470616_112030_Generic.zip p13498243_112030_Generic.zip p13508115_112030_Generic.zip p13992953_112030_Generic.zip p14698700_112030_Generic.zip p14802958_112030_Generic.zip p16287905_112030_Generic.zip p16763016_112030_Generic.zip

Table 8–2 (Cont.) Mandatory Oracle Database Patches

Operating System	Patches
aix	Opatch: p6880880_112000_AIX64-5L.zip DBPSU6: p16056266_112030_AIX64-5L.zip One-off patches: p10255235_112030_AIX64-5L.zip p11837095_112030_AIX64-5L.zip p12621588_112036_AIX64-5L.zip p12646746_112030_AIX64-5L.zip p12738119_112036_AIX64-5L.zip p12772404_112036_AIX64-5L.zip p12889054_112030_AIX64-5L.zip p12977501_112030_AIX64-5L.zip p12985184_112030_AIX64-5L.zip p13014128_112030_AIX64-5L.zip p13078786_112030_AIX64-5L.zip p13365700_112030_AIX64-5L.zip p13404129_112030_AIX64-5L.zip p13429702_112030_AIX64-5L.zip p13615767_112030_AIX64-5L.zip p13632653_112030_AIX64-5L.zip p13741583_112036_AIX64-5L.zip p13743987_112030_AIX64-5L.zip p13790109_112030_AIX64-5L.zip p13863932_112036_AIX64-5L.zip p13902963_112036_AIX64-5L.zip p13918644_112030_AIX64-5L.zip p13989379_112030_AIX64-5L.zip p14015403_112036_AIX64-5L.zip p14029429_112030_AIX64-5L.zip p14058884_112030_AIX64-5L.zip p14143796_112030_AIX64-5L.zip p14153464_112030_AIX64-5L.zip p14164849_112030_AIX64-5L.zip p14207317_112036_AIX64-5L.zip p14343501_112030_AIX64-5L.zip p14499293_112030_AIX64-5L.zip p14555370_112036_AIX64-5L.zip p14571027_112030_AIX64-5L.zip p14653598_112036_AIX64-5L.zip p14679292_112030_AIX64-5L.zip p14808639_112036_AIX64-5L.zip p16099033_112030_AIX64-5L.zip p16196536_112036_AIX64-5L.zip p16423432_112030_AIX64-5L.zip p16780710_112036_AIX64-5L.zip

Table 8–2 (Cont.) Mandatory Oracle Database Patches

Operating System	Patches
linux64	OPatch: p6880880_112000_Linux-x86-64.zip DBPSU6: p16056266_112030_Linux-x86-64.zip One-off patches: p10255235_112030_Linux-x86-64.zip p11837095_112030_Linux-x86-64.zip p12621588_112036_Linux-x86-64.zip p12646746_112030_Linux-x86-64.zip p12738119_112036_Linux-x86-64.zip p12772404_112036_Linux-x86-64.zip p12889054_112030_Linux-x86-64.zip p12977501_112030_Linux-x86-64.zip p12985184_112030_Linux-x86-64.zip p13014128_112030_Linux-x86-64.zip p13078786_112030_Linux-x86-64.zip p13365700_112030_Linux-x86-64.zip p13404129_112030_Linux-x86-64.zip p13429702_112030_Linux-x86-64.zip p13615767_112030_Linux-x86-64.zip p13632653_112030_Linux-x86-64.zip p13741583_112036_Linux-x86-64.zip p13743987_112030_Linux-x86-64.zip p13790109_112030_Linux-x86-64.zip p13863932_112036_Linux-x86-64.zip p13902963_112036_Linux-x86-64.zip p13918644_112030_Linux-x86-64.zip p13989379_112030_Linux-x86-64.zip p14015403_112036_Linux-x86-64.zip p14029429_112030_Linux-x86-64.zip p14058884_112030_Linux-x86-64.zip p14143796_112030_Linux-x86-64.zip p14153464_112030_Linux-x86-64.zip p14164849_112030_Linux-x86-64.zip p14207317_112036_Linux-x86-64.zip p14343501_112030_Linux-x86-64.zip p14499293_112030_Linux-x86-64.zip p14555370_112036_Linux-x86-64.zip p14571027_112030_Linux-x86-64.zip p14653598_112036_Linux-x86-64.zip p14679292_112030_Linux-x86-64.zip p14808639_112036_Linux-x86-64.zip p16099033_112030_Linux-x86-64.zip p16196536_112036_Linux-x86-64.zip p16423432_112030_Linux-x86-64.zip p16780710_112036_Linux-x86-64.zip

Table 8–2 (Cont.) Mandatory Oracle Database Patches

Operating System	Patches
solaris64	OPatch: p6880880_112000_Solaris86-64.zip DBPSU6: p16056266_112030_Solaris86-64.zip One-off patches: p10255235_112030_Solaris86-64.zip p11837095_112030_Solaris86-64.zip p12621588_112036_Solaris86-64.zip p12646746_112030_Solaris86-64.zip p12738119_112036_Solaris86-64.zip p12772404_112036_Solaris86-64.zip p12889054_112030_Solaris86-64.zip p12977501_112030_Solaris86-64.zip p12985184_112030_Solaris86-64.zip p13014128_112030_Solaris86-64.zip p13078786_112030_Solaris86-64.zip p13365700_112030_Solaris86-64.zip p13404129_112030_Solaris86-64.zip p13429702_112030_Solaris86-64.zip p13615767_112030_Solaris86-64.zip p13632653_112030_Solaris86-64.zip p13741583_112036_Solaris86-64.zip p13743987_112030_Solaris86-64.zip p13790109_112030_Solaris86-64.zip p13863932_112036_Solaris86-64.zip p13902963_112036_Solaris86-64.zip p13918644_112030_Solaris86-64.zip p13989379_112030_Solaris86-64.zip p14015403_112036_Solaris86-64.zip p14029429_112030_Solaris86-64.zip p14058884_112030_Solaris86-64.zip p14143796_112030_Solaris86-64.zip p14153464_112030_Solaris86-64.zip p14164849_112030_Solaris86-64.zip p14207317_112036_Solaris86-64.zip p14343501_112030_Solaris86-64.zip p14499293_112030_Solaris86-64.zip p14555370_112036_Solaris86-64.zip p14571027_112030_Solaris86-64.zip p14653598_112036_Solaris86-64.zip p14679292_112030_Solaris86-64.zip p14808639_112036_Solaris86-64.zip p16099033_112030_Solaris86-64.zip p16196536_112036_Solaris86-64.zip p16423432_112030_Solaris86-64.zip p16780710_112036_Solaris86-64.zip

Table 8–2 (Cont.) Mandatory Oracle Database Patches

Operating System	Patches
solaris_sparc64	OPatch: p6880880_112000_SOLARIS64.zip DBPSU6: p16056266_112030_SOLARIS64.zip One-off patches: p10255235_112030_SOLARIS64.zip p11837095_112030_SOLARIS64.zip p12621588_112036_SOLARIS64.zip p12646746_112030_SOLARIS64.zip p12738119_112036_SOLARIS64.zip p12772404_112036_SOLARIS64.zip p12889054_112030_SOLARIS64.zip p12977501_112030_SOLARIS64.zip p12985184_112030_SOLARIS64.zip p13014128_112030_SOLARIS64.zip p13078786_112030_SOLARIS64.zip p13365700_112030_SOLARIS64.zip p13404129_112030_SOLARIS64.zip p13429702_112030_SOLARIS64.zip p13615767_112030_SOLARIS64.zip p13632653_112030_SOLARIS64.zip p13741583_112036_SOLARIS64.zip p13743987_112030_SOLARIS64.zip p13790109_112030_SOLARIS64.zip p13863932_112036_SOLARIS64.zip p13902963_112036_SOLARIS64.zip p13918644_112030_SOLARIS64.zip p13989379_112030_SOLARIS64.zip p14015403_112036_SOLARIS64.zip p14029429_112030_SOLARIS64.zip p14058884_112030_SOLARIS64.zip p14143796_112030_SOLARIS64.zip p14153464_112030_SOLARIS64.zip p14164849_112030_SOLARIS64.zip p14207317_112036_SOLARIS64.zip p14343501_112030_SOLARIS64.zip p14499293_112030_SOLARIS64.zip p14555370_112036_SOLARIS64.zip p14571027_112030_SOLARIS64.zip p14653598_112036_SOLARIS64.zip p14679292_112030_SOLARIS64.zip p14808639_112036_SOLARIS64.zip p16099033_112030_SOLARIS64.zip p16196536_112036_SOLARIS64.zip p16423432_112030_SOLARIS64.zip p16780710_112036_SOLARIS64.zip

Table 8–2 (Cont.) Mandatory Oracle Database Patches

Operating System	Patches
windows64	OPatch: p6880880_112000_MSWIN-x86-64.zip windows64 BP24 (under psu/ directory): p17327041_112030_MSWIN-x86-64.zip

8.2.2.5 DBA Directories

Create directories in the file system accessible by the database which will be referenced by the DBA directories used by Oracle Fusion Applications. These directories are specified in the *Oracle Fusion Applications Installation Workbook* - Database tab -> FA transaction Database table and they are:

- `RCU APPLCP_FILE_DIR`
- `RCU APPLLOG_DIR`
- `RCU FUSIONAPPS_PROV_RECOVERY_DIR` (OBIEE Backup Dir)
- `RCU OTBI_DBINSTALL_DUMP_DIR` (OTBI Dump File Directory)
- `RCU FUSIONAPPS_DBINSTALL_DP_DIR` (FA Dump File Directory)

For more information about the specific requirements for these directories, see Section 4.4.2.4, "Oracle Fusion Applications RCU Directories".

8.2.2.6 Make Oracle Fusion Applications RCU Software Available on the Host where it is Run

Complete the following steps to make the Oracle Fusion Applications software available in the host where it is run.

- Locate the appropriate Oracle Fusion Applications RCU software for your platform. For Linux, go to *`REPOSITORY_LOCATION`*`/installers/apps_rcu/linux` to find the rcuHome_fusionapps_linux.zip file. For Windows, go to *`REPOSITORY_LOCATION`*`/installers/apps_rcu/windows` and locate the `rcuHome_fusionapps_win.zip` file. These files were staged when you created the installer repository.
- Extract the contents of rcuHome_fusionapps_linux.zip (or `rcuHome_fusionapps_win.zip`) to a directory (`APPS_RCU_HOME`) on a Windows or Linux machine where you run the Oracle Fusion Applications RCU. All dependent components that the Oracle Fusion Applications RCU needs are included in this zipped file.

8.2.2.7 Make dmp Files Available on the Database Server

Complete the following steps to make dmp files available on the database server.

- Locate the file *`APPS_RCU_HOME`*`/rcu/integration/fusionapps/export_fusionapps_dbinstall.zip`.
- Unzip `export_fusionapps_dbinstall.zip` to the directory you specified for `FUSIONAPPS_DBINSTALL_DP_DIR`.
- Go to *`APPS_RCU_HOME`*`/rcu/integration/biapps/schema` and locate the `otbi.dmp` file.
- Copy `otbi.dmp` to `OTBI_DBINSTALL_DUMP_DIR`.

8.3 Oracle Fusion Applications Database Installation Checklist

Before initiating the Oracle Fusion Applications database installation process, verify the following checklist:

- Necessary infrastructure
  - Access to the database server console is provided for the database OS user as well as root/pseudo access (VNC recommended).
  - The provisioning repository or Oracle database installers are available and accessible from the database nodes.
  - Database patches are available and accessible from the database nodes.
  - The Oracle Fusion Applications Provisioning Framework has been installed.
  - (Wizard Install only) The Oracle Fusion Applications Provisioning Wizard can be run from the database host.
  - (Manual Install only) The appropriate DBCA template from the Provisioning Framework has been copied to the database host.
- Prerequisites for the database server
  - General Oracle database prerequisites have been satisfied.
- Planning
  - *Oracle Fusion Applications Installation Workbook* - Databases tab -> FA Transactional Database table has been filled out with information that will be used for the database installation.

8.4 Installing the Oracle Fusion Applications Transaction Database

You install the Oracle Fusion Applications transaction database using the provisioning wizard or manually as described in this section.

- Installing Oracle Database Enterprise Edition with the Wizard
- Manually Installing Oracle Database Enterprise Edition or Oracle RAC

8.4.1 Installing Oracle Database Enterprise Edition with the Wizard

As a part of the provisioning process, the Provisioning Wizard performs prerequisite and validation checks. These validations must pass before you create a response file.

User Input Validations

The Provisioning Wizard:

- Validates the service name or global database name.
- Validates the installer location. In the Preverify phase, validates that the database is present.
- Validates that the database password value and the password confirmation match.
- Performs specific user ID and password validations for all Oracle Fusion Middleware schema owners.

Preinstallation Validations

The Provisioning Wizard:

- Checks to see if the specified database file location has sufficient disk space for the initial database provisioning and performs an Oracle home space check.
- Performs a port availability check.
- Performs a platform check. There is no validation that specific platform packages have been installed.

Postinstallation Validations

The Provisioning Wizard ensures that a JDBC connection can be established.

You can install a single-node instance of Oracle Database Enterprise Edition using the Provisioning Wizard. The wizard uses the database template delivered with your software. The database is initially empty. After the installation is complete, the Provisioning Wizard has applied the required database patches for Oracle Fusion Applications automatically, however, you must run any manual postinstallation tasks that are required by the database patches as described in the patch's readme files, then run the Oracle Fusion Applications RCU to create schemas and tablespaces. For more information about manual postinstallation tasks, see Section 8.4.1.5, "Complete Database Patch Postinstallation Tasks".

The wizard invokes the database build script and performs the following tasks:

- Installs database software.
- Generates an Oracle Universal Installer (OUI) response file based on the configuration that you specify.
- Accesses the provisioning repository and invokes the database installer in silent mode. If the applications environment does not meet the database installation requirements, the wizard terminates the process.
- Requests a copy of the nonseeded database template.
- Creates an instance of Oracle Database 11.2.0.3 using the configuration settings that you entered in the wizard interview, and the database template.

8.4.1.1 Start the Provisioning Wizard

Note the following requirement when installing a transaction database on a UNIX platform:

- Verify that the length of the PATH environment variable is less than 900 characters. Use this command to check the character count:

```
env | grep ^PATH= | wc -m
```

To start the Provisioning Wizard, do the following:

1. Set the *JAVA_HOME* environment variable to point to the JDK location in the provisioning repository, for example:

   UNIX:

   ```
   export JAVA_HOME=REPOSITORY_LOCATION/jdk6
   ```

   > **Tip:** For the *REPOSITORY_LOCATION* value, see *Oracle Fusion Applications Installation Workbook* - Storage tab -> Temporary Shared Storage -> Installers Directory Location.

   ```
   export PATH=$JAVA_HOME/bin:$PATH
   ```

   AIX:

```
export JAVA_HOME=REPOSITORY_LOCATION/jdk6
export PATH=$JAVA_HOME/bin:$PATH
export SKIP_ROOTPRE=TRUE
```

Windows:

```
set JAVA_HOME=REPOSITORY_LOCATION\jdk6
set PATH=%JAVA_HOME%\bin;%PATH%
```

2. Verify that the `LIBPATH` value is null.
3. Run the following command on the machine where you want the database to reside:

   UNIX:

   > **Tip:** For the *FAPROV_HOME* value, see *Oracle Fusion Applications Installation Workbook* - Storage tab -> Install Directories ->FA Provisioning Framework Location.

   ```
   cd FAPROV_HOME/provisioning/bin
   ./provisioningWizard.sh
   ```

   On Solaris, use `bash provisioningWizard.sh` instead of `./provisioningWizard.sh`.

   Windows:

   ```
   FAPROV_HOME\provisioning\bin
   provisioningWizard.bat
   ```

   > **Note:** Ensure that provisioning on Microsoft Windows platforms is performed from a Run as Administrator console. By default, the command prompt has the necessary privilege set. If not, you can run the Run as Administrator option by right clicking the Command Prompt from the Start menu.

8.4.1.2 Wizard Interview Screens and Instructions

Table 8–3 shows the steps necessary to install a transaction database. For help with any of the interview screens, see or click **Help** on any interview screen.

> **Note:** If you do not input the correct values required, the error and warning messages are displayed at the bottom of the screen.

Table 8–3 Interview Flow for Database Installation

Screen	Description and Action Required
Welcome	No action is required on this read-only screen. Click **Next** to continue.
Specify Central Inventory Directory	This screen displays only if one or more of the following conditions are not met: ■ The `-invPtrLoc` option is used to specify the central inventory location on non-Windows platforms, so the default value for your platform is not used. Note that the default for Linux and AIX platforms is `/etc/oraInst.loc` and for Solaris, it is `/var/opt/oracle/oraInst.loc`. ■ The Central Inventory Pointer File is readable. ■ The Central Inventory Pointer File contains a value for `inventory_loc`. ■ The `inventory_loc` directory is writable. ■ The `inventory_loc` directory has at least 150K of space. ■ `inventory_loc` is not a file. Specify the location of the **Central Inventory Directory** that meets the previous criteria. The `inventory_loc` directory can be created by the `createCentralInventory.sh` script and does not have to exist at the time you specify its location. **Tip: This value is available in the** *Oracle Fusion Applications Installation Workbook* - **Storage tab -> Inventories -> FA Provisioning Framework**. For non-Windows platforms, in the **Operating System Group ID** field, select or enter the group whose members will be granted access to the inventory directory. All members of this group can install products on this host. Click **OK** to continue. **Tip: This value is available in the** *Oracle Fusion Applications Installation Workbook* - **Storage tab -> Shared Storage -> FA Shared -> OS Group Owner**. The **Inventory Location Confirmation** dialog prompts you to run the *`inventory_directory`*`/createCentralInventory.sh` script as root, to confirm that all conditions are met and to create the default inventory location file, such as `/etc/oraInst.loc`. After this script runs successfully, return to the interview and click **OK** to proceed with the installation. If you do not have root access on this host but want to continue with the installation, select **Continue installation with local inventory** and click **OK** to proceed with the installation. For Windows platforms, this screen displays if the inventory directory does not meet requirements. For more information about inventory location files, see "Oracle Universal Installer Inventory" in the *Oracle Universal Installer and OPatch User's Guide*. Click **Next** to continue.
Installation Options	Presents the list of valid installation actions that you can perform using the wizard. Select **Install an Applications Transaction Database**. Click **Next** to continue.

Table 8–3 (Cont.) Interview Flow for Database Installation

Screen	Description and Action Required
Specify Security Updates	Set up a notification preference for security-related updates and installation-related information from My Oracle Support. ▪ **Email**: Enter your email address to have updates sent by this method. ▪ **I wish to receive security updates via My Oracle Support**: Select this option to have updates sent directly to your My Oracle Support account. You must enter your **My Oracle Support Password** if you select this option. **Note:** If you provide invalid My Oracle Support (MOS) credentials, a dialog box is displayed informing that you will be anonymously registered. You must complete the following steps before you continue with provisioning the new environment: 1. Cancel and exit the Provisioning Wizard. 2. Obtain the correct MOS credentials. 3. Restart the Provisioning Wizard to update the provisioning response file with the correct MOS credentials or uncheck the checkbox next to **I wish to receive security updates via My Oracle Support**. Save the provisioning response file and then exit the Provisioning Wizard. 4. Restart the Provisioning Wizard to provision the Oracle Fusion Applications environment. Click **Next** to continue.
Database Install Configuration	Specify the configuration details for the database that you want to install. See Section 8.4.1.3 for details. Click **Next** to continue.
Prerequisite Checks	The **Prerequisite Checks** list shows each prerequisite check performed, and its status: ▪ **Block**: Processing has not yet started on this host for the named phase. ▪ **Clock**: Performing the build for a phase. ▪ **Check mark**: The build was completed successfully. ▪ **x** mark: The build has failed for this phase. You must correct the errors before you can continue. ▪ **Restricted** symbol: The validation process has stopped due to a failure within another process. Click an **x** or a **Restricted** symbol to display information about failures. Click the **Log** file for details about the validation. Fix any issues reported. Click **Retry** to run the prerequisite checks again. If recovery is necessary, see Section 9.3 for details. When prerequisite checking has finished with no errors, click **Next** to continue.
Summary	Click **Save** to create and save a text file to use as a record of this configuration. Click **Install** to start the installation. **Note**: Record the name and location of the file. You must supply these details when you create a response file.
Database Installation Progress	The progress of the installation phases is listed. A message appears after the installation phase is complete directing you to run `root.sh`. Follow this instruction and click **OK** to continue the installation. The central log file location is displayed below the **Progress** bar. Click a Log icon to view phase log files. Click **Retry** if a failure occurs. If recovery is necessary, see Section 9.3 for details. Click **Next** to continue.
Installation Complete	Summarizes the actions and validations that were performed for this installation. Click **Save** to record the database summary information in a text file. **Note**: Be sure to make a note of the name and location of this file. You must supply these details when you create a response file. Your system administrator may also need this information as they perform maintenance tasks. Click **Close** to dismiss the screen and exit the wizard.

8.4.1.3 Database Installation Parameters

On the **Database Install Configuration** interview screen, specify values for these database configuration parameters.

- **Database Listener Port**: The port number designated for the database server. The default port for Oracle Database is 1521.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> FA Transactional Database -> FA DB Instances.

- **Installers Directory Location**: Enter the path to the `REPOSITORY_LOCATION` directory you created when you downloaded the provisioning repository. For Windows, the location must be a symbolically linked directory. See Section 5.3.2.21 for additional details. Note that the symbolic link is not necessary if the repository and the database are on the same node.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Storage tab -> Temporary Shared Storage -> Installers Directory Location.

- **Oracle Base**: Enter the top-level directory for Oracle software installations. You can change the path based on your requirements.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> FA Transactional Database -> FA DB Oracle Home (The ORACLE_BASE is part of the ORACLE_HOME).

- **Software Location**: Accept the default value or enter the Oracle home directory path that points to where you want the data files to reside. The directory path must not contain spaces.

  Tip: This field will be automatically filled. This value is available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> FA Transactional Database -> FA DB Oracle Home.

- **Database File Location**: Accept the default value or enter the path to the .dbf, .dtl, and .log files.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> FA Transactional Database -> FA DB Datafiles Location.

- **OSDBA Group**: The UNIX operating system group that the database administrator is a member of. Displayed only if the platform detected by the installer is UNIX.

  Tip: If the database is installed on the FA shared storage as defined in the *Oracle Fusion Applications Installation Workbook*, use the value available in the Storage tab -> Shared Storage -> FA Shared -> OS Group Owner.

- **Global Database Name**: Enter a name to distinguish this database instance from other Oracle Database instances running on the same host. The name can be written as *database name* or *database name.domain name*. This is the database service name.

Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> FA Transactional Database -> FA DB Service Name.

- **Administrative Password**: Specify a valid password. Retype the password to **Confirm**.

8.4.1.4 Validate the catbundle.sql Script

After the database installation, review the following log file to validate that the `catbundle.sql` script has completed successfully:
`<ORACLE_HOME>/tpu/DB_YYYY-MM-DD_HH-MM-SS/db_server_bundle/techpatch/fatechpatch_YYYY-MM-DD_HH-MM-SS[AM|PM].log`.

See "Ignorable Errors Reported by catbundle.sql" in the *Oracle Fusion Applications Upgrade Guide* for a list of ignorable errors from the `catbundle.sql` script.

8.4.1.5 Complete Database Patch Postinstallation Tasks

After the database installation, the required database patches are automatically applied and the database is started. However, you must check the patch readme files to determine whether you need to perform postinstallation tasks manually as required by the database patches. Go to the *`REPOSITORY_LOCATION`*`/installers/database/patch` directory to find the readme files. Any manual steps associated with the patches are typically located in a section called "Post-Install Instructions" or "Postinstallation."

You can aggregate all the readme files by running this script, depending on which database version you installed.

```
find REPOSITORY_LOCATION/installers/database/patch/ -name "README.txt" | xargs cat
>> REPOSITORY_LOCATION/PATCHES_README_ALL.txt
```

Use a text editor of your choice to view `PATCHES_README_ALL.txt`.

After running all patch postinstallation tasks, in SQL*Plus, connect to the database instance with SYSDBA administrative privilege, then run the `catmetx.sql` script to ensure that the `PLSQL_CCFLAGS` value for `PACKAGE BODY` is set to true:

```
@?/rdbms/admin/catmetx.sql
```

8.4.2 Manually Installing Oracle Database Enterprise Edition or Oracle RAC

Though Oracle Fusion Applications Provisioning automates the installation and configuration of a transaction database for use with Oracle Fusion Applications environments, you can manually install a single-node instance of Oracle Database or Oracle Real Application Clusters to meet your specific requirements.

To manually install and configure a transaction database, you must complete the following steps:

1. Install Oracle Database or Oracle RAC
2. Configure OCM
3. Configure and Start the Database Listener for Oracle Database (NETCA)
4. Create a Transaction Database Instance Using Oracle Database Configuration Assistant (DBCA)
5. Run RUP Lite for RDBMS

6. Complete Database Patch Postinstallation Tasks

8.4.2.1 Install Oracle Database or Oracle RAC

The first step in creating a custom transaction database instance is to install the database software.

8.4.2.1.1 How to Install Oracle Database If you are installing Oracle Database manually (interactively) instead of using the Provisioning Wizard, see *Oracle Database Installation Guide* for your platform for instructions.

When performing the installation, ensure that the following components are enabled:

- Oracle Partitioning (default)
- Oracle Data Mining RDBMS Files (default)

If these components are not enabled, application functionality will not work.

When performing the installation, choose the **Software Only** option. You will manually create the database instance and configure the database.

To verify that your system meets all minimum requirements associated with the database, see *Oracle Database Installation Guide* for your platform for details.

8.4.2.1.2 How to Install Oracle RAC For complete information about installing and configuring Oracle RAC, see *Oracle Database Installation Guide* for your platform for instructions. This library contains installation guides for Oracle RAC, as well as Oracle Database installations for all platforms.

> **Note:** For a RAC database, the passwords for all schemas must be the same across all RAC instances.

When you install Oracle RAC, note that by default the database listener creates a log file in the grid ORACLE_HOME, that is, GRID_HOME. If the GRID_HOME and database instance owners are different, and if the database listener is started by the database instance operating system user from the GRID_HOME, then you **must** set diagnostic destination for the listener in the `listener.ora` file to avoid any core dump issues in the Web Tier host by adding the following line:

```
ADR_BASE_<name of the LISTENER>=<a file path / location where
the database instance owner has the read/write permission>
```

8.4.2.2 Configure OCM

For more information about configuring OCM, see the *Oracle Configuration Manager Installation and Administration Guide for OCM.*

8.4.2.3 Configure and Start the Database Listener for Oracle Database (NETCA)

- You must configure the database listener as described in the Oracle 11*g* Release 2 Documentation Library.
- After you complete the configuration, start the database listener.

8.4.2.4 Create a Transaction Database Instance Using Oracle Database Configuration Assistant (DBCA)

You can use the Oracle Database Configuration Assistant (DBCA) to create the transaction database from the database template that is shipped with Oracle Fusion

Applications software. This template contains the database structure and features, but is not seeded. It is generic for use across platforms.

Instructions on database installation and configuration can be found in the Oracle 11*g* Release 2 Documentation Library.

If you choose to not use the database template, you must ensure that your database configuration parameters are aligned with the values specified in Section 8.2.2.2.

8.4.2.4.1 How to Create a Single-Node Oracle Database Instance from the Template

You use DBCA to manually create an instance of Oracle Database from the nonseeded database template that is shipped with Oracle Fusion Applications software.

To create a single-node Oracle Database instance:

1. Review and edit the nonseeded database template at *FAPROV_HOME*`/provisioning/template/dbca/empty_database_11.2.dbt` or `empty_database_11.2.large.dbt` (for a large database instance).
2. Navigate to the database *ORACLE_HOME*`/bin` directory and execute the following command. Make appropriate changes based on the selected database template.

```
dbca -silent -createDatabase -templateName\
FAPROV_HOME/provisioning/template/dbca/empty_database_11.2.large.dbt  \
-gdbName "ORACLE_SID" \
-sid "ORACLE_SID" \
-sysPassword "SYS_PASSWORD" \
-systemPassword "SYSTEM_PASSWORD" \
-emConfiguration "NONE" \
-characterSet "AL32UTF8" - \
-nationalCharacterSet "AL16UTF16" \
-variables ORACLE_BASE=ORACLE_BASE, ORACLE_HOME=ORACLE_HOME \
-initParams audit_trail=NONE \
-datafileDestination DATAFILE_LOC
```

Replace the following variables with the appropriate values:

- *FAPROV_HOME*: Home of Oracle Fusion Applications Provisioning framework.
- *ORACLE_SID*: Global database name of the Oracle Fusion Applications database.
- *SYS_PASSWORD*: Password for the SYS user. The SYS schema is the location of base tables and views.
- *SYSTEM_PASSWORD*: User SYSTEM password. The user can create additional tables and views.
- *ORACLE_BASE*: Top-level directory for the database installation.
- *ORACLE_HOME*: Oracle home of the database installation.
- *DATAFILE_LOC*: Physical location of the files that store the data of all logical structures in the database.

8.4.2.4.2 How to Create an Oracle RAC Database Instance from the Template

You use DBCA to manually create a database instance for each Oracle RAC node using the nonseeded database template that is shipped with Oracle Fusion Applications software.

To create an Oracle RAC database instance:

1. Review and edit the nonseeded database template at *FAPROV_HOME*/provisioning/template/dbca/empty_database_11.2.dbt or empty_database_11.2.large.dbt (for a large database instance).
2. For each RAC node, navigate to the database *ORACLE_HOME*/bin directory of the RAC node and execute the following command. Make appropriate changes based on the selected database template.

```
dbca -silent -createDatabase \
-templateName  FAPROV_HOME/provisioning/template/dbca/empty_database_11.2.dbt
\
-gdbName "ORACLE_SID" \
-sid "ORACLE_SID" \
-sysPassword "SYS_PASSWORD" \
-systemPassword "SYSTEM_PASSWORD" \
-emConfiguration "NONE" \
-characterSet "AL32UTF8" - \
-nationalCharacterSet "AL16UTF16" \
-variables ORACLE_BASE=ORACLE_BASE, ORACLE_HOME=ORACLE_HOME \
-initParams audit_trail=NONE \
-datafileDestination DATAFILE_LOC \
-nodeinfo node1,node2
```

   Replace the following variables with the appropriate values:

   - *FAPROV_HOME*: Home of Oracle Fusion Applications Provisioning framework.
   - *ORACLE_SID*: Global database name of the Oracle Fusion Applications database.
   - *SYS_PASSWORD*: Password for the SYS user. The SYS schema is the location of base tables and views.
   - *SYSTEM_PASSWORD*: User SYSTEM password. The user can create additional tables and views.
   - *ORACLE_BASE*: Top-level directory for the database installation.
   - *ORACLE_HOME*: Oracle home of the database installation.
   - *DATAFILE_LOC*: Physical location of the files that store the data of all logical structures in the database.

Note: In the nonseeded database template, the following common attributes required by the Oracle Fusion Applications RCU must be set as follows:

```
<option name="OMS" value="true"/>
<option name="JSERVER" value="true"/>
<option name="SPATIAL" value="true"/>
<option name="IMEDIA" value="true"/>
<option name="XDB_PROTOCOLS" value="true">
<tablespace id="SYSAUX"/>
</option>
<option name="ORACLE_TEXT" value="true">
<tablespace id="SYSAUX"/>
</option>
<option name="SAMPLE_SCHEMA" value="false"/>
<option name="CWMLITE" value="false">
<tablespace id="SYSAUX"/>
</option>
<option name="EM_REPOSITORY" value="true">
<tablespace id="SYSAUX"/>
</option>
<option name="APEX" value="false"/>
<option name="OWB" value="false"/>
<option name="DV" value="false"/>
```

8.4.2.5 Run RUP Lite for RDBMS

For more information, see "Run RUP Lite for RDBMS" in the *Oracle Fusion Applications Upgrade Guide*.

8.4.2.6 Complete Database Patch Postinstallation Tasks

For more information, see Section 8.4.1.5, "Complete Database Patch Postinstallation Tasks".

8.4.3 Validating the Oracle Fusion Applications Database

To verify if the Oracle Fusion Applications database installation has been completed successfully, check the following:

- The database is up and running on all nodes.
- The database listener is up and running.
- The database installation includes the required components.

Validation Task 1: Validating the Database Installation

Verify that the database installation includes the required components.

Prerequisites

The only prerequisite is that the database has been installed according to the instructions in Section 8.4.1, "Installing Oracle Database Enterprise Edition with the Wizard".

How to Validate the Database Installation

Verify that all the required components have been installed.

- Correct version of Enterprise Edition or RAC
- Oracle Partitioning
- Data Mining

Verify that you have correctly installed the components via any of the following methods.

- Run the following query from SQL*Plus:

```
select * from PRODUCT_COMPONENT_VERSION;
```

- Run the following query from SQL*Plus:

```
select COMP_NAME, VERSION, STATUS from dba_registry;
```

- Start SQL*Plus and examine the initial output that lists the installed options.

Expected Results

All components should be present in the installed database directory.

The queries return a list of installed components along with version and status, such as the following:

```
Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, Data Mining
and Real Application Testing options
```

Corrective Actions

Install any missing components.

1. Run the database installation wizard.
2. Make sure to select all the required components.

For more information, see Section 8.4.1, "Installing Oracle Database Enterprise Edition with the Wizard"

- Use SQL* Plus or another tool to check that the system user is able to connect to the database remotely.
- Ensure that the minimum database parameters have been configured.

Validation Task 2: Verifying Database Parameter Configuration

Verify that the minimum database parameters have been configured.

Prerequisites

Make sure you have completed Validation Task 1: Validating the Database Installation.

How to Verify the Configuration of Database Parameters

Review the initialization parameters listed in Section 8–1, " Recommended Initialization Parameters" to those in the installed database. Update any initialization parameters to meet minimum requirements as necessary.

– Login to SQL*Plus using the sys as sysdba identity.

– Run either of the following commands.

To check a parameter value:

```
show parameter <parameter>
```

To update a parameter value:

```
alter system set <parameter> = <value>
```

For example:

```
alter system set processes = 1500 scope = SPFILE
```

Adding the scope directive writes the updated parameter value to the database spfile. Restart the database to enable the change.

Expected Results

All initialization parameters should meet minimum specifications. The initialization parameters are listed in Table 8–1. Check the release notes to see if any parameters have been added.

Corrective Actions

Set initialization parameters to meet minimum requirements as needed.

- Run `opatch -lsinventory` on the database to verify that patches have been applied according to the document for the specific platform.

Validation Task 3: Verifying Database Patching

Verify that all mandatory patches have been applied to the database.

Prerequisites

Make sure you have completed Validation Task 2: Verifying Database Parameter Configuration.

How to Verify Database Patching

Check the database patches that have been installed against the list of patches in Section 8–2, " Mandatory Oracle Database Patches".

– Compare the patch list against the output of opatch lsinventory.

From the database `ORACLE_HOME`, run the command opatch lsinventory to get a list of patches that have been applied to the database. In the following example, `ORACLE_HOME` is set to the database home.

```
$ORACLE_HOME/OPatch/opatch lsinventory
```

The output from this command lists all patches applied to date.

Expected Results

All required patches must be installed, and all patch post-processing tasks must be completed, as described in each individual patch README document. The patch README text or HTML files are located in the top level patch directory after the patch zip file has been unzipped.

Corrective Actions

Apply any patches that may have been overlooked, and confirm that all post-processings tasks have been completed.

- Manual patch post-installation steps have been performed on all patches.
- The password policy has been defined and the passwords defined for the Oracle Fusion Applications database schemas are in line with the policy.
- The file system directories for the DBA directories have been created on the database server and are accessible (read-write) from all database nodes. Specifically, check the directory paths assigned to the directory names `APPLCP_FILE_DIR` and `APPLLOG_DIR` in the `ALL_DIRECTORIES` database table existing in the file system.

8.5 Oracle Fusion Applications RCU Installation Checklist

Before running the Oracle Fusion Applications RCU, verify the following checklist:

- Necessary infrastructure
  - Oracle Fusion Applications database is available and has passed post-install validation.
  - Access to the server console is provided for the OS user (VNC recommended).
- Prerequisites for the host running the Oracle Fusion Applications RCU.
- Planning
  - *Oracle Fusion Applications Installation Workbook* - Databases tab -> FA Database and FA Transactional Database tables have been filled out with information that will be used for the database installation.
  - Passwords have been chosen for the Oracle Fusion Applications schemas.

8.6 Running the Oracle Fusion Applications RCU to Create Oracle Fusion Applications Database Objects

The Oracle Fusion Applications Repository Creation Utility (Oracle Fusion Applications RCU) is a self-sufficient tool that runs from a graphical interface or from the command line. It creates applications-specific schemas and tablespaces for Oracle Database Enterprise Edition or Oracle Real Application Clusters.

8.6.1 Introduction to the Oracle Fusion Applications RCU

The Oracle Fusion Applications RCU components are included in the zipped Oracle Fusion Applications RCU file delivered in the provisioning framework. The Oracle Fusion Applications RCU offers these features:

- Integrates Oracle Fusion Middleware and Oracle Fusion Applications schema and storage definitions using declarative XML.
- Runs locally or remotely as a standalone tool.
- Lets you modify or use custom tablespaces for the default Oracle Fusion Applications schemas.
- Performs checks against both global and component-level prerequisites at runtime. If a prerequisite is not met, the Oracle Fusion Applications RCU may issue a warning and allow the procedure to continue (soft stop), or it may notify you that a prerequisite must be met (hard stop).

- Creates a resource plan, called `FUSIONAPPS_PLAN`, to manage Oracle Fusion Applications queries. For more information, see "How to Configure the Database Resource Manager" in *Oracle Fusion Applications Performance and Tuning Guide*.

8.6.1.1 Functional Design

The Oracle Fusion Applications RCU is designed to:

- Be completely self-contained. It has all the technical components necessary to perform the operations required (Oracle Client, binaries, scripts, data, and PL/SQL packages).
- Support Oracle Database 11.2.0.3 and database configurations such as ASM and Oracle RAC.
- Perform a silent execution.
- Operate on remote databases.
- Connect to an existing database, read existing tablespace definitions, and create schema owners and new tablespaces.

Some limitations of the Oracle Fusion Applications RCU are as follows:

- The database that you run it on must be empty. If applications-related schemas already exist, the option to modify them is grayed out.
- The Oracle Fusion Applications RCU does not provision delta schemas and does not perform database upgrades.
- The Oracle Fusion Applications RCU supports the import of full schemas only.
- The Oracle Fusion Applications RCU does not support the dropping of a component schema. You can, however, drop the entire instance directly through the database, if required.

8.6.1.2 How Does the Oracle Fusion Applications RCU Work?

You use the Oracle Fusion Applications RCU to create a repository of applications-specific schemas and tablespaces for Oracle Database.

Internally, the Oracle Fusion Applications RCU performs actions related to Oracle Fusion Middleware components and Oracle Fusion Applications components. In addition, the utility takes appropriate action to see that the tables are enabled to store repository resources.

Oracle Fusion Middleware Components

The Oracle Fusion Applications RCU loops through all the middleware components in the component definition file and applies the relevant ones to the database. For each component, the Oracle Fusion Applications RCU creates the appropriate middleware tablespace and schema user. After creating the schema user, it defines the tables, views, and other artifacts that the schema owner owns.

Oracle Fusion Applications Components

The Oracle Fusion Applications RCU creates empty tablespaces for the Oracle Fusion Applications components. It then creates the schema owners (for example, FUSION and FUSION_RUNTIME). These schema owners are initially empty — they do not own any tables or data.

The Oracle Fusion Applications RCU employs Oracle Data Pump to import the seed data and the dump files containing tables, views, and other artifact definitions that

belong to the schema users it has created. All dump files are packaged with the Oracle Fusion Applications RCU.

XML Schema Registration

When tables are created as part of an XML schema registration, by default the tables are enabled for hierarchy; that is, repository resources can be stored in the tables. Several triggers are created for this purpose. If resources are created, updated, or deleted based on the registered XML schema, the corresponding `XMLtype` rows in the tables are inserted, updated, or deleted.

Tables are disabled for the hierarchy before they are exported in dumpfile mode because some of the special features that make these tables store resources may not be meaningful in the target database. Disabling the hierarchy drops some triggers so that they do not show up in the target database after import of the dump files.

8.6.2 Running the Oracle Fusion Applications Repository Creation Utility using the Wizard

Use the information in this section to prepare to run the Oracle Fusion Applications RCU and complete the wizard screens necessary to create schemas and tablespaces.

Note: The Oracle Fusion Applications RCU is available only on Windows and Linux platforms. For other platforms, such as Solaris and AIX, you must install and run the Oracle Fusion Applications RCU from a Windows or Linux machine.

If you experience a failure in the Oracle Fusion Applications RCU, see Section 9.3.1, "General Troubleshooting Tips" to confirm if you can restart the Oracle Fusion Applications RCU. In some cases, you must start from the beginning by installing an empty database or using the Database Configuration Assistant and then running the Oracle Fusion Applications RCU.

8.6.2.1 Starting the Oracle Fusion Applications RCU

After you have completed the steps in the Getting Ready section, run the Oracle Fusion Applications RCU from (UNIX) *APPS_RCU_HOME*`/bin` or (Windows) *APPS_RCU_HOME*`\bin` with the following command:

UNIX: `./rcu`

Windows: `rcu.bat`

Note: The Oracle Fusion Applications RCU is available only on Linux and Windows platforms. On Windows systems, do not extract the rcuHome_fusionapps_win.zip file to a directory whose name contains spaces.

8.6.2.2 Wizard Screens and Instructions

Table 8–4 lists the steps for running the Oracle Fusion Applications RCU. For help with any of the screens, click **Help** on any screen.

Table 8–4 Running the Oracle Fusion Applications Repository Creation Utility

Screen	Description and Action Required
Welcome	No action is necessary on this read-only screen. Click **Skip this Page Next Time** if you do not want to see it the next time you log in to the Oracle Fusion Applications RCU. Click **Next** to continue.
Create Repository	Select **Create** to create and load component schemas into the database. See Section 4.4.2.3, "Schema and Password Requirements" for a list of schemas. Click **Next** to continue.
Database Connection Details	Specify the database connection details. See Section 8.6.2.3, "Specifying Database Connection Details" for specifics. Click **Next** to continue.
Select Components	The Oracle Fusion Applications RCU retrieves the names of the Oracle Fusion Middleware and the Oracle Fusion Applications components. You cannot change the schema owner names. By default, all components are checked so that they are included in the prerequisite check process. Click **Next** to begin the process. When the progress bar reports 100 percent complete and all prerequisites report a check mark, click **OK**. Click **Next** to continue. When you use the Provisioning Wizard to install the database using the dbca template, the default values for the disk_asynch_io and filesystemio_options parameters are as follows: disk_asynch_io is set to TRUE filesystemio_options will be set to the default value based on the platform where the database is installed. It could be either "none", "setall", "asynch", or "diskio". To verify that the filesystemio_options parameter is using the default value, run the following query: "select isdefault from v$parameter where name='filesystemio_options". If it returns TRUE, the default value is set. If you change the parameter value from the original default value to another value and then change it back to the original default value, the default value will still remain FALSE. The following Warning messages will be displayed based on the values set: If disk_asynch_io is set to FALSE and filesystemio_options is set to the default value, a Warning message will be displayed recommending setting the value for disk_asynch_io to TRUE. If disk_asynch_io is set to FALSE and filesystemio_options is not set to the default value, a Warning message will be displayed recommending setting the value for disk_asynch_io to TRUE for the best performance optimization.
Schema Passwords	Specify the passwords for main and additional (auxiliary) schemas. Passwords must have a minimum length of eight characters and contain alphabetic characters combined with numbers or special characters. ▪ **Use same passwords for all schemas**: Specify a single password for both schemas. Retype to **Confirm**. ▪ **Use main schema passwords for auxiliary schemas**: Specify a different password to use for each main schema and for the associated auxiliary schema. Only the main schemas are visible. Retype the password to **Confirm**. ▪ **Specify different passwords for all schemas**: Specify a unique password for each main schema and its auxiliary schema. All schemas are visible. Retype to **Confirm**. Note the passwords you enter. You must supply them when you create a response file. Click **Next** to continue.

Table 8–4 (Cont.) Running the Oracle Fusion Applications Repository Creation Utility

Screen	Description and Action Required
Custom Variables	Each Oracle Database directory object has a value represented by a physical directory on the database server. Custom variables are pre-defined, platform-specific directory objects that the Oracle Fusion Applications RCU creates. In the **Value** column, you specify a pre-existing physical directory (located on the database server) for each custom variable. See Section 8.6.2.4, "Managing Custom Variables" for a list of variables. Click **Next** to continue.
Map Tablespaces	If you want to start the tablespace create process without making any changes, click **Next** on this screen. A message informs you that any tablespaces that do not already exist will be created. Click **OK** to continue. The **Creating Tablespaces** progress screen appears. Click **OK** when the operation is completed. Or, view default tablespace mappings, change default and temporary tablespaces, view and change additional tablespaces, and manage tablespaces and datafiles (add, modify, or remove) before they are created. See Section 8.6.2.5, "Mapping Tablespaces". If you make changes, click **Next** when you are finished, then click **OK** to create the tablespaces. Click **OK** when the operation is complete.
Summary	Review the information and click **Create**. While the schemas are being created, the utility displays the **Repository Creation Utility – Create** screen, showing the creation progress. Typically, it takes 1 to 10 minutes to create each schema; however, the process may run for an additional half hour or more. To stop creating the schemas, click **Stop**.
Completion Summary	The Logfile column lists log file names. If errors are encountered during the Create operation, or if a Create operation fails for any component, the **Cleanup for failed components** checkbox appears on this page and is selected by default. If the checkbox is selected, the Oracle Fusion Applications RCU will perform cleanup operations for the components that failed. Click **Close** to dismiss the screen.

8.6.2.2.1 Database Schema User Password Complexity Rule

Starting with Oracle Fusion Applications 11*g* Release 8 (11.1.8), password check is enabled at the database level. The password check is enabled at the end of the install phase during provisioning (See Chapter 13, "Provisioning a New Oracle Fusion Applications Environment"). After the environment is provisioned, stronger schema user passwords will be required when you attempt to change schema passwords.

Ensure that the following conditions are satisfied when you change schema passwords:

- The password contains no fewer than 8 characters and does not exceed 30 characters.
- The password cannot be the same as the user name.
- The password cannot be the same length as the user name.
- The password cannot be the user name spelled backwards.
- The password cannot be the same as the server name or the server name with digits from 1 to 100 appended.
- Simple passwords will be rejected (for example, "welcome1").
- The password must start with an alphabetic character.
- The password must include at least one digit OR one special character $, #, or _.

8.6.2.3 Specifying Database Connection Details

Specify information about the hosts and ports that you want to use for your database.

- **Database Type**: Select the database type.

- **Host Name**: Enter the name of the node on which the database resides, for example, `myhost.mydomain.com`. For Oracle RAC, specify the VIP name or one of the node names as the host name.
- **Port**: Specify the listener port number for the database. The default port number is 1521.
- **Service Name**: This is the global database name. If you do not know it, see the `SERVICE_NAMES` parameter in the database initialization file. If it is not there, use the global name in `DB_NAME` and `DB_DOMAIN`. For Oracle RAC, specify the service name of one of the nodes, for example, `examplehost.exampledomain.com`.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> FA Transactional Database.

- **User Name**: Supply the name of the user with DBA or SYSDBA privileges. The default user name with SYSDBA privileges is `SYS`.
- **Password**: Enter the password for the database user.
- **Role**: Select Normal or SYSDBA. All schemas installed for Oracle Database require the `SYSDBA` role. For Oracle Internet Directory (OID) database schemas, use `SYS` and `SYSDBA`.

8.6.2.4 Managing Custom Variables

Enter a pre-existing physical directory on the database server where the custom variables for each component should be created.

- **FUSIONAPPS_DBINSTALL_DP_DIR**: The directory on the database server where you unzipped `export_fusionapps_dbinstall.zip` and copied the `otbi.dmp` file.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> FA Transactional Database -> RCU OTBI_DBINSTALL_DUMP_DIR.

- **APPLCP_FILE_DIR**: Used by Oracle Enterprise Scheduler to store the log and output files. Must be valid on the database server with read-write permissions to the database owner. For Oracle RAC, must point to a location that is shared across all nodes.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> FA Transactional Database -> RCU APPLCP_FILE_DIR.

- **APPLLOG_DIR**: Location of the PL/SQL log files from Oracle Fusion Applications PL/SQL procedures on the database server. Ensure that the database owner has read-write privileges. For Oracle RAC, you must point to the same file location that exists in each node or a location shared across all nodes.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> FA Transactional Database -> RCU APPLLOG_DIR.

- **OBIEE Backup Directory**: Location of the Oracle Business Intelligence Enterprise Edition dump files. These files are used for enabling a restart action.

> **Note:** You must manually create the directories on the database server and enter the full file path to the directories as the corresponding custom variable.
>
> This value is available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> FA Transactional Database -> RCU FUSIONAPPS_PROV_RECOVERY_DIR.

Secure Enterprise Search

- **Do you have Advanced Compression Option (ACO) License? Yes (Y) or No (N)**: Default is No.
- **Do you have Oracle Partitioning option License? Yes (Y) or No (N)**: Default is No.

Master and Work Repository

Note: The default values are the **only** valid values. If you change any of these values, the ODI-related provisioning process will not work.

- **Master Repository ID**: Default = 501
- **Supervisor Password**: Enter and confirm your ODI supervisor password.
- **Work Repository Type**: (D) Development or (R). Default = D
- **Work Repository ID**: Default = 501
- **Work Repository Name**: Default = FUSIONAPPS_WREP
- **Work Repository Password**: Enter and confirm your Work Repository supervisor.

Oracle Transactional BI

- Directory on the database server where Oracle Transactional Business Intelligence import and export files are stored.

  > **Tip:** This value is available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> FA Transactional Database -> RCU OTBI_DBINSTALL_DUMP_DIR.

Activity Graph and Analytics

- **Install Analytics with Partitioning (Y/N)**: Default is N.

8.6.2.5 Mapping Tablespaces

You can perform several operations from the **Map Tablespaces** screen including view, add, modify, or remove tablespaces. These actions are also available for additional tablespaces or datafiles.

8.6.2.5.1 Default Tablespace Mappings In the Default Tablespace and Temp tablespace columns, click a cell to select from a list of available additional tablespace names. The default tablespaces are as follows:

- `FUSION_TEMP`: For temporary tables.
- `FUSION_DYN_TS`: For dynamically generated PL/SQL statements.
- `FUSION_IAS_ORASDPM_AQ`: For advanced queuing JMS data and indexes.
- `FUSION_TS_AQ`: For advanced queuing JMS data and indexes.

- FUSION_TS_DQ: For data quality data and indexes.
- FUSION_TS_TOOLS: Associated with Oracle Fusion Middleware data and indexes.
- FUSION_TS_QUEUES: For advanced queuing and dependent tables and indexes.
- FUSION_TS_TX_DATA: For transactional data.
- FUSION_TS_TX_IDX: Indexes for transactional data.
- FUSION_TS_SEED: For seed or reference data and indexes.
- FUSION_TS_INTERFACE: For temporary or interface data and indexes.
- FUSION_TS_SUMMARY: For summary management objects.
- FUSION_TS_NOLOGGING: For materialized views and other temporary or scratch pad objects.
- FUSION_TS_ARCHIVE: For tables and objects that are no longer used.
- FUSION_TS_MEDIA: Contains multimedia objects such as text, video, and graphics.

For tablespaces that need to be created, the datafile defaults to %DATAFILE LOCATION%\%sid%\%tablespace_name%.dbf. You can select from existing tablespaces if they are already defined in the database.

8.6.2.5.2 Setting the Size of Tablespace Datafiles The default out-of-the-box Oracle Fusion Applications tablespace sizes are optimal. If you want to use different tablespace sizes, you can update the sizes of the tablespace (datafiles) on the **Manage Tablespaces** screen, accessed from the **Map Tablespaces** screen in the Oracle Fusion Applications RCU interface.

> **Note:** Due to a limitation in the framework used by Oracle Fusion Applications RCU, you cannot update the size for the tablespaces FUSION_TS_TX_DATA and FUSION_TS_TX_IDX from Oracle Fusion Applications RCU because their respective datafile names exceed 29 characters. You will need to manually change the datafile size using SQL. For example, if you want to resize the datafile to 2000 MB, use:
> `ALTER DATABASE DATAFILE '<full file path and file name of the datafile (file.dbf)>' RESIZE 2000M;`

Table 8–5 lists the sizes of the optimal and out-of-the-box tablespaces. You must make changes during the running of Oracle Fusion Applications RCU.

Table 8–5 Tablespace Optimal and OOTB Sizes

Tablespace Name	# of data files	Name of datafile	Size (MB) per datafile	Optimal/ out-of-the-box size (MB)
FUSION_DYN_TS	1	fusion_dyn_01.dbf	20	20
FUSION_IAS_ORASDPM_AQ	1	fusion_ias_sdpmqa_01.dbf	20	20
FUSION_TS_AQ	1	fusion_aq_01.dbf	200	200
FUSION_TS_ARCHIVE	1	fusion_archive_01.dbf	20	20
FUSION_TS_DQ	1	fusion_dq_01.dbf	20	20
FUSION_TS_INTERFACE	1	fusion_interface_01.dbf	750	750

Table 8–5 (Cont.) Tablespace Optimal and OOTB Sizes

Tablespace Name	# of data files	Name of datafile	Size (MB) per datafile	Optimal/ out-of-the-box size (MB)
FUSION_TS_MEDIA	1	fusion_media_01.dbf	20	20
FUSION_TS_NOLOGGING	1	fusion_nologging_01.dbf	20	20
FUSION_TS_QUEUES	1	fusion_queues_01.dbf	20	20
FUSION_TS_SEED	2	fusion_seed_01.dbf and fusion_seed_02.dbf	2048 and 1152	3200
FUSION_TS_SUMMARY	1	fusion_summary_01.dbf	20	20
FUSION_TS_TOOLS	4	fusion_tools_01.dbf - fusion_tools_04.dbf	2048, 2048, 2048, 1556	7700
FUSION_TS_TX_DATA	3	fusion_transaction_table_01.dbf - fusion_transaction_table_03.dbf	2048, 2048, 354	4450
FUSION_TS_TX_IDX	2	fusion_transaction_index_01.dbf and fusion_transaction_index_02.dbf	2048 and 1352	3400

8.6.2.5.3 Changing Default and Temporary Tablespace Names To change the default tablespace name for a component, select the name in the Default Tablespace column, and then select the name that you want to use from the list. You can have your components use any number of tablespaces to suit your configuration.

Follow the same procedure to change a temporary tablespace for a component by selecting a tablespace name from the Temp Tablespace list.

8.6.2.5.4 Viewing and Changing Additional Tablespaces Some components have additional tablespaces associated with their schemas. If so, the **Additional Tablespaces** button is active. Click it to view or modify additional tablespaces. Click the Tablespace Name column to select a tablespace.

Click **OK** when you are finished.

8.6.2.5.5 Managing Tablespaces and Datafiles Click **Manage Tablespaces** to add, modify, or remove tablespaces. Only tablespaces that have not yet been created can be modified or removed. Existing tablespaces are visible, but cannot be modified or removed.

Only tablespaces used by a component are created. You can specify a new tablespace, but unless it is used by a component, it will not be created.

To edit a tablespace, select it from the navigation tree. Complete the following:

- **Name**: Specify a new name for the tablespace.
- **Type**: Indicate whether this tablespace is temporary or permanent.
- **Block Size**: The block size (in kilobytes) to be used for data retrieval.
- **Storage Type**: Select **Use Bigfile Tablespace** if you have single large files. Select **Use Automatic Segment Space Management** to use bitmaps to manage free space within segments.

To **Add** a tablespace, specify the same details as for modifying one. Select a tablespace from the navigation tree and click **Remove** to prevent it from being created.

Manage Datafiles

Click the **Plus** (**+**) icon and complete the **Add Datafile** details:

- **File Name**: The name of the datafile.
- **File Directory**: The location where the datafile will reside.
- **Size**: The initial size of the datafile.
- **Automatically extend datafile when full (AUTOEXTEND)**: Select this option to extend the datafile size automatically when it becomes full. In the **Increment** field, select the size by which the datafile should be increased.
- To limit maximum size, specify a value in the **Maximum Size** field.

Select a datafile and click the **pencil** icon. Modify the information on the **Edit Datafile** screen. Select a datafile and click the **X** icon to delete the file.

Edit the Size of a Datafile

To change the size of a tablespace:

1. Click a tablespace name to select it.
2. Click the **pencil** icon to bring up the **Edit Datafile** screen.
3. In the **Size** field, enter a new file size. For tablespaces with multiple data files, such as `FUSION_TS_TX_DATA`, you may delete the additional data files using the Remove Data File icon (**X**).
4. Click **OK** when you have configured all the tablespaces to return to the Map Tablespaces screen.

Click **OK** to dismiss the screen.

8.6.3 Oracle Fusion Applications RCU Post-Installation Checklist

After running the Oracle Fusion Applications RCU, complete the following tasks:

- Use SQL*Plus or another tool to verify that the Oracle Fusion Applications schemas have been created. Run this SQL statement to get the list of schema owners in the database instance. Ensure that the list contains all schema owners listed in Table 4–4, " Oracle Fusion Middleware and Oracle Fusion Applications Schema Owners":

  ```
  select username from dba_users where default_tablespace not
  in ('SYSTEM','SYSAUX');
  ```

- Use SQL* Plus or another tool to verify that the Oracle Fusion Applications DBA directories have been created. Run this SQL statement to get the list of defined directory names:

  ```
  select * from ALL_DIRECTORIES;
  ```

- Use SQL*Plus or another tool to verify the ability to connect as one of the Oracle Fusion Applications schema users.

8.7 What to Do Next

When you have completed the database installation and the schema and tablespace creation, follow the instructions in Chapter 9 to troubleshoot any issues.

9

Troubleshooting Database Installations

This chapter describes database troubleshooting instructions.

This chapter contains the following sections:

9.1 Introduction to Troubleshooting Database Installations

You can follow the instructions described in this chapter if you encounter issues during database installation for Oracle Identity Management or Oracle Fusion Applications.

It also describes troubleshooting tips for the Oracle Fusion Middleware Repository Creation Utility (used for Oracle Identity Management) and Oracle Fusion Applications Repository Creation Utility operations.

9.2 Troubleshooting the Oracle Identity Management Database Installation and Oracle Fusion Middleware RCU Operations

For more information about troubleshooting Oracle Database, see "Troubleshooting" in the *Oracle Database Installation Guide for Linux*.

For more information about troubleshooting the Oracle Fusion Middleware RCU, see "Troubleshooting Repository Creation Utility" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

9.3 Troubleshooting Oracle Fusion Applications Database Installation and Oracle Fusion Applications RCU Operations

This section contains troubleshooting tips for database installation and the Oracle Fusion Applications RCU operations. It is divided into sections for general tips and sections about log files and cleanup features.

9.3.1 General Troubleshooting Tips

If you encounter an error during the creation of applications schemas and tablespaces, take note of the following:

- Oracle Fusion Applications release notes may contain additional information about this release, such as mandatory Oracle Database server and client patches that must be applied to your environment.
- This release of Oracle Fusion Applications relies on specific system requirements that are explained in the "Certification" section of Oracle Fusion Applications release notes.
- If you encounter abnormal program termination and the error log displays: `Java Exception: java.lang.StackOverflowError occurred` while installing Oracle database, then see document id 1056200.1 at My Oracle Support.
- Ensure that your database is up and running.
- If you experience a failure in the Oracle Fusion Applications RCU during the creation of the tablespaces and loading of the Fusion schemas, you must start from the beginning by installing an empty database or using the Database Configuration Assistant. There is no drop option.
- Clean up these areas before you redo the installation:
  - /tmp
  - old log file directories
  - /oraInventory folder contents
  - ORACLE_HOME (or remove the ORACLE_HOME if you need to re-use the directory
- If you entered incorrect information on one of the Oracle Fusion Applications RCU screens, use the navigation pane on the left side of the graphical interface to return to that screen.
- If an error occurred while the Oracle Fusion Applications RCU was running:
  1. Note the error and review the Oracle Fusion Applications RCU log files.
  2. Correct the issue that caused the error. Depending on the type of error, you can either continue with your operation or restart the Oracle Fusion Applications RCU.
  3. Continue or restart the Oracle Fusion Applications RCU to complete the desired operation.

9.3.2 Database Installation Log Files

The database installation log file reports what happened during each of the phases in a database installation. Click a log file symbol on the **Database Installation Progress** screen in the Provisioning Wizard to view the log file for that phase. Log files are located in *`tmp_directory`*`/dbInstall_`*`time_stamp`*`_provtop/logs/provisioning/`*`host`*. An example on a Linux platform is `/tmp/dbInstall_20120216092937_provtop/logs/provisioning/host123`. The `tmp` directory may differ depending on what is considered to be the temporary directory for various platforms. The location of the plan file for the database flow is to tmp_directory/`dbInstall`_time_stamp_`provtop/dbInstall`_time_stamp.`plan`.

9.3.3 Oracle Fusion Applications RCU Log Files

Log files describe what happened during the schema and tablespace creation process, including any failures that occurred. The main Oracle Fusion Applications RCU log file (rcu.log) is written to (Linux) *APP_RCU_HOME*/rcu/log/logdir.*date_timestamp* or (Windows) *APP_RCU_HOME*\rcu\log\logdir.*date_timestamp*. For example, the log file on a Linux operating system is:

APP_RCU_HOME/rcu/log/logdir.2010-01-02_03-00/rcu.log

The custom_comp_create_tbs.log file lists the PL/SQL statements that created the tablespaces.

In the fusionapps schema, three types of log files are created:

- **fusionapps.log**: Lists the PL/SQL that was run.
- **fusionapps_runimport.log**: The Oracle Data Pump import log file.
- **fusionapps_verify.log**: Lists verification errors if objects created are not what was expected.

In addition to the general log files, each component writes a log file of its own. The file name is in the form of *component_name*.log. For example, the log file for the BIAPPS_OTBI_RUNIMPORT component is biapps_otbi_runimport.log. All component log files are written to the same directory as the main log file.

Table 9–1 lists the log files in alphabetical order, by component name.

Table 9–1 Oracle Fusion Applications RCU Log File Names

Component Log File Name
biapps_otbi_runimport.log
crm_fusion_mds_soa.log
crm_fusion_orabam.log
crm_fusion_soainfra.log
fin_fusion_mds_soa.log
fin_fusion_soainfra.log
fscm_fusion_orabam.log
fusion_activities.log
fusionapps.log
fusion_biplatform.log
fusion_discussions.log
fusion_ipm.log
fusion_ocserver11g.log
fusion_ora_ess.log
fusion_orasdpls.log
fusion_orasdpm.log
fusion_orasdpsds.log
fusion_orasdpxdms.log
fusion_otbi.log
fusion_mds.log
fusion_mds_ess.log
fusion_mds_spaces.log

Table 9–1 (Cont.) Oracle Fusion Applications RCU Log File Names

Component Log File Name
fusion_portlet.log
fusion_webcenter.log
hcm_fusion_mds_soa.log
hcm_fusion_orabam.log
hcm_fusion_soainfra.log
oic_fusion_mds_soa.log
oic_fusion_soainfra.log
prc_fusion_mds_soa.log
prc_fusion_soainfra.log
prj_fusion_mds_soa.log
prj_fusion_soainfra.log
scm_fusion_soainfra.log
scm_fusion_mds_soa.log
searchsys.log
setup_fusion_mds_soa.log
setup_fusion_soainfra.log

9.3.4 Preverification and Preconfigure Failures (Windows)

You may encounter the following errors while running the preverification phase on Windows systems:

```
"C:\repository_location/installers/database/Disk1/setup.exe":
CreateProcess error=740, The requested operation requires elevation at
java.lang.ProcessBuilder.start(ProcessBuilder.java:460)
```

If you receive this error, disable User Account Control (UAC) or log in as a Local Administrator to the machine where the Provisioning Wizard is not functioning properly.

If you receive this error when running the preconfigure phase, close the Provisioning Wizard and restart. Select another Oracle Home location.

```
OPatch failed with error code = 73
```

```
UtilSession failed: Prerequisite check "CheckActiveFilesAnd Executables"
failed
```

See http://technet.microsoft.com for more information about UAC.

9.3.5 Preverification Failure (Solaris)

During provisioning, the preverify phase (target) may display a message that some of the Solaris operating system patches are missing. On Solaris x86-64, the following preverify failures may be reported:

```
WARNING: Check:Patches failed.
Checking for 127111-02; Not found.  Failed <<<<
Checking for 137111-04; Not found.  Failed <<<<
```

These failure messages can be ignored.

9.3.6 Using the Cleanup Feature

If there is a failure in creation of the tablespaces or schemas for any component, the **Cleanup for failed components** checkbox appears on the **Completion Summary** screen. Select this option to clean up tablespaces and schemas for the failed components.

If an environment (such as the database server) is running out of space, correct it and rerun the software. Any components that are not applied successfully are still enabled (not grayed out) in the interface. Rerun the Oracle Fusion Applications RCU as described in Section 8.6, "Running the Oracle Fusion Applications RCU to Create Oracle Fusion Applications Database Objects".

9.4 What to Do Next

Follow the instructions in Chapter 10 to create a response file and provision an Oracle Identity Management environment.

Part V

Provisioning Oracle Identity Management

This part describes Oracle Identity Management provisioning.

Part V contains the following chapters:

10

Oracle Identity Management Provisioning

This chapter describes the tasks you should complete if you want to implement Oracle Identity Management Provisioning for both the Single Host and Enterprise (EDG) topologies.

> **Note:** The Single Host topology is recommended only for test environments, whereas the Enterprise topology, which is more complex, is suitable for staging, QA, and production deployments.

This chapter contains the following sections:

10.1 Introduction to Oracle Identity Management Provisioning

The Oracle Identity Management Provisioning Wizard and related tools were developed to automate Oracle Identity Management Provisioning and reduce the time required to configure Oracle Identity Management for Oracle Fusion Applications.

> **Note:** All server machines in an Oracle Identity Management Provisioning environment must be running the same operating system major version and patch level. Heterogeneous operating system deployments are not supported.

Before you provision Oracle Identity Management, ensure that you have completed the following tasks:

1. Follow the instructions in Chapter 6 and successfully installed the Oracle Identity Management Provisioning framework.
2. Create an Oracle Identity Management provisioning profile as described in Section 10.2, "Creating an Oracle Identity Management Provisioning Profile".

The Oracle Identity Management Provisioning process itself consists of two tasks:

1. Running the Oracle Identity Management Provisioning Wizard, a graphical user interface that uses an interview process to gather information about the environment and store it in a Provisioning Response file. This task is described in Section 10.6, "Monitoring Provisioning Using the Oracle Identity Management Provisioning Wizard"
2. Executing command-line tools to set up the environment on the selected host machines. In many cases, you can monitor the progress of the command-line tools by using the wizard. This task is described in Section 10.5, "Performing Provisioning by Running the Provisioning Commands"

After provisioning, perform the tasks in Section 10.7, "Performing Mandatory Oracle Identity Management Post-Installation Tasks".

10.2 Creating an Oracle Identity Management Provisioning Profile

Before you can perform provisioning, you must provide information about your topology to the Oracle Identity Management Provisioning Wizard. Once you have provided all the necessary input, the wizard will create a provisioning file called `provisioning.rsp` that you use to perform the provisioning operation.

> **Note:** Even if you select a single node install, the screens in the Oracle Identity Management Provisioning Wizard show multinode items such as Virtual Host Configuration and Load Balancer Configuration. You can ignore the unused fields.

10.2.1 Creating a Provisioning Profile

Before running the provisioning tool, set the following environment variables:

- Set `JAVA_HOME` to: *`REPOSITORY_LOCATION`*`/jdk6`
- On UNIX systems, set the `DISPLAY` environment variable to an active and authorized display.

To start the Oracle Identity Management Provisioning Wizard, execute the following commands from: `IDMLCM_HOME/provisioning/bin`, where *`IDMLCM_HOME`* is the place where you installed the Oracle Home Directory for Oracle Identity Management, using the installation script for the Oracle Identity Management Provisioning Wizard and Oracle Identity Management Patching Tools, as described in Section 6.2.3, "Installing the Oracle Identity Management Lifecycle Tools".

Linux or UNIX:

```
./idmProvisioningWizard.sh
```

Windows:

```
idmProvisioningWizard.bat
```

When the wizard starts, proceed as described in the following sections:

- Welcome Page
- Specify Inventory Directory Page
- Identity Management Installation Options Page
- Specify Security Updates Page
- Product List Page
- Response File Description Page
- Install Location Configuration Page
- Node Topology Configuration Page
- Virtual Hosts Configuration Page
- Common Passwords Page
- OID Configuration Page
- ODSM Configuration Page
- OHS Configuration Page
- OIM Configuration Page
- OAM Configuration Page
- SOA Configuration Page
- OID Identity Store DB Configuration Page
- OID Policy Store DB Configuration Page
- OIM DB Configuration Page
- OAM DB Configuration Page
- Load Balancer Page
- Summary Page

10.2.1.1 Welcome Page

Use the Welcome page to learn more about the wizard, including some prerequisites for using it.

The Welcome page provides a brief overview of the wizard and lists some requirements that must be met.

Click **Next** to continue.

10.2.1.2 Specify Inventory Directory Page

If you are presented with the Specify Inventory Directory page, proceed as described in Step 2 in Section 6.2.3, "Installing the Oracle Identity Management Lifecycle Tools".

Click **OK** to continue.

10.2.1.3 Identity Management Installation Options Page

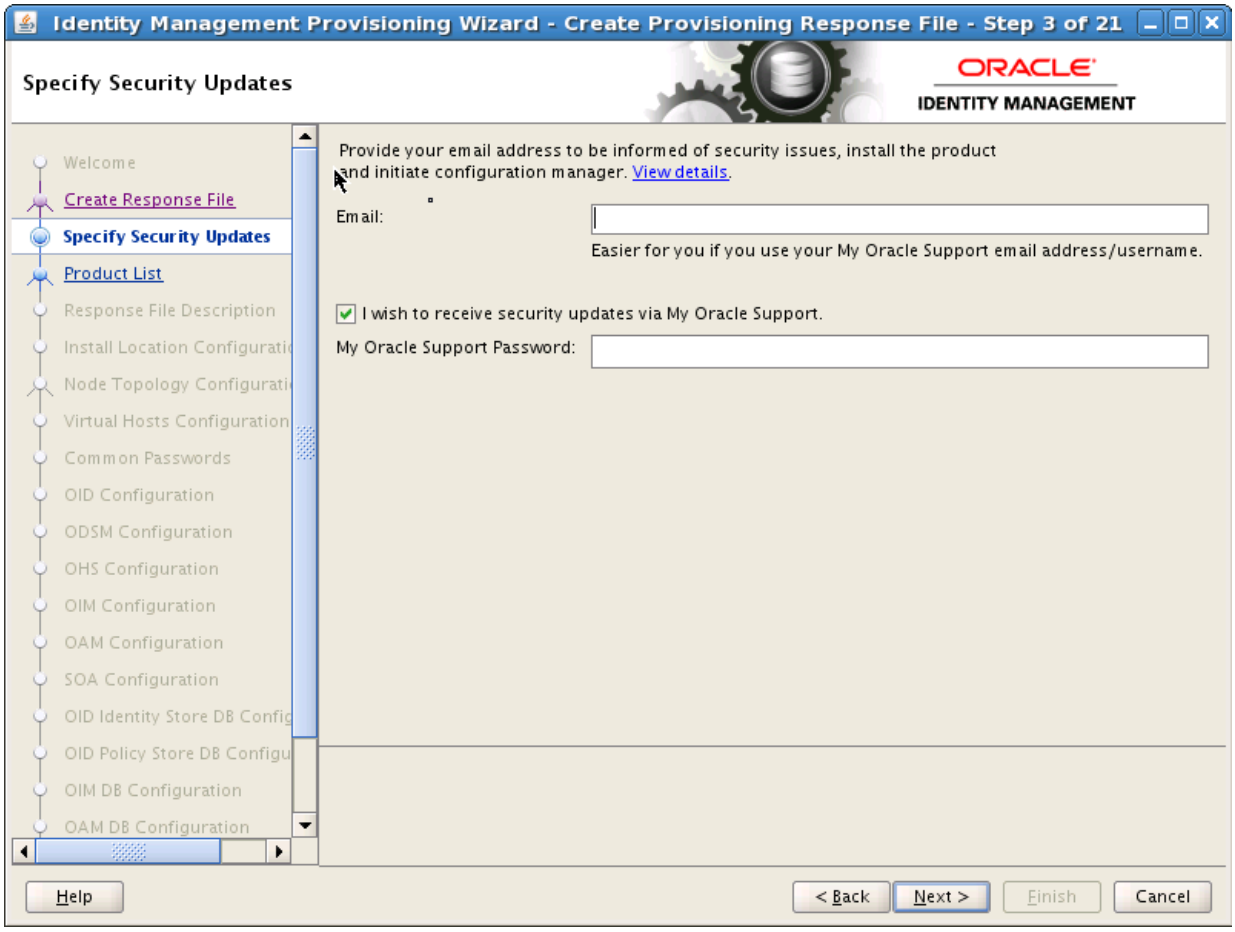
Select **Create a New Identity Management Environment Provisioning Response File** if you are creating a response file for the first time.

Update an Existing Identity Management Environment Provisioning Response File is not supported.

Click **Next** to continue.

10.2.1.4 Specify Security Updates Page

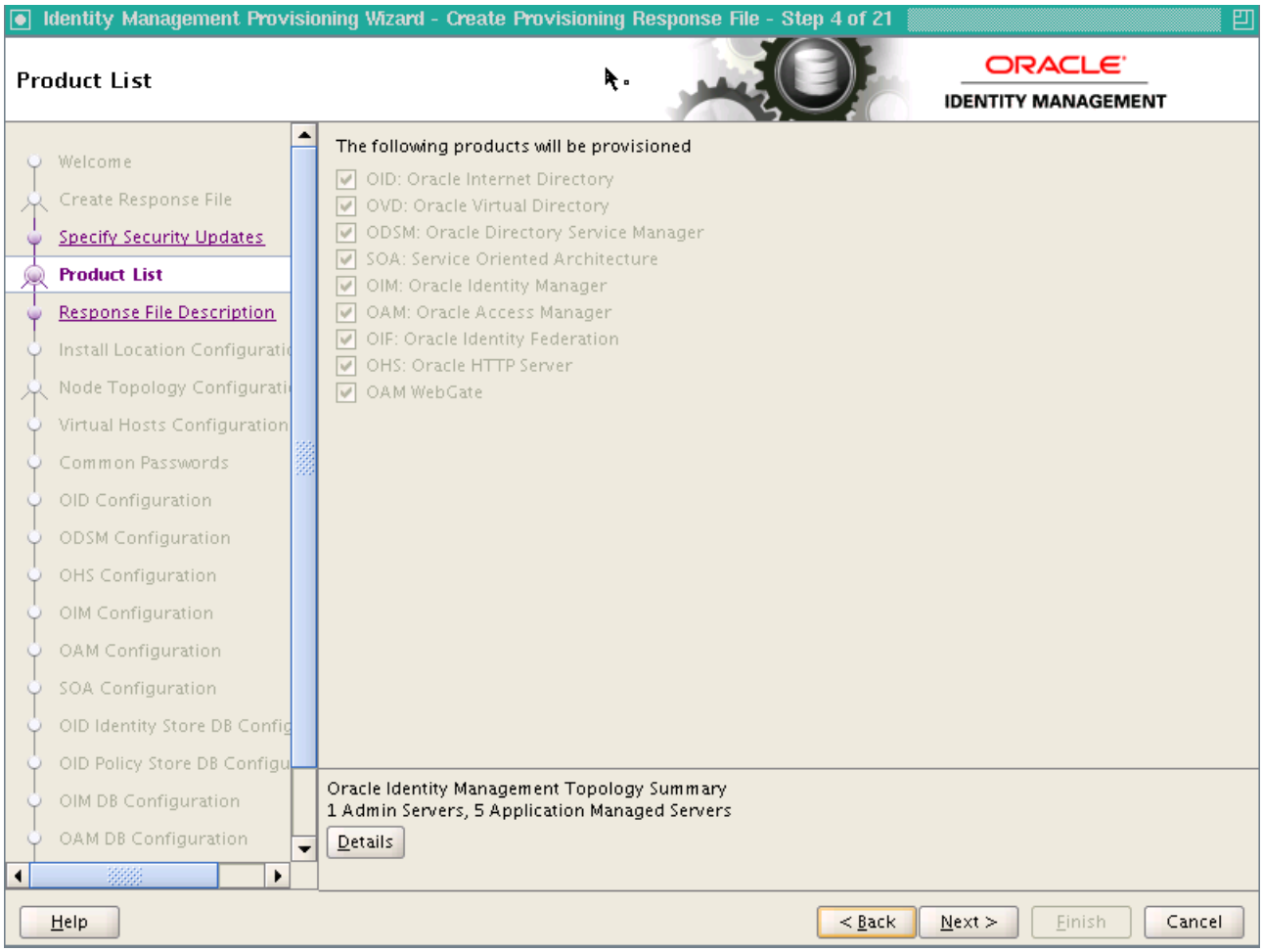
The checkbox should be unchecked, as this feature is not supported.



Click **Next** to continue.

10.2.1.5 Product List Page

The Product List page is purely informational. It displays the list of products that are installed and configured by the Oracle Identity Management Provisioning Wizard.

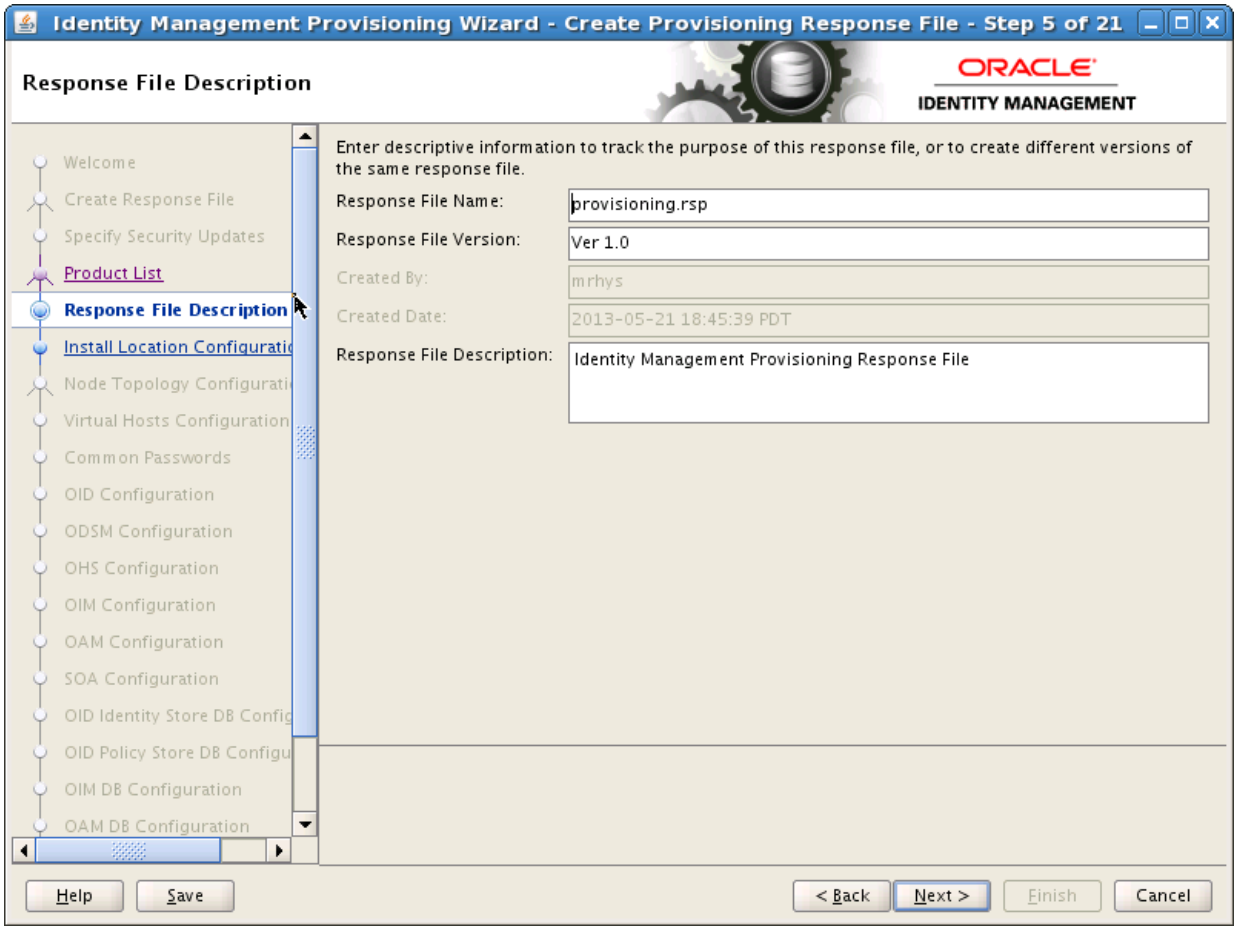


Click **Next** to continue.

10.2.1.6 Response File Description Page

Specify descriptive information to identify this response file. This description is not associated in any way with the executable plan file, or the summary file, that you save at the end of the response file creation process.

- **Response File Name**: The Oracle Identity Management Provisioning Wizard provides the default title Oracle Identity Management Provisioning Response File. You can change this.
- **Response File Version**: The Oracle Identity Management Provisioning Wizard provides a default value, which you can change. You can use this to keep track of different file versions.
- **Created By**: Defaults to the operating system user who invoked the Provisioning Wizard. Set when the response file is initially created and cannot be modified for the current response file.
- **Created Date**: Defaults to the date that the response file was initially created. Set when the response file was initially created and cannot be modified for the current response file.
- **Response File Description**: Provide a description of this response file. This is an optional field.



Click **Next** to continue.

10.2.1.7 Install Location Configuration Page

Use the Install Location Configuration page to supply the location of the various directories required for installation and configuration actions.

Installation and Configuration

- **Software Repository Location**: Specify the location of the software repository, either by typing it in the field or by clicking the **Browse** button, navigating to the desired location, and selecting it. This location must contain a folder named `installers`, which contains the software to install.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Storage tab -> Temporary Shared Storage -> Provisioning Repository Location.

- **Software Installation Location**: Specify the location on shared storage where you want the Middleware Homes to be placed, either by typing it in the field or by clicking the **Browse** button, navigating to the desired location, and selecting it. In a multinode scenario, this folder must be shared across all machines.

  Ensure that this directory path is 45 characters or fewer in length. A longer path name can cause errors during Oracle Identity Management provisioning.

Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Storage tab -> Install Directories -> IDM Software Installation Location.

- **Shared Configuration Location**: Specify the shared configuration location, either by typing it in the field or by clicking the **Browse** button, navigating to the desired location, and selecting it.

  In a single host environment, the shared configuration location is not actually shared.

  For the Enterprise topology , this is where the artifacts to be shared across all hosts, such as keystores, scripts to start/stop services, and life cycle management information, will be created. In a multi-node scenario, this folder must be shared across all machines.

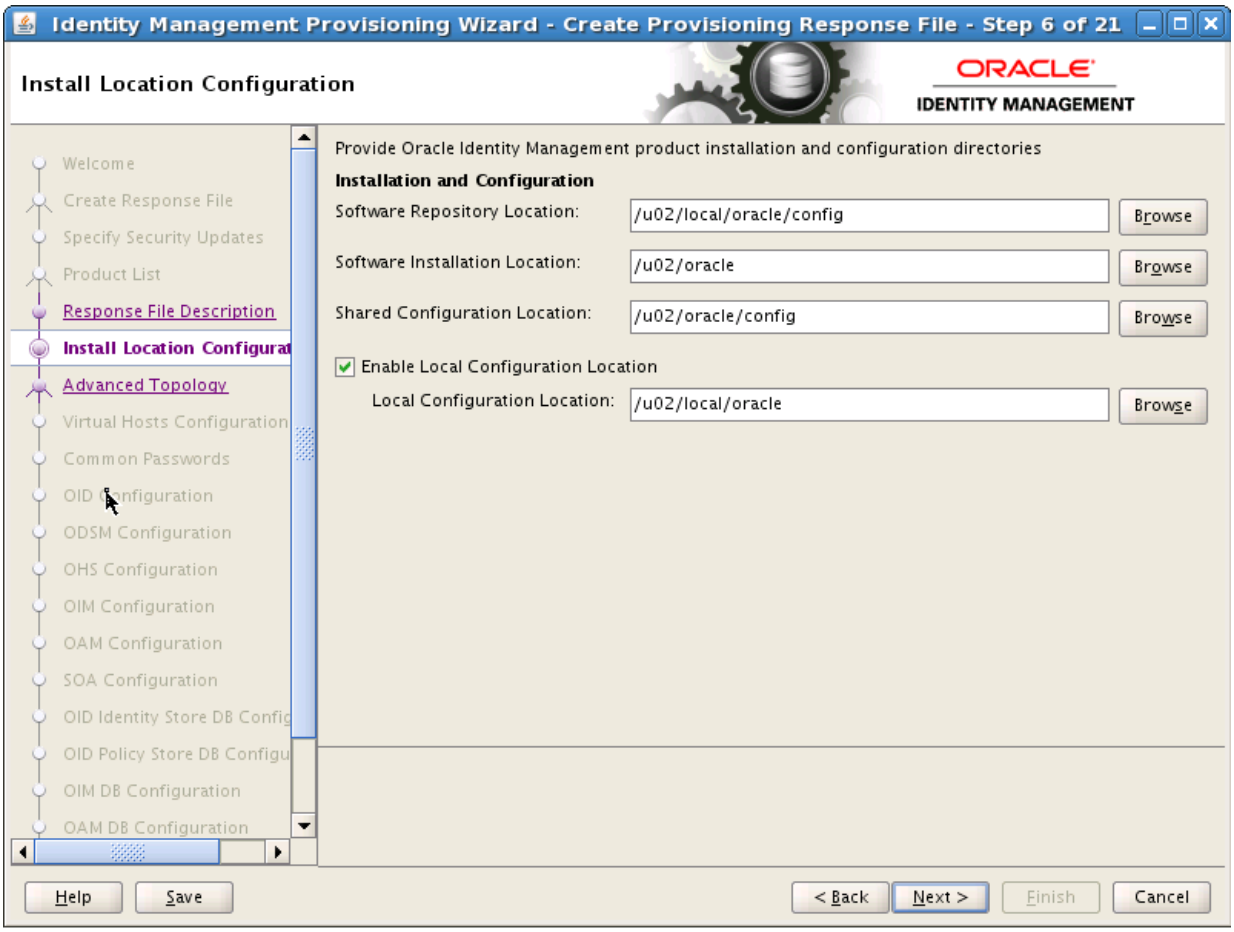
  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Storage tab -> Install Directories -> IDM Shared Configuration Location.

- **Enable Local Configuration Location**: Select this option **only** when provisioning the Enterprise topology.

  Depending on the decision made during the planning phase this option will be available in the *Oracle Fusion Applications Installation Workbook* - Storage tab -> Install Directories -> IDM Local Configuration Location. If the value is not specified in the *Oracle Fusion Applications Installation Workbook*, clear this checkbox.

  – **Local Configuration Location**: Specify the location for the local domain directory that you want to set up, either by typing it in the field or by clicking the **Browse** button, navigating to the desired location, and selecting it. This field is required if you selected **Enable Local Applications Configuration**. The specified directory must initially be empty. This folder should not be shared across hosts.

    Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Storage tab -> Install Directories -> IDM Local Configuration Location.



Click **Next** to continue.

10.2.1.8 Node Topology Configuration Page

Use the Node Topology Configuration page to select configuration options and provide information about hosts and products.

> **Tip:** This value is available in the *Oracle Fusion Applications Installation Workbook* - Environment tab -> Environment Info -> IDM Topology Type.

- **Single Host**: Select to provision a simple, single host topology. This topology is recommended **only** for test and development environments.
  - **Host Name**: Specify the host where you want to provision Oracle Identity Management, as a fully-qualified host name.
- **EDG Topology**: Select to provision a multiple host topology.
  - **Product(s)**: This field cannot be edited. It specifies the tier that will be installed and configured on the host.
  - **Host Name**: Specify each host where you want to provision the corresponding product tier, as a fully-qualified host name. To install Oracle Identity Management on a single host, specify the same host name for all products.

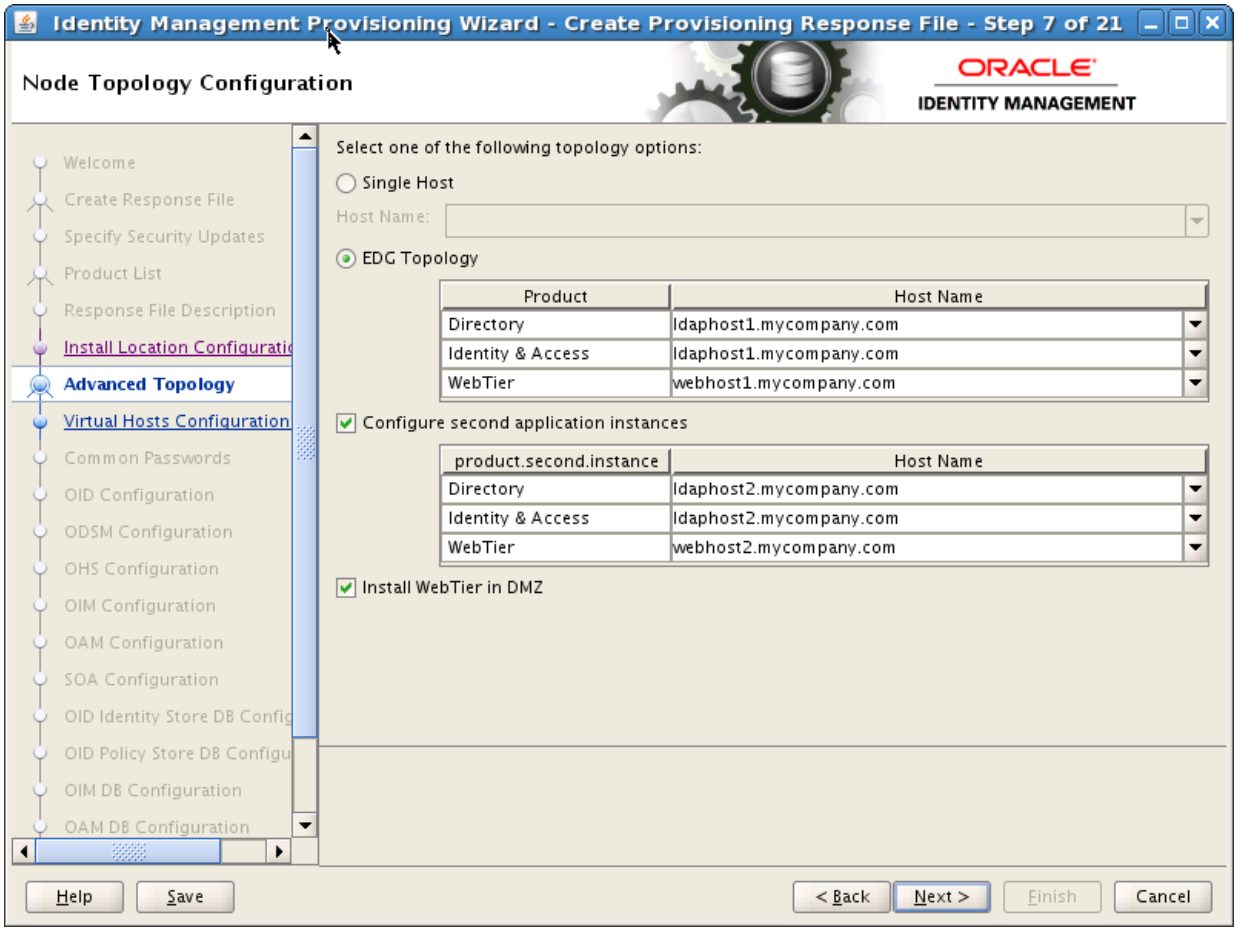
- **Configure second application instances**: Select to configure second instances of the applications you specified under EDG Topology. Selecting this option will provision a highly-available environment.
  - **Application(s) - Second Instance**: This field cannot be edited and specifies the tier that will be installed and configured on the host.
  - **Host Name**: Specify the host where you want to provision the second instance of these applications, as a fully-qualified host name. To install all second instances of all products on a single host, specify the same host name for all products.

    Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Topology tab:

    - Abstract Hostname (or real Hostname if no Abstract) from Topology table row that matches the following components:
      - IDM Directory
      - IDM Identity and Access
      - IDM WebTier

- **Install WebTier in DMZ**: Do not select this option for a Single Host topology or when the Web Tier is installed on the same host as other products.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Topology tab -> Topology -> DMZ (Yes/No) - for the node that corresponds to the component IDM WebTier.



Click **Next** to continue.

10.2.1.9 Virtual Hosts Configuration Page

Use the Virtual Hosts Configuration page to select virtual host configuration options. If you selected **Single Host**, the Virtual Hosts Configuration page cannot be edited.

You can associate the Administration Server, Oracle Identity Manager and Oracle SOA Suite servers with virtual IP addresses. If you selected **Configure second application instances** on the Node Topology Configuration page, having a virtual IP address will allow the Administration Server to be started on a different host if the primary host fails. Virtual IP addresses and virtual host names are required to enable server migration on Oracle Identity Manager andOracle SOA Suite servers. Server migration must be configured for the Oracle Identity Manager and Oracle SOA Suite managed servers for high availability.

Specify the configuration settings for the virtual hosts required by Oracle Fusion Applications.

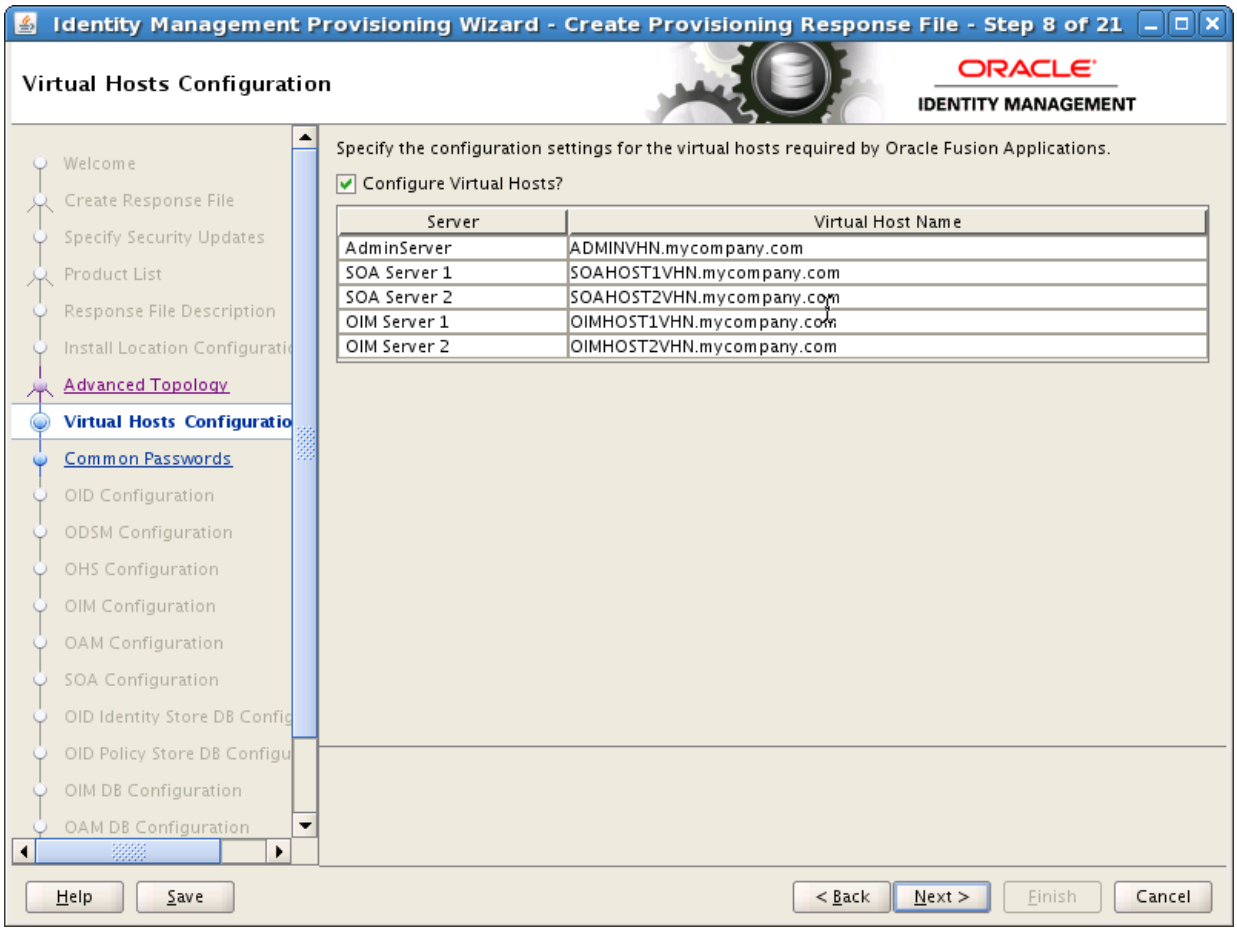
- **Configure Virtual Hosts?**: Select to configure virtual hosts.
- **Server**: Identifies each server.
- **Virtual Host Name**: Specify the virtual host name for the server.

Tip: This value is available in the *Oracle Fusion Applications Installation Workbook*:

- Admin Server: Network - Virtual Hosts tab -> AdminServer Virtual Hosts/VIPs -> IDMDomain AdminServer
- SOA Server 1: Network - Virtual Hosts tab -> Managed Server Virtual Hosts/VIPs -> IDMDomain SOA Server
- OIM Server 1: Network - Virtual Hosts tab -> Managed Server Virtual Hosts/VIPs -> IDMDomain OIM Server

For the Enterprise topology, specify the virtual host name from the *Oracle Fusion Applications Installation Workbook* for each managed server in the topology. For example:

- Admin Server:ADMINVHN.mycompany.com
- SOA Server: SOAHOST1VHN.mycompany.com
- SOA Server 2: SOAHOST2VHN.mycompany.com
- OIM Server: OIMHOST1VHN.mycompany.com
- OIM Server 2: OIMHOST2VHN.mycompany.com

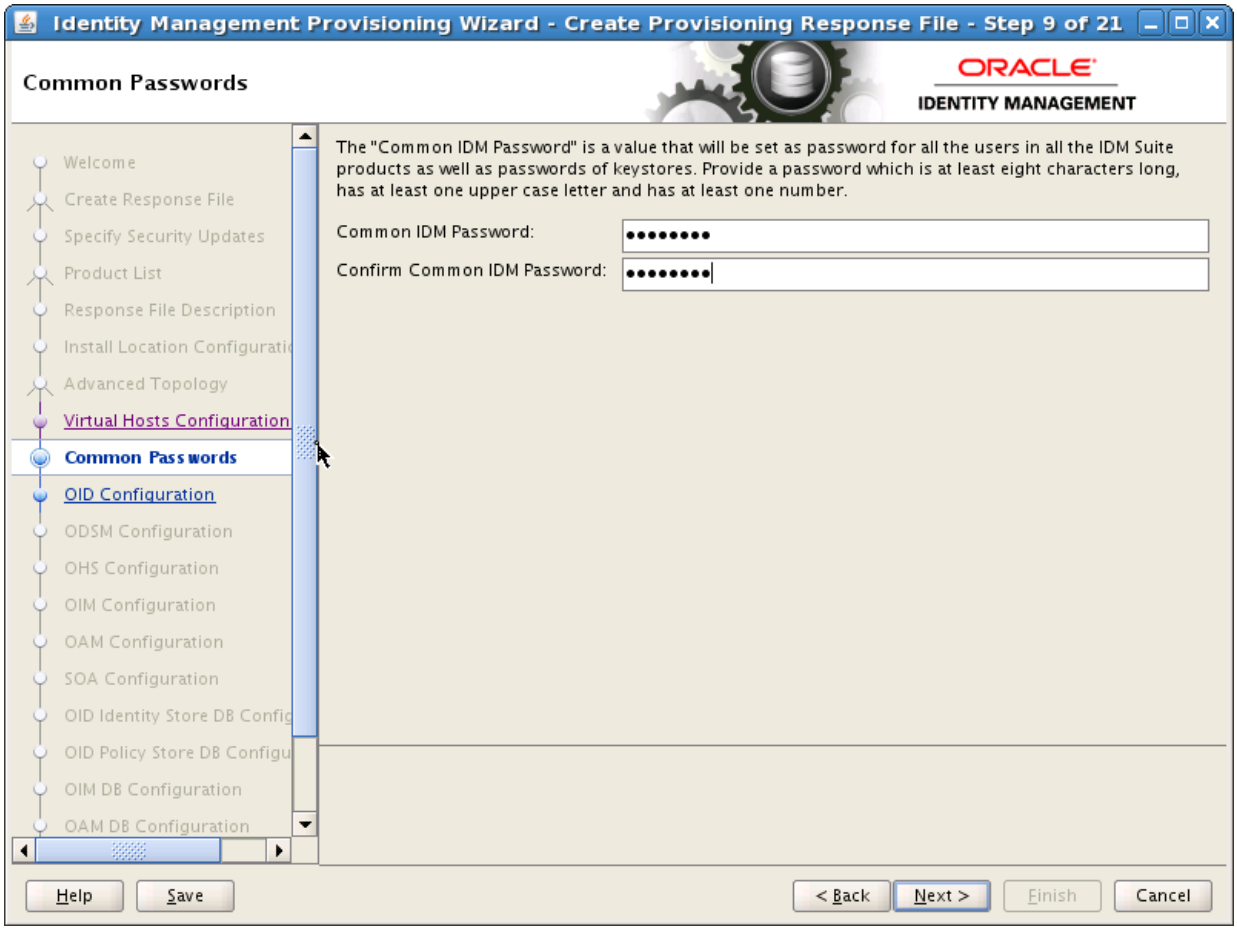


Click **Next** to continue.

10.2.1.10 Common Passwords Page

Use the Common Passwords page to select a common password.

- **Common Identity Management Password**: Specify a password to be used for all administrative users in the Oracle Identity Management Suite and for keystores. The password must be at least eight characters long and must contain at least one uppercase letter and at least one number.
- **Confirm Common Identity Management Password**: Reenter the password.



Click **Next** to continue.

10.2.1.11 OID Configuration Page

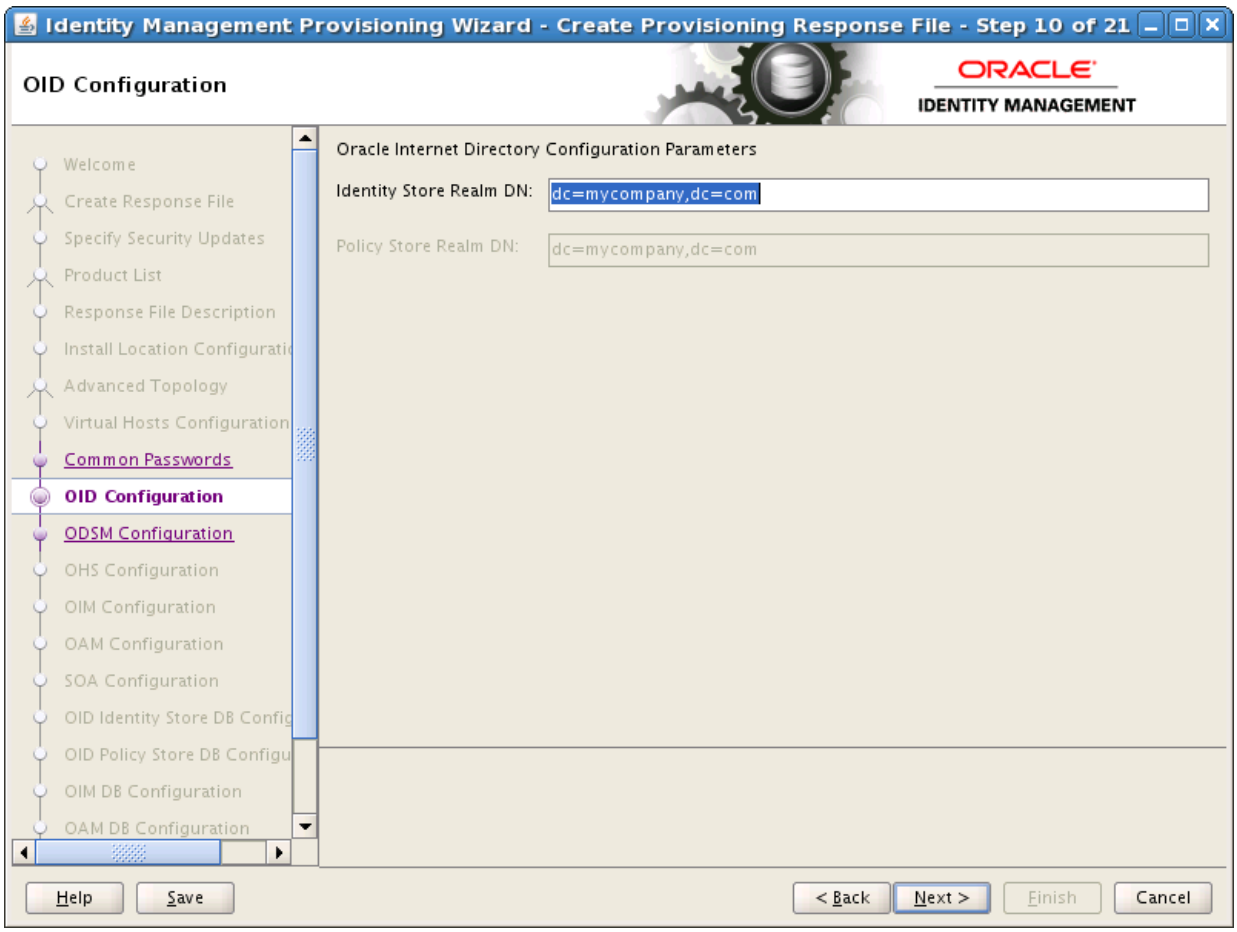
Use the OID Configuration page to select configuration options for Oracle Internet Directory.

Oracle Internet Directory Configuration Parameters

- **Identity Store Realm DN**: Specify the Distinguished Name of the Oracle Internet Directory realm, for example: `dc=mycompany,dc=com`.

Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Identity Management tab -> LDAP -> Identity Store Realm DN.

- **Policy Store Realm DN**: This field cannot be edited. The Policy Store and Identity Store will always be the same.



Click **Next** to continue.

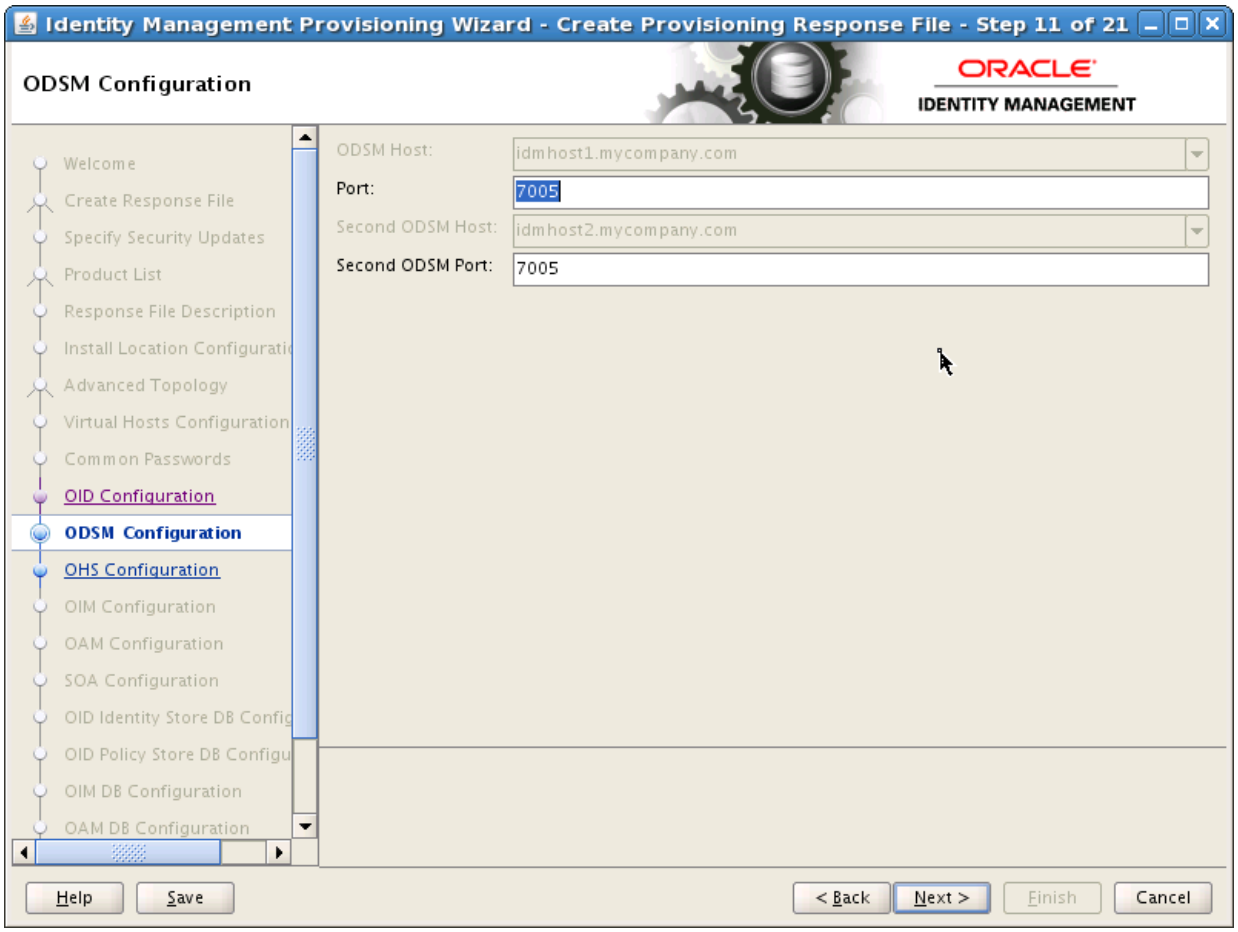
10.2.1.12 ODSM Configuration Page

Use the ODSM Configuration page to select configuration options for Oracle Directory Services Manager (ODSM). Information about the second host will appear on the page for EDG topology or if Configure Second Instances Topology was selected in the Node Topology Configuration Page.

- **ODSM Host**: This field is purely informational. The value is determined by the host entered in the Node Topology Configuration Page.
- **Port**: Specify the port to be used by the first ODSM instance.

Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Identity Management Port Numbers -> IDMDomain ODSM.

- **Second ODSM Host**: This field is purely informational. The value is determined by the host entered in the Node Topology Configuration Page.
- **Second ODSM Port**: Specify the port to be used by the second ODSM instance.



Click **Next** to continue.

10.2.1.13 OHS Configuration Page

Use the OHS Configuration page to change the installation ports used for Oracle HTTP Server (OHS). Information about the second host will appear on the page only if Configure Second Instances Topology was selected in the Node Topology Configuration Page.

Oracle HTTP Server for Identity Management Configuration Parameters

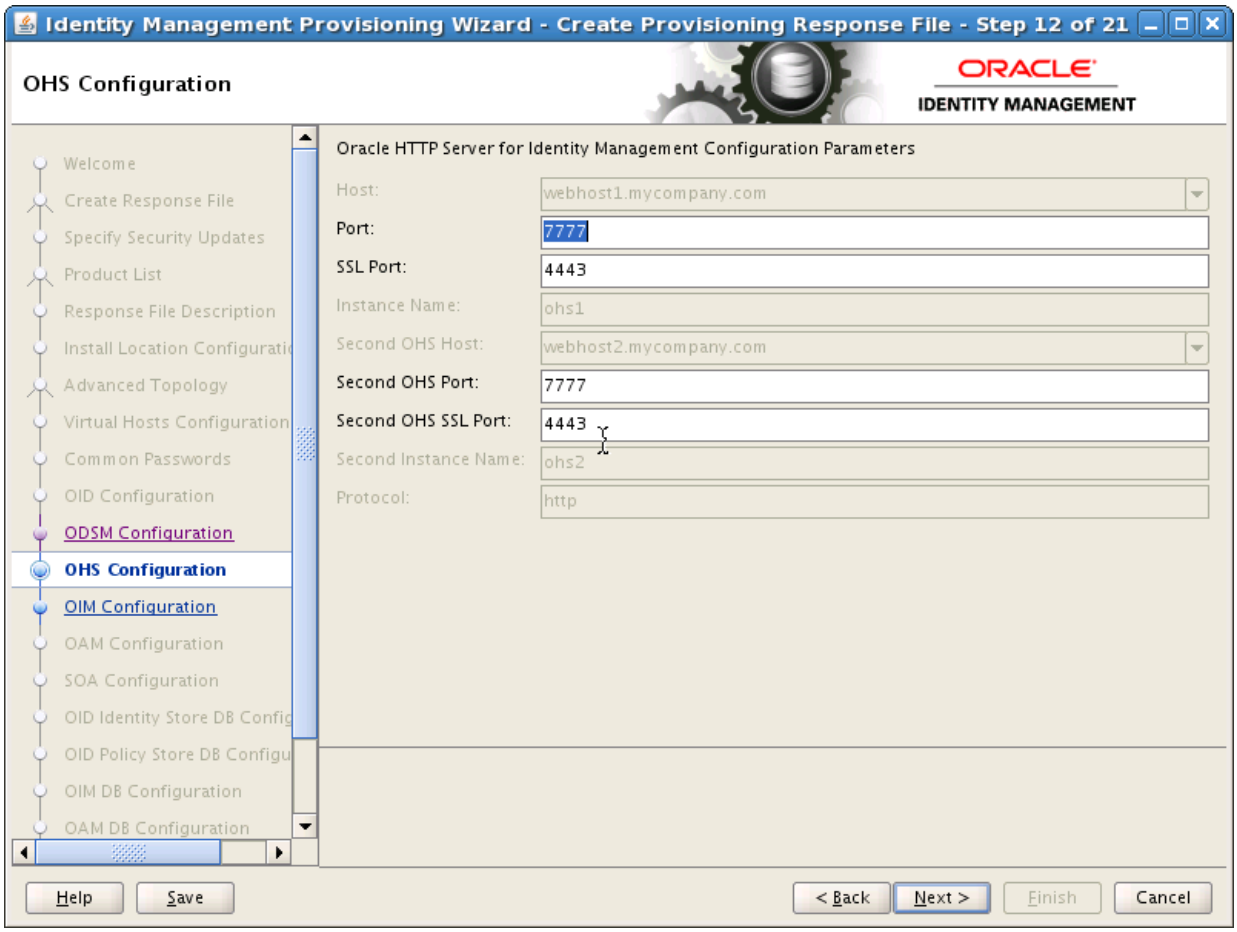
- **Host**: This field is purely informational. The value is determined by the host entered in the Node Topology Configuration Page.
- **Port**: Specify the non-SSL port number to be used for the first instance of the Oracle HTTP Server.

> **Tip:** This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Identity Management Port Numbers -> IDM Oracle HTTP Server.

- **SSL Port**: Specify the SSL port number to be used for the first instance of the Oracle HTTP Server.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Identity Management Port Numbers -> IDM Oracle HTTP Server SSL.

- **Instance Name**: This field is purely informational. It displays the instance name of the first Oracle HTTP Server.
- **Second OHS Host**: This field is purely informational. The value is determined by the host entered in the Node Topology Configuration Page.
- **Second OHS Port**: Specify the non-SSL port number to be used for the second instance of the Oracle HTTP Server.
- **Second OHS SSL Port**: Specify the SSL port number to be used for the second instance of the Oracle HTTP Server.
- **Second Instance Name**: This field is purely informational. It displays the instance name of the second Oracle HTTP Server.
- **Protocol**: This field is purely informational.



Click **Next** to continue.

10.2.1.14 OIM Configuration Page

Use the OIM Configuration page to modify the ports used by Oracle Identity Manager and, optionally, to configure an email server. Information about the second host will appear on the page only if Configure Second Instances Topology was selected in the Node Topology Configuration Page.

Oracle Identity Manager Configuration Parameters

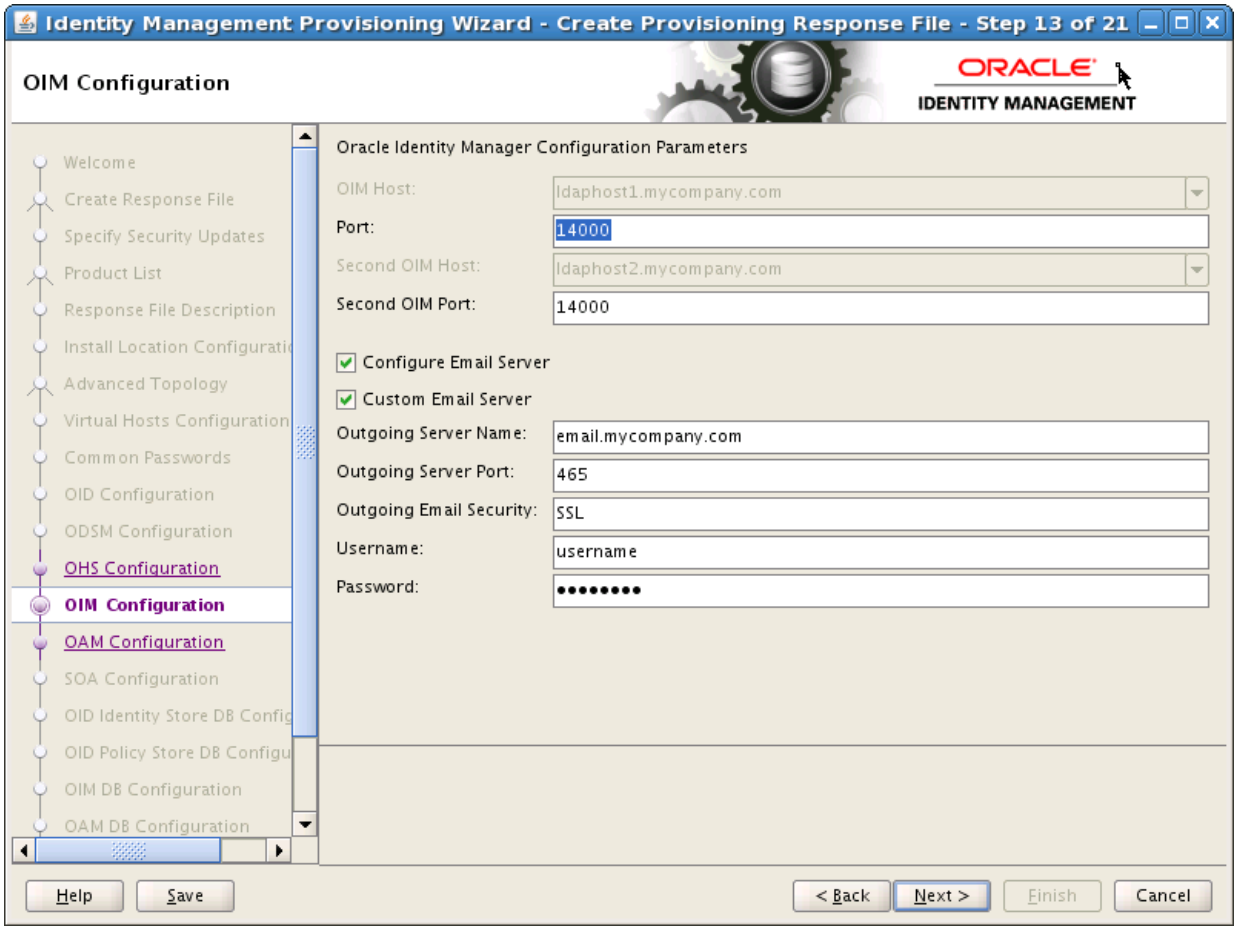
- **OIM Host**: This field is purely informational. The value is determined by the host entered in the Node Topology Configuration Page.
- **Port**: Specify the port to be used by the Oracle Identity Manager managed servers.

  > **Tip:** This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Identity Management Port Numbers -> IDMDomain OIM.

- **Second OIM Host**: This field is purely informational. The value is determined by the host entered in the Node Topology Configuration Page.
- **Second OIM Port**: Specify the port to be used by the Oracle Identity Manager managed servers.
- **Configure Email Server**: Select to configure the default email server on Linux. If you select this option on Windows, you must also select **Custom Email Server**.
- **Custom Email Server**: Select to configure a custom email server. On Windows, you must select this option if you selected **Configure Email Server**.
- **Outgoing Server Name**: Specify the name of your outgoing email server, for example: mail.mycompany.com
- **Outgoing Server Port**: Specify the port that your outgoing email server uses. This is typically 465.

  > **Tip:** This value is available in the *Oracle Fusion Applications Installation Workbook* - Environment tab -> Email Server -> SMTP Server Port.

- **Outgoing Email Security**: The security used by SMTP server. Possible values are `None`, `TLS` and `SSL`.
- **Username**: If you require a username to authenticate with the email server, enter that username.
- **Password**: Enter the password for the username.



Click **Next** to continue.

10.2.1.15 OAM Configuration Page

Use the OAM Configuration page to select installation options for Oracle Access Manager. Information about the second host will appear on the page only if Configure Second Instances Topology was selected in the Node Topology Configuration Page.

Oracle Access Manager Configuration Parameters

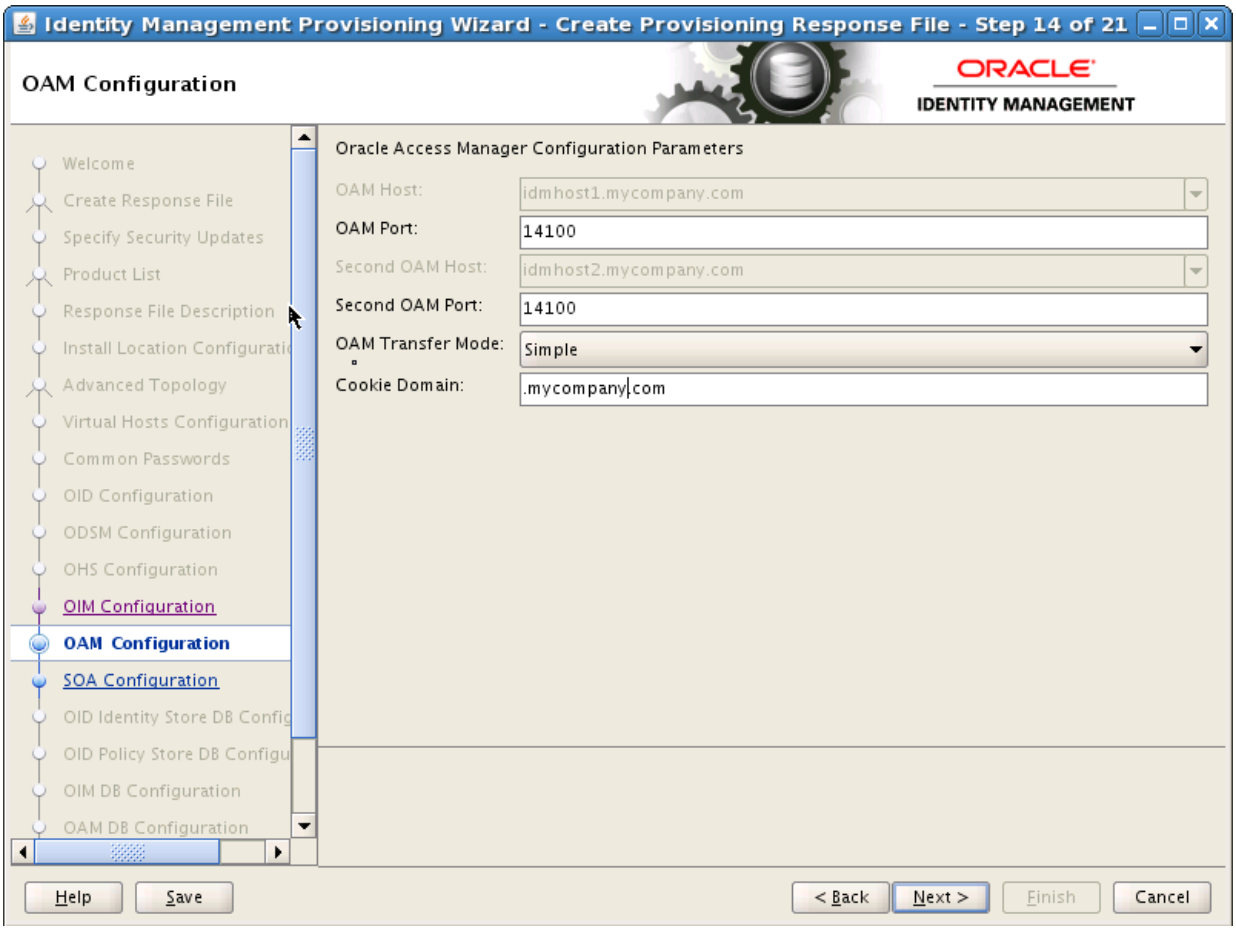
- **OAM Host**: This field is purely informational. The value is determined by the host entered in the Node Topology Configuration Page.
- **OAM Port**: Specify the port number of the first instance.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Identity Management Port Numbers -> IDMDomain OAM.

- **Second OAM Host**: This field is purely informational. The value is determined by the host entered in the Node Topology Configuration Page.
- **Second OAM Port**: Specify the port number of the second instance.
- **OAM Transfer Mode**: Specify the transfer mode to be used by Oracle Access manager. This must be `Open` on AIX and `Simple` on other platforms.

- **Cookie Domain**: Specify the cookie domain. For example: `.mycompany.com`

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Environment tab -> Environment Info -> Domain name.



Click **Next** to continue.

10.2.1.16 SOA Configuration Page

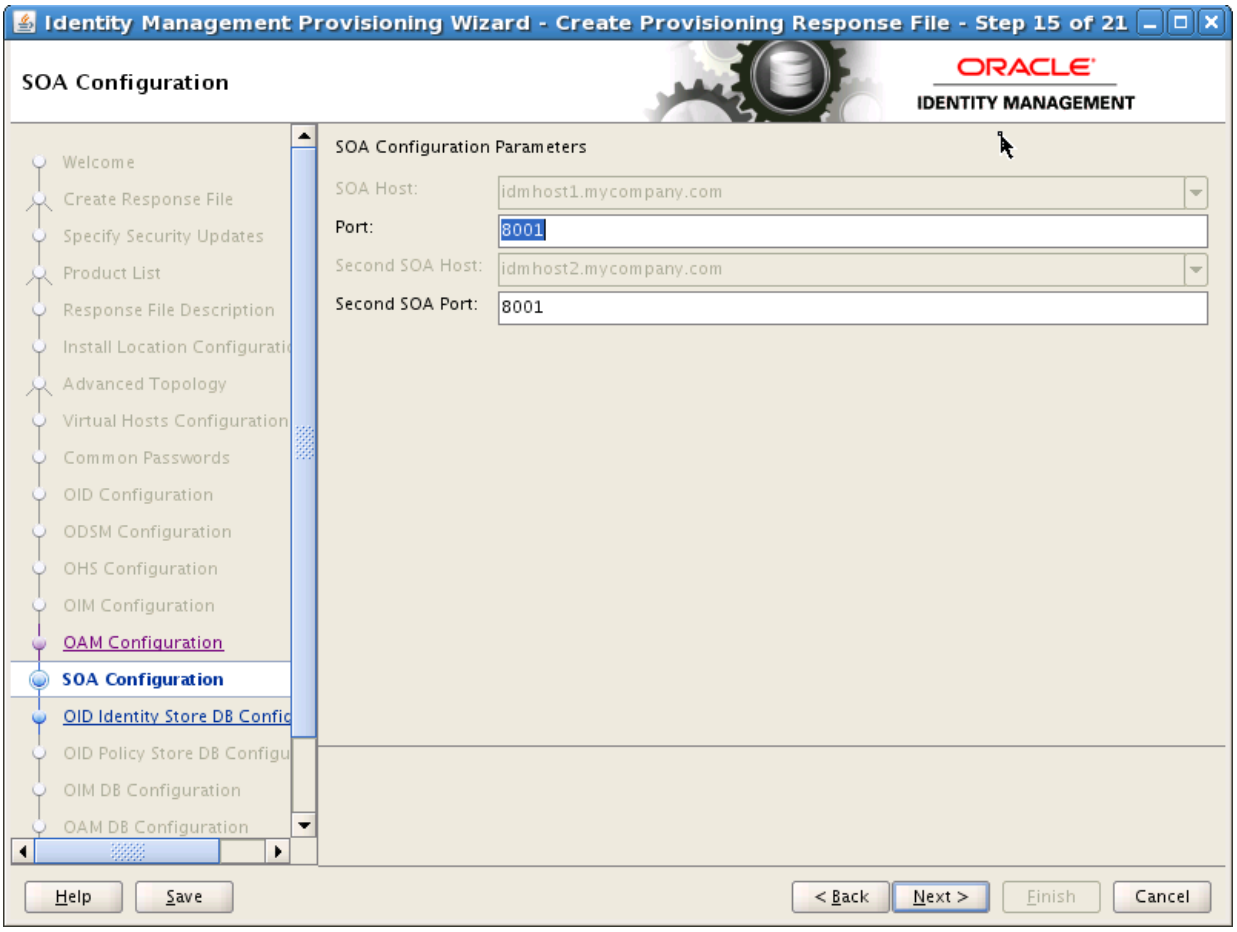
Use the SOA Configuration page to enter the ports to be used by the Oracle SOA Suite Managed servers. Information about the second host will appear on the page only if Configure Second Instances Topology was selected in the Node Topology Configuration Page.

SOA Configuration Parameters

- **SOA Host**: This field is purely informational
- **Port**: This field specifies the port for the first Oracle SOA Suite instance. You can change this.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Identity Management Port Numbers -> IDMDomain SOA.

- **Second SOA Host**: This field is purely informational.
- **Second SOA Port**: This field specifies the port for the second Oracle SOA Suite instance. You can change this value.



Click **Next** to continue.

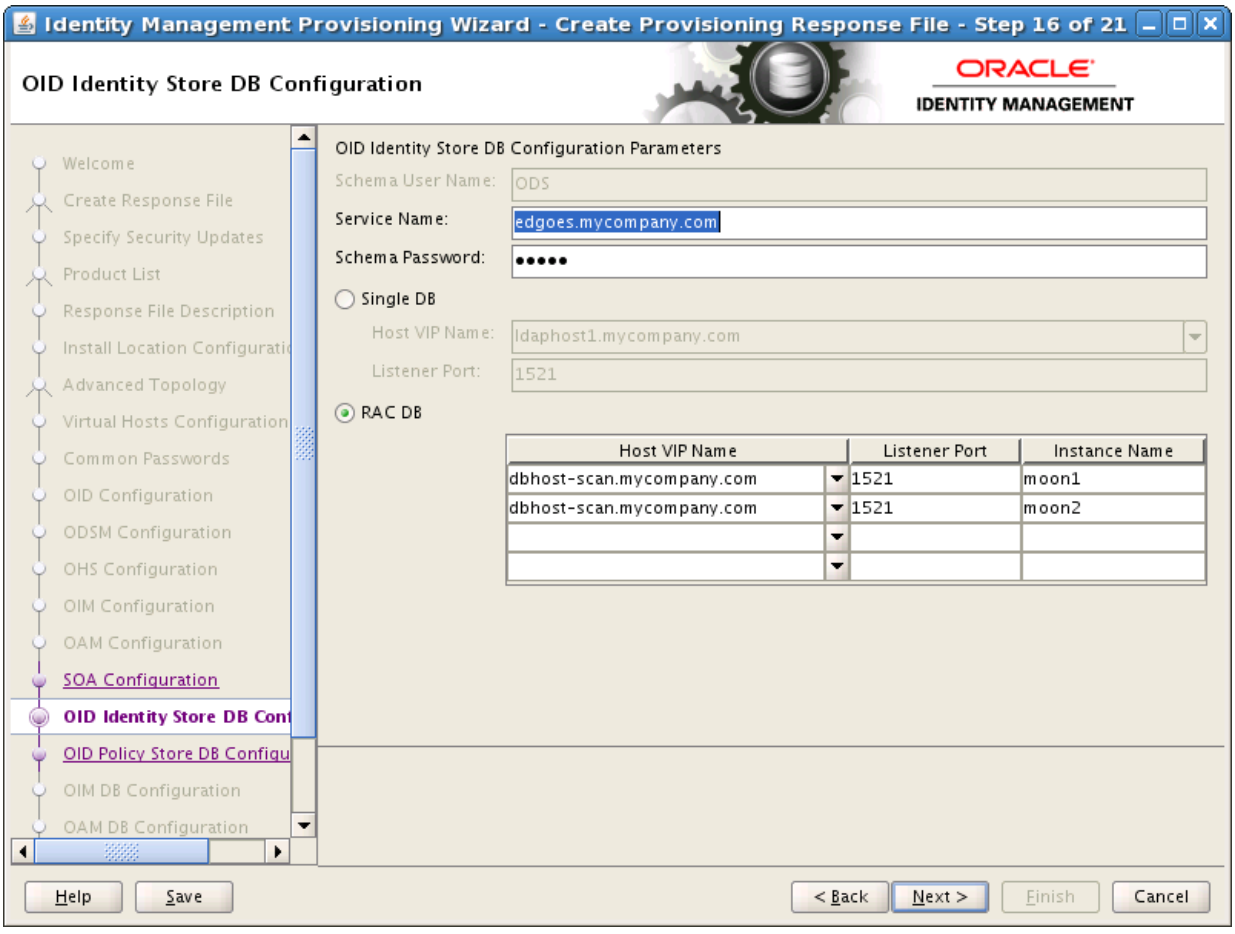
10.2.1.17 OID Identity Store DB Configuration Page

Use the OID Identity Store DB Configuration page to enter the database connection details for your Oracle Internet Directory Database.

OID Identity Store DB Configuration Parameters

> **Tip:** These values are available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> IDM Database or OID Database (optional).
>
> Depending on the topology decisions made during the planning phase (Section 4.4.2.5, "Oracle Identity Management Split Database Configuration") you may have one (IDMDB) or two (OIDDB and IDMDB) Oracle Identity Management database(s). If you have an OIDDB, which is specific for OID, specify the details here. Otherwise use the information for the single IDMDB.

- **Schema User Name**: This field specifies the name of the Oracle Internet Directory schema user, ODS. You cannot change this name.
- **Service Name**: Specify the service name of the database service, for example: idmdb.mycompany.com
- **Schema Password**: Specify the password you used when creating the Oracle Internet Directory schema using the Oracle Fusion Middleware Repository Creation Utility (Oracle Fusion Middleware RCU) when creating the FA_OIM schema.
- **Single DB**: Select if you are using a single Oracle Database.
  - **Host VIP Name**: Specify the host name of the Oracle Database.
  - **Listener Port**: Specify the database listener port.
- **RAC DB**: Select if you are using an Oracle Real Application Clusters (RAC) Database. Up to four RAC instances are supported.
  - **Host VIP Name**: Specify the host name of the Oracle RAC Database instance. If you are using Oracle Database 11.2, this must be the SCAN address.
  - **Listener Port**: Specify the database listener port
  - **Instance Name**: Specify the database instance name, for example, idmdb1.

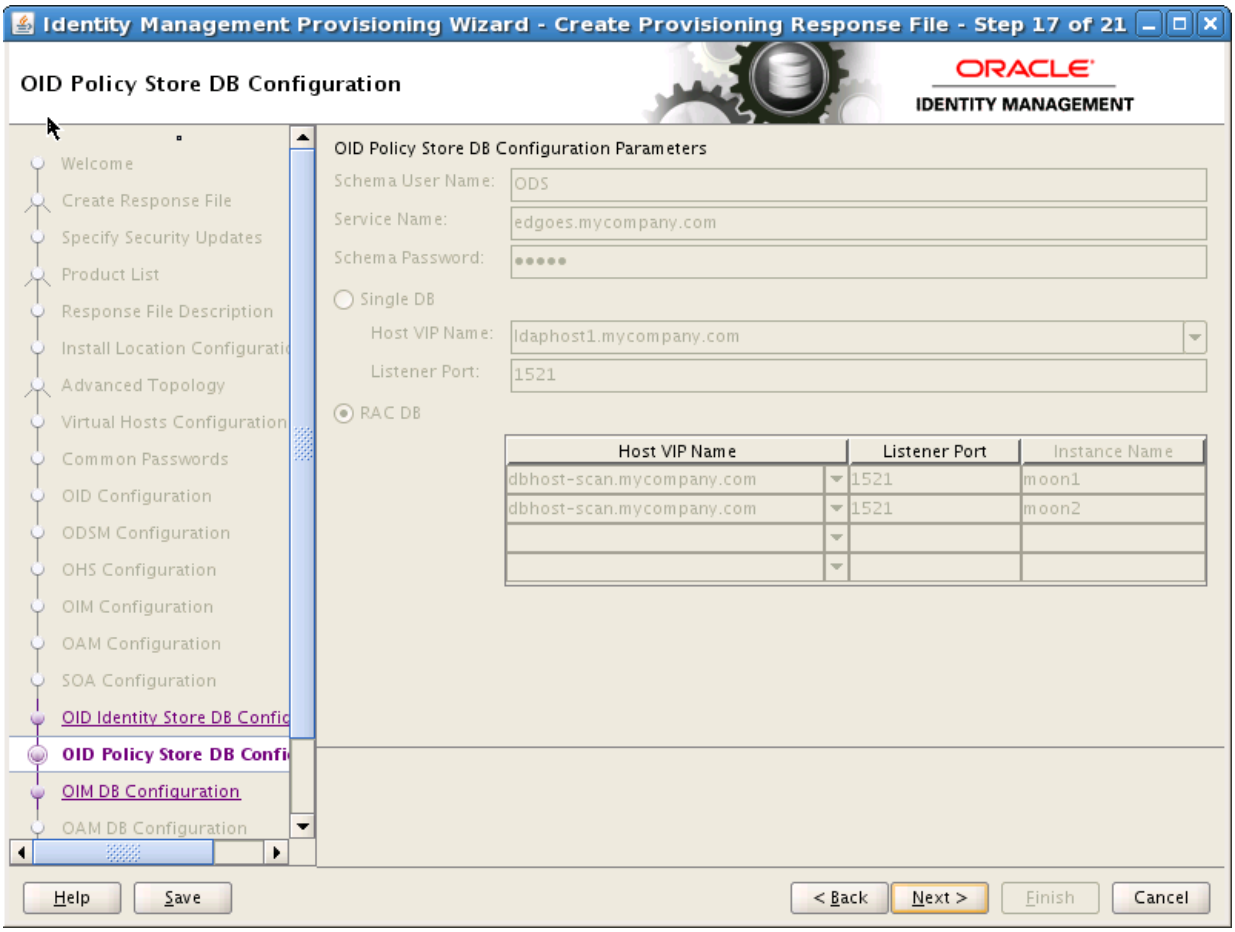


Click **Next** to continue.

10.2.1.18 OID Policy Store DB Configuration Page

The OID Policy Store DB Configuration page cannot be edited. The values are purely informational and are the same as those entered on the OID Identity Store DB Configuration Page.

- **Schema User Name**: The name of the Oracle Internet Directory schema user, ODS.
- **Service Name**: The service name of the database service, for example: idmdb.mycompany.com
- **Schema Password**: The password you used when creating the Oracle Internet Directory schema using the Oracle Fusion Middleware RCU when creating the FA_OAM schema.
- **Single DB**: Selected if you are using a single Oracle Database.
  - **Host VIP Name**: The host name of the Oracle Database.
  - **Listener Port**: The database listener port.
- **RAC DB**: Selected if you are using an Oracle RAC Database. Up to four RAC instances are supported.
  - **Host VIP Name**: The host name of the RAC database instance. If you are using Oracle Database 11.2, this must be the SCAN address.
  - **Listener Port**: The database listener port.
  - **Instance Name**: The database instance name, for example, idmdb1.



Click **Next** to continue.

10.2.1.19 OIM DB Configuration Page

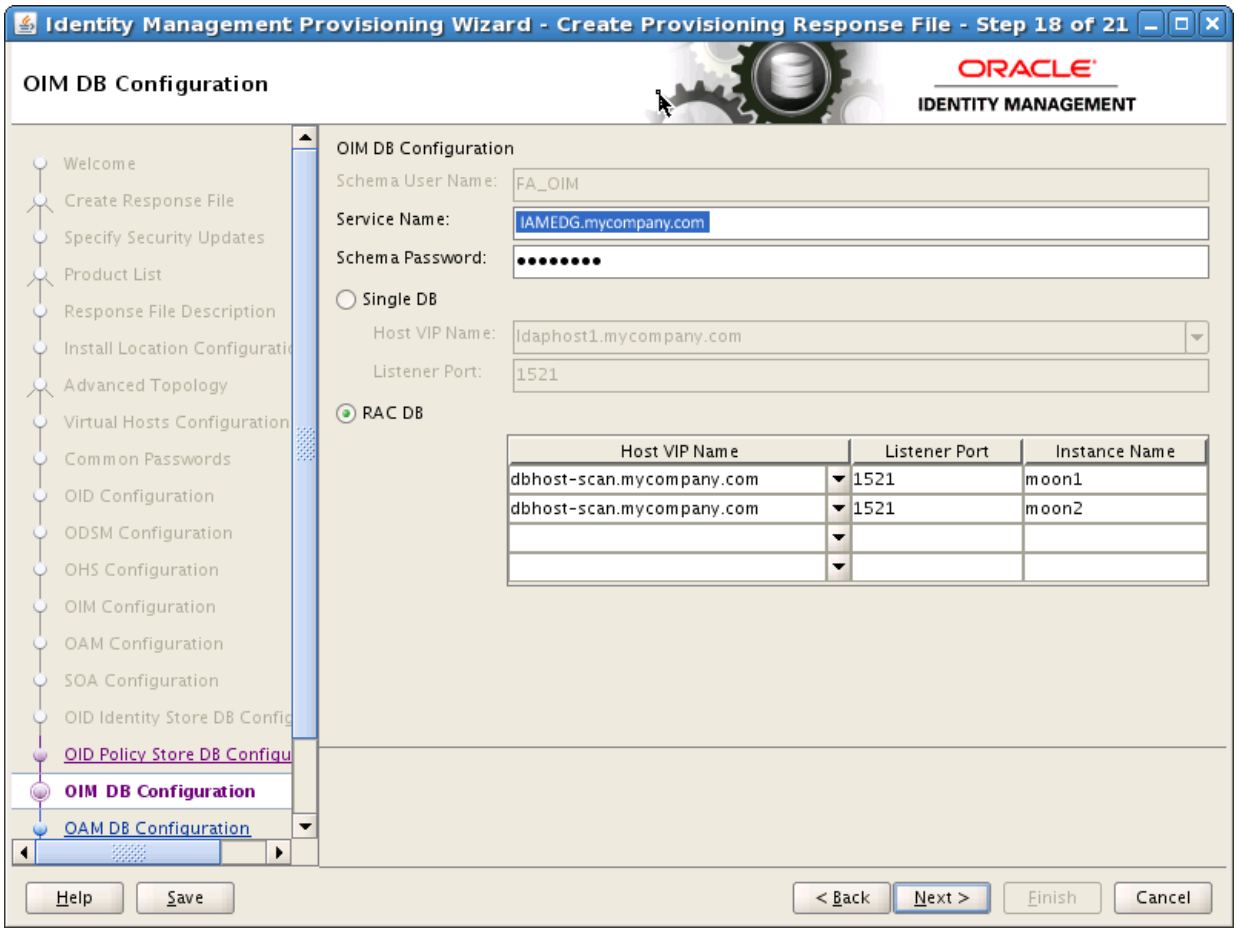
Use the OIM DB Configuration page to enter information about the database that contains the schemas for Oracle Identity Manager, Oracle SOA Suite, Oracle Access Manager, and Oracle Identity Federation.

OIM DB Configuration Page

- **Schema User Name**: This field specifies the name of the schema user, `FA_OIM`. You cannot change this name.
- **Service Name**: Specify the service name of the database service, for example: idmdb.mycompany.com

  > **Tip:** This value is available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> IDM Database -> IDM DB Service Name.

- **Schema Password**: For creating the FA_OIM schema, specify the password you used when creating the Oracle Internet Directory schema using the Oracle Fusion Middleware RCU.
- **Single DB**: Select if you are using a single Oracle Database.
  - **Host VIP Name**: Specify the host name of the Oracle Database.
  - **Listener Port**: Specify the database listener port.
- **RAC DB**: Select if you are using an Oracle RAC Database.
  - **Host VIP Name**: Specify the host name of the RAC database instance. If you are using Oracle Database 11.2, this must be the SCAN address.
  - **Listener Port**: Specify the database listener port.
  - **Instance Name**: Specify the database instance name, for example, idmdb1.



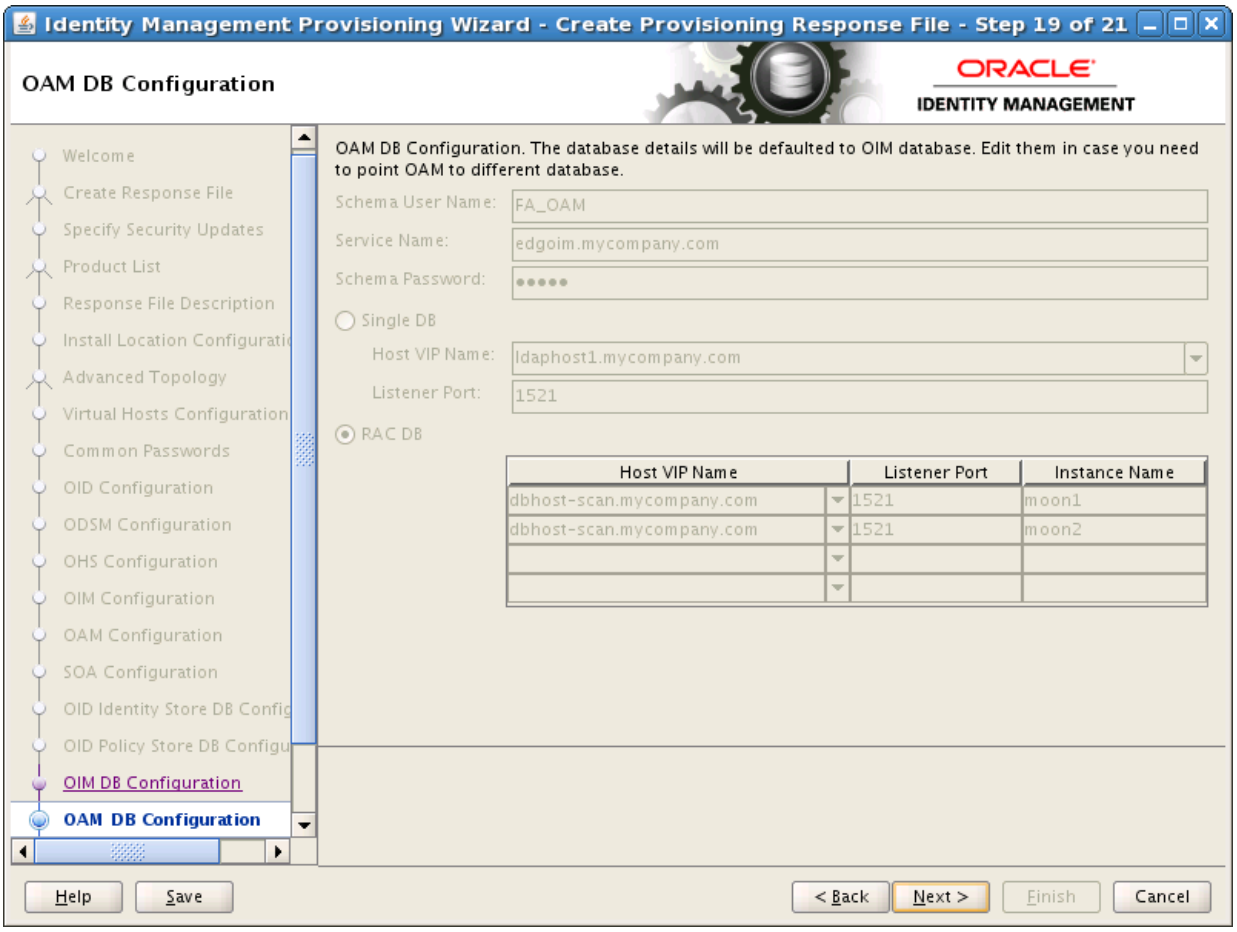
Click **Next** to continue.

10.2.1.20 OAM DB Configuration Page

The OAM DB Configuration page cannot be edited. The values are purely informational and are the same as those entered on the OIM DB Configuration Page, except for the **Schema User Name**.

- **Schema User Name**: The name of the schema user, `FA_OAM`.
- **Service Name**: The service name of the database service, for example: idmdb.mycompany.com
- **Schema Password**: For creating the FA_OAM schema, specify the password you used when creating the Oracle Internet Directory schema using the Oracle Fusion Middleware RCU.
- **Single DB**: Selected if you are using a single Oracle Database.
  - **Host VIP Name**: The host name of the Oracle Database.
  - **Listener Port**: Specify the database listener port.
- **RAC DB**: Selected if you are using an Oracle RAC Database. Up to four instances are supported.
  - **Host VIP Name**: The host name of the RAC database instance. If you are using Oracle Database 11.2, this must be the SCAN address.

- **Listener Port**: The database listener port.
- **Instance Name**: The database instance name, for example, idmdb1.



Click **Next** to continue.

10.2.1.21 Load Balancer Page

The Load Balancer page is editable only if you have selected the **EDG topology** option.

The Load Balancer page is arranged in the following sections:

- HTTP/HTTPS Load Balancer Details
- LDAP Load Balancer Details

HTTP/HTTPS Load Balancer Details

The HTTP/HTTPS Load Balancer Details section of the Load Balancer Configuration page enables you to enter configuration information about the HTTP/HTTPS Load Balancer.

- **Endpoint**: This column lists the HTTP/HTTPS Load Balancer endpoints. These are:
  - **Admin**: Admin Virtual Host, for example: `admin.mycompany.com`

Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> IDM Admin -> Internal Name, Internal Port.

– **Internal Callbacks**: Internal call back virtual host, for example: `Identity Managementinternal.mycompany.com`

Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> IDM -> Internal Name, Internal Port.

– **SSO**: Main application entry point, for example: `sso.mycompany.com`.

Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints -> IDM -> External Name, External Port.

- **Virtual Host Name**: Specify the virtual host name that corresponds with this endpoint. Examples are shown in the **Endpoint** descriptions.
- **Port**: Specify the port used by the endpoint. This port will be either HTTP or HTTPS, depending on whether the SSL box is checked or not.
- **SSL**: Select this box if this endpoint will use SSL. This box is editable only for **Admin** endpoint.

Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - SSL and Certificates tab -> SSL Communication -> End User - -> IDM Admin HTTP Endpoint.

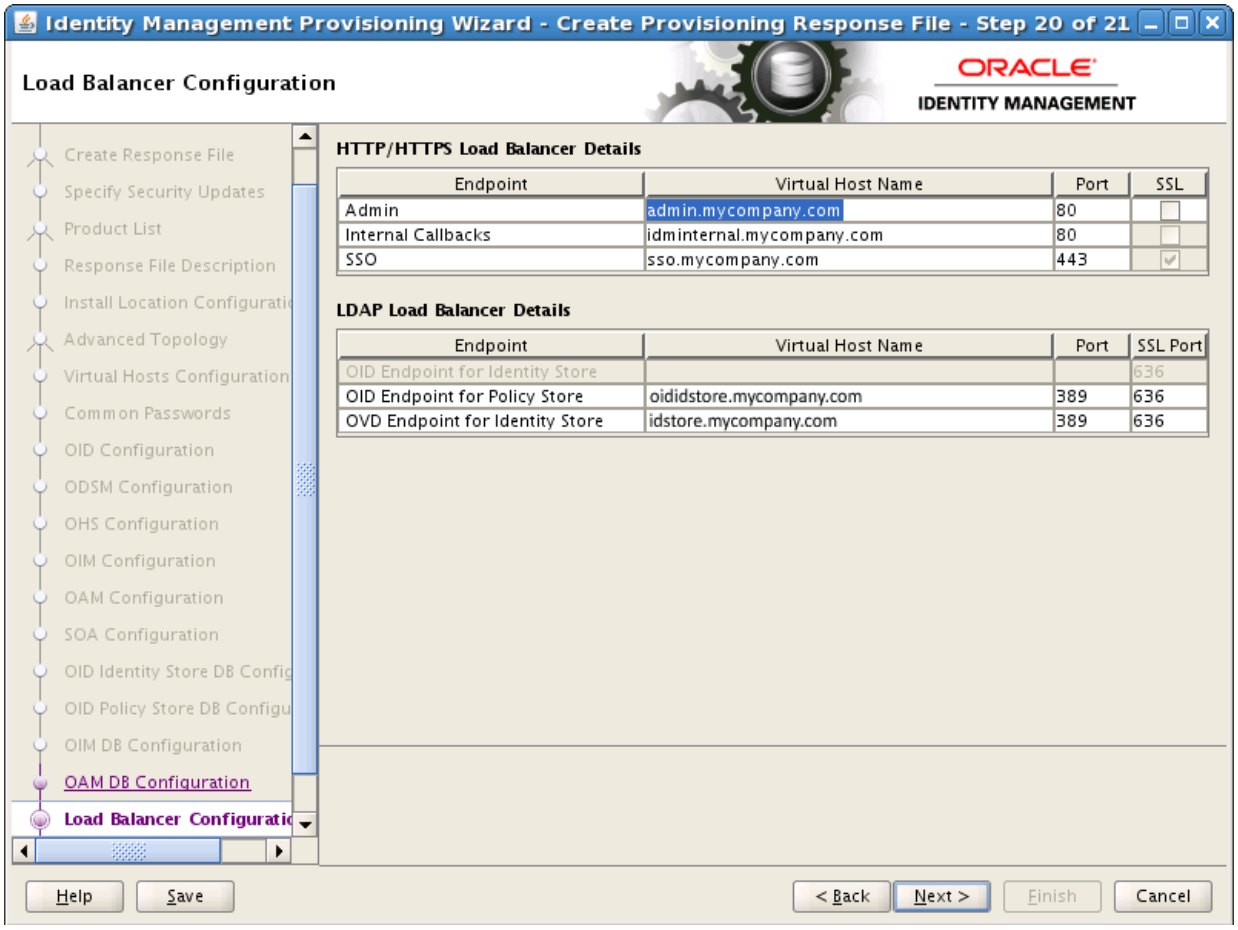
LDAP Load Balancer Details

The LDAP Load Balancer Details section of the Load Balancer Configuration page enables you to enter configuration information about the LDAP Load Balancer.

The **OID Endpoint for Identity Store** field is not editable because your Identity Store and Policy Store will be the same Oracle Internet Directory. See Section 4.5.1, "Identity Store Planning".

Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> LDAP Endpoints.

- **Endpoint**: This column lists the LDAP Load Balancer endpoints.
- **Virtual Host Name**: Specify the virtual host name that corresponds with this endpoint.
- **Port**: Specify the port used by the endpoint.
- **SSL Port**: Specify the SSL port used by the endpoint.

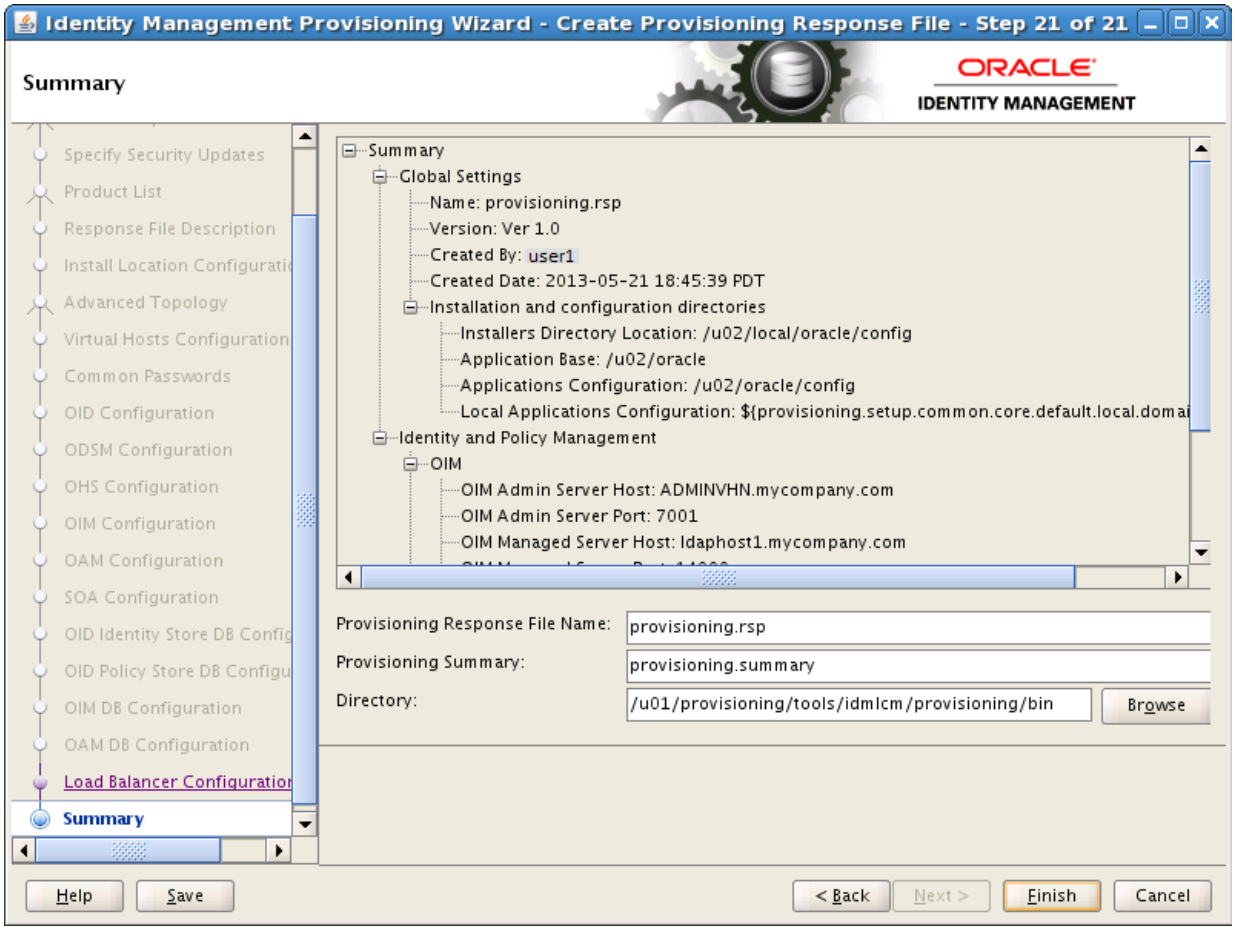


Click **Next** to continue.

10.2.1.22 Summary Page

Use the Summary page to view a summary of your selections and enter additional information.

- **Response File Name**: Provide the name of the response file to be created.
- **Provisioning Summary**: Provide the name of the provisioning summary file to be created.
- **Directory**: Specify the directory where you want to save the Provisioning Response File.



10.2.2 Copy Required Files to DMZ Hosts

The process described in this chapter creates a provisioning file in the directory you specified on the Summary screen in Step 22. This process also creates a folder named `responsefilename_data`, for example: `provisioning_data`. This folder contains `cwallet.sso`, which has encryption and decryption information.

The provisioning response file and the folder containing `cwallet.sso` must be available to each host in the topology. If you have a shared provisioning directory, then these files are automatically available. If, however, you have not shared your deployment directory, you must manually copy the deployment response file (`provisioning.rsp`) and the folder containing `cwallet.sso` (`provisioning_data`) to the same location on the DMZ hosts, WEBHOST1 and WEBHOST2.

Note: If the deployment response file and the folder containing cwallet.sso are not copied to the DMZ hosts, the deployment process might fail in the preverify phase.

10.3 Introduction to Performing Oracle Oracle Identity Management Provisioning

After you create the provisioning response file, you use it to provision an Oracle Identity Management environment.

There are eight stages to provisioning. These stages must be run in the following order:

1. Preverify - This checks that each of the servers being used in the topology satisfies the minimum requirements of the software being installed and configured.
2. Install - This installs all of the software and related patches present in Provisioning Repository.
3. Preconfigure - This does the following:
   - Creates OID and seeds it with Users/Groups.
   - Creates OVD
   - Configures ODSM
   - Creates the WebLogic Domain
   - Creates OHS instance
4. Configure - This does the following:
   - Associates the Policy Store to OID
   - Starts managed servers as necessary
   - Associates OAM with OID
   - Configure OIM
5. Configure-Secondary - This does the following:
   - Integrates Weblogic Domain with Web Tier
   - Register Web Tier with domain
   - Integrate OAM and OIM
6. Postconfigure - This does the following:
   - Register OID with Weblogic Domain
   - SSL Enable OID and OVD
   - Tune OID
   - Run OIM Reconciliation
   - Configure UMS Mail Server
   - Generate OAM Keystore
   - Configure OIF
   - Configure WebGate
7. Startup - This starts up all components in the topology
8. Validate - This performs a number of checks on the built topology to ensure that everything is working as it should be.

You specify the stage using the `-target` option to the `runIDMProvisioning.sh` or `runIDMProvisioning.bat` command. Each stage must be completed before the next stage can begin. Failure of a stage will necessitate a cleanup and restart.

Provisioning is accomplished by using either the command line or the Oracle Identity Management Provisioning Wizard.

10.3.1 Processing Order

You must process hosts in the following order. Each provisioning phase needs to be run only once on each host, even if multiple products are configured on a single host.

1. LDAP Host 1
2. LDAP Host 2 (if using the EDG topology with the **Configure second application instances** option)
3. Identity and Access Management Host 1
4. Identity and Access Management Host 2 (if using the EDG topology with the **Configure second application instances** option)
5. Web Host 1
6. Web Host 2 (if using the EDG topology with the **Configure second application instances** option)

10.3.2 Installation Phase Actions for Oracle Identity Management Components

During installation, the Provisioning Wizard performs actions that are associated with the Oracle Identity Management components you installed previously. This section contains a summary of those actions, arranged by the installation phase where the action is performed.

Provisioning phases

The wizard performs the following actions:

- Preverify phase

  Verifies the existence of the system administrators group (if it was declared as existing during the wizard interview) and the existence of the designated super user in the identity store.

- Preconfigure phase

  Prepares the Oracle Identity Management components for configuring as follows:

  - Uploads the LDIF files to the identity store. These files contain entries that represent the application administrator groups used to update the identity store.
  - Creates the system administrator group (according to what is indicated in the interview).
  - Makes the super user a member of the administrators group and all the application family directory groups.
  - Seeds the bootstrap of `AppID` and gives it membership in the system administrator group.

- Configure phase

  Configures the Oracle Identity Management components as follows:

  - Creates the Oracle Fusion Applications domains using the default Oracle WebLogic Server template, with the bootstrap `AppID` as an administrator.
  - Disables the default authenticator and enables the LDAP authenticator.
  - Starts the Oracle WebLogic Server domain using the bootstrap `AppID`.

- Postconfigure phase

Following configuration, the system administrator groups are assigned the appropriate enterprise roles at the product family level. Therefore, the super user has:

- Administrator privileges for all Oracle WebLogic Server domains and all middleware
- Functional setup privileges for all Oracle Fusion Applications offerings
- Administration privileges to Oracle Fusion Applications offerings, excluding transactional privileges

10.4 Performing Oracle Identity Management Provisioning

Provisioning is accomplished by using either the command line or the Oracle Identity Management Provisioning Wizard.

This section contains the following topics:

- Performing Provisioning by Running the Provisioning Commands
- Monitoring Provisioning Using the Oracle Identity Management Provisioning Wizard

10.5 Performing Provisioning by Running the Provisioning Commands

To use the command line, you must run the command `runIDMProvisioning.sh` or `runIDMProvisioning.bat` a number of times, specifying the provisioning stage with the `-target` option. You MUST complete each command, in order, before running the next command.

Before running the provisioning tool, set the following environment variables:

- Set `JAVA_HOME` to: *`REPOSITORY_LOCATION`*`/jdk6`
- Check whether the *`TNS_ADMIN`* environment variable is set on your Oracle Internet Directory hosts.

  ```
  env | grep TNS_ADMIN
  ```

  If it is set, unset it.

  Bash

  ```
  unset TNS_ADMIN
  ```

  Csh

  ```
  unsetenv TNS_ADMIN
  ```

- On UNIX systems, set the DISPLAY environment variable to an active and authorized display.

The command syntax for the provisioning tool on UNIX is:

```
runIDMProvisioning.sh -responseFile RESPONSE_FILE -target STAGE
```

The command syntax on Windows is:

```
runIDMProvisioning.bat -responseFile RESPONSE_FILE -target STAGE
```

Where:

RESPONSE_FILE is the provisioning response file. You specified the file name and directory on the Summary page when you ran the wizard to create the file. See Section 10.2.1.22, "Summary Page." The default value is *IDMLCM_HOME*/provisioning/bin/provisioning.rsp on UNIX and *IDMLCM_HOME*\provisioning\bin\provisioning.rsp on Windows.

STAGE is one of the stages listed in Section 10.3, "Introduction to Performing Oracle Oracle Identity Management Provisioning."

10.6 Monitoring Provisioning Using the Oracle Identity Management Provisioning Wizard

If you want to use the Oracle Identity Management Provisioning Wizard to monitor the progress of provisioning, follow these steps:

Note: ■For a single node topology, it is recommended that to use the Oracle Identity Management Provisioning Wizard for provisioning.

- For a multiple node topology, it is recommended to use the command line (runIDMProvisioning) for provisioning.
- You can use the Oracle Identity Management Provisioning Wizard to monitor the provisioning for a multiple node install. However, you can run the Oracle Identity Management Provisioning Wizard only on the primordial host, IDMHOST1.

1. Set JAVA_HOME to: *REPOSITORY_LOCATION*/jdk6
2. Invoke idmProvisioningWizard.sh (on Linux or UNIX) or idmProvisioningWizard.bat (on Windows).
3. When you get to the Oracle Identity Management Installation Options page, select **Provision an Identity Management Environment** and specify the provisioning.rsp file you created in Chapter 10.2, "Creating an Oracle Identity Management Provisioning Profile."

Then proceed as described in the following sections.

Note: In the Prerequisite Checks, Installation, Preconfigure, Configure, Configure Secondary, Postconfigure, and Startup pages, the Status of each build is indicated by one of these icons:

- **Block**: Processing has not yet started for the named phase.
- **Clock**: Performing the build for a phase.
- **Check mark**: The build was completed successfully.
- **x** mark: The build has failed for this phase. You must correct the errors before you can continue.

Click an **x** to display information about failures. Click the host-level **Log** file for details about this phase. Click a build **Log** file to see details specific to that build.

In case of errors, you must manually clean up everything. Kill all running processes, delete the directories, rerun RCU, and start over from the beginning.

10.6.1 Identity Management Installation Options Page

Select **Provision an Identity Management Environment** to use an existing provisioning response file to provision the environment.

If your Oracle Identity Management topology spans multiple hosts, you must make the provisioning response file accessible to all hosts (preferrably by including it on shared storage) and run the provisioning tool on each host other than the primordial host, where the Oracle Identity Management Provisioning Wizard is running. This is explained in more detail on the Installation page.

In the **Response File** field, specify the path name of the file you want to use, either by typing it in the field or by clicking the **Browse** button, navigating to the desired file, and selecting it.

Click **Next** to continue.

10.6.2 Install Location Configuration Page

The Install Location Configuration page allows you to modify the details entered previously when you created the response file. For details about the settings on this page, see Section 10.2.1.7, "Install Location Configuration Page".

Installation and Configuration.

- **Software Repository Location**: Specify the location of the software repository, either by typing it in the field or by clicking the **Browse** button, navigating to the desired location, and selecting it.
- **Software Installation Location**: Specify the location on shared storage where you want the Middleware Home to be placed, either by typing it in the field or by clicking the **Browse** button, navigating to the desired location, and selecting it.
- **Shared Configuration Location**: Specify the shared configuration location, either by typing it in the field or by clicking the **Browse** button, navigating to the desired location, and selecting it.
- **Enable Local Configuration Location**: Do not select this checkbox if you are provisioning a single host environment.

  Select this checkbox if you want Managed Servers to run from a local disk on the host, visible only to the processes running on that host. If you enable this option, the Oracle Identity Management Provisioning Wizard copies the domain configuration from the shared location and places it on the local disk you specify. This configures all Managed Servers to run from the non-networked location.

  – **Local Configuration Location**: Specify the location for the local domain directory that you want to set up, either by typing it in the field or by clicking the **Browse** button, navigating to the desired location, and selecting it. This field is required if you selected **Enable Local Applications Configuration**. The specified directory must initially be empty.

10.6.3 Review Provisioning Configuration Page

The Review Provisioning Configuration page enables you to select configurations you want to review. Select a configuration and click **Next** to view the corresponding configuration page.

- **Node Topology Configuration**
- **Virtual Hosts Configuration**
- **Common Passwords**
- **OID: Oracle Internet Directory Configuration**
- **ODSM: Oracle Directory Services Manager Configuration**
- **OHS: Oracle HTTP Server Configuration**
- **OAM: Oracle Access Manager Configuration**
- **OIM: Oracle Identity Manager Configuration**
- **Load Balancer Configuration**

Click **Next** to continue.

10.6.4 Summary Page

Use the Summary page to view a summary of your selections and enter additional information.

Review the information displayed to ensure that the installation details are what you intend. To make changes, click **Back** to return to previous screens in the interview.

Click **Next** to continue.

10.6.5 Prerequisite Checks Page

Use the Prerequisite Checks page to observe the progress of the preverification steps. During this stage, the Oracle Identity Management Provisioning Wizard checks for the basic prerequisites, such as free disk space, port availability, and Database connections.

See the note at the beginning of Section 10.6 for information about viewing build status on this page.

Click **Next** to continue.

10.6.6 Installation Page

Use the Installation page to install the Oracle Fusion Middleware products. The host is marked with a Home symbol in the Host column. The Domains column lists the domains deployed in the new environment.

For the EDG topology, if you are not sharing your provisioning directory onto the WEBHOSTs, you must manually copy the following directories from IDMHOST1 to the local provisioning directories on those hosts. You must do this BEFORE running the install on those hosts and AFTER completing the install phase on IDMHOST2.

```
IDM_CONFIG/lcmconfig/topology
```

```
IDM_CONFIG/lcmconfig/credconfig
```

For example:

```
scp -r IDM_CONFIG/lcmconfig/topology WEBHOST1:IDM_CONFIG/lcmconfig/
```

```
scp -r IDM_CONFIG/lcmconfig/credconfig WEBHOST1:IDM_CONFIG/lcmconfig/
```

During this stage, the Oracle Identity Management Provisioning Wizard installs the software bits and applies the patches present in the repository.

In a terminal session on the hostprimary, secondary, and DMZ host (if present), run the install phase with the command:

Linux or UNIX:

```
runIDMProvisioning.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target install
```

Windows:

```
runIDMProvisioning.bat  -responseFile IDMLCM_
HOME\provisioning/bin/provisioning.rsp -target install
```

See the note at the beginning of Section 10.6 for information about viewing build status on this page.

After performing the install phase on the primordial host (IDMHOST1), you must download Patch 16708003 and apply it on IDMHOST1.

Click **Next** to proceed.

10.6.7 Preconfigure Page

During this stage, the Oracle Identity Management Provisioning Wizard configures Oracle Internet Directory, Oracle Virtual Directory, and Oracle Directory Services Manager. It also creates the domain and extends it for all the necessary components.

In a terminal session on the hostprimary, secondary, and DMZ host (if present), run the preconfigure phase with the command:

```
runIDMProvisioning.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target preconfigure
```

Linux or UNIX:

```
runIDMProvisioning.bat  -responseFile IDMLCM_
HOME\provisioning/bin/provisioning.rsp -target preconfigure
```

Windows:

Note: Each new phase must run sequentially; that is, you cannot start a new phase until the previous phase has been completed successfully on all the hosts.

See the note at the beginning of Section 10.6 for information about viewing build status on this page.

Note: If a DMZ host is present, recopy the response file to the DMZ host.

Click **Next**. The Oracle Identity Management Provisioning Wizard starts the configure phase on the primordial host and displays the Configure screen.

10.6.8 Configure Page

During this stage, the Oracle Identity Management Provisioning Wizard performs OIM configuration.

See the note at the beginning of Section 10.6 for information about viewing build status on this page.

Click **Next**. The Oracle Identity Management Provisioning Wizard starts the Configure-secondary phase on the primordial host and displays the Configure Secondary screen.

10.6.9 Configure Secondary Page

During this stage, the Oracle Identity Management Provisioning Wizard performs Oracle Identity Manager-Oracle Access Manager integration.

See the note at the beginning of Section 10.6 for information about viewing build status on this page.

Click **Next**. The Oracle Identity Management Provisioning Wizard starts the Postconfigure phase and displays the Postconfigure screen.

10.6.10 Postconfigure Page

During this stage, the Oracle Identity Management Provisioning Wizard performs tuning and enables the environment for SSL communication. Oracle Identity Federation is configured in this stage.

Copying WebGate Configuration Files to WEBHOST1 and WEBHOST2

This is applicable only for EDG topology when the OHS is on a DMZ host.

When configuring WebGate during the postconfigure stage, the provisioning tool requires access to files created on the primordial host. So BEFORE postconfigure is run on WEBHOST1 and WEBHOST2, you must copy the entire directory *IDM_CONFIG/domains/IDMDomain/output* to the same location on WEBHOST1 and WEBHOST2.

For example:

`scp -r IDMHOST1:$`*IDM_CONFIG/domains/IDMDomain*`/output WEBHOST1:$`*IDM_CONFIG/domains/IDMDomain*

Note: Before making the copy, you might need to manually create the directory *IDM_CONFIG/domains/IDMDomain* on WEBHOST1 and WEBHOST2. After provisioning is complete, you can remove this directory from WEBHOST1 and WEBHOST2.

See the note at the beginning of Section 10.6 for information about viewing build status on this page.

Click **Next**. The Oracle Identity Management Provisioning Wizard starts the Startup phase and displays the Startup screen.

10.6.11 Startup Page

During this stage, the Oracle Identity Management Provisioning Wizard starts or restarts all the services except for Oracle Identity Federation. If you plan to use Oracle Identity Federation, you can run it manually as a post-installation task described in Section 16.10.3, "Configuring Oracle Identity Federation".

The Domains column lists the domains deployed in the new environment.

See the note at the beginning of Section 10.6 for information about viewing build status on this page.

Click **Next**. The Oracle Identity Management Provisioning Wizard starts the Validate phase and displays the Validation screen.

10.6.12 Validation Page

During this stage, the Oracle Identity Management Provisioning Wizard performs the basic validations, such as server status and Oracle Internet Directory connectivity.

The host is marked with a Home symbol in the Host column. The Domains column lists the domains deployed in the new environment.

See the note at the beginning of Section 10.6 for information about viewing build status on this page.

Click **Next**. The Oracle Identity Management Provisioning Wizard starts the Validate phase on the host and displays the Validation screen.

10.6.13 Install Complete

This page appears after provisioning has completed successfully. It shows a summary of the products that have been installed.

Click **Finish** to save the summary and exit the Oracle Identity Management Provisioning Wizard.

10.7 Performing Mandatory Oracle Identity Management Post-Installation Tasks

This section describes tasks you must perform after provisioning.

10.7.1 Creating ODSM Connections to Oracle Virtual Directory

Before you can manage Oracle Virtual Directory you must create connections from ODSM to each of your Oracle Virtual Directory instances. To do this, proceed as follows:

1. Access ODSM through the load balancer at: `http://ADMIN.mycompany.com/odsm`
2. To create connections to Oracle Virtual Directory, follow these steps. Create connections to each Oracle Virtual Directory node separately. Using the Oracle Virtual Directory load balancer virtual host from ODSM is not supported:
   a. Create a direct connection to Oracle Virtual Directory on LDAPHOST1 providing the following information in ODSM:

      `Host`: `LDAPHOST1.mycompany.com`

      `Port`: `8899` (The Oracle Virtual Directory proxy port, *`OVD_ADMIN_PORT`*)

      Enable the SSL option.

      `User`: `cn=orcladmin`

      `Password`: password_to_connect_to_OVD

   b. Create a direct connection to Oracle Virtual Directory on LDAPHOST2 providing the following information in ODSM:

      `Host`: `LDAPHOST2.mycompany.com`

      `Port`: `8899` (The Oracle Virtual Directory proxy port)

      Enable the SSL option.

      `User`: `cn=orcladmin`

      `Password`: password_to_connect_to_OVD

10.7.2 Passing Configuration Properties File to Oracle Fusion Applications

Oracle Fusion Applications requires a property file which details the Oracle Identity Management deployment. After provisioning, this file can be found at the following location:

`IDM_CONFIG``/fa/idmsetup.properties`

10.8 Validating Provisioning

The provisioning process includes several validation checks to ensure that everything is working correctly. This section describes additional checks that you can perform for additional sanity checking

10.8.1 Validating the Administration Server

Validate the WebLogic Administration Server as follows.

10.8.1.1 Verify Connectivity

Verify that you can access the administration console by accessing the URL:

`http://admin.mycompany.com/console and logging in as the user weblogic_idm`

Verify that all managed servers are showing a status of Running.

Verify that you can access Oracle Enterprise Manager Fusion Middleware Control by accessing the URL:

`http://admin.mycompany.com/em and logging in as the user weblogic_idm`

10.8.2 Validating the Oracle Access Manager Configuration

To validate that this has completed correctly.

1. Access the OAM console at: `http://ADMIN.mycompany.com/oamconsole`
2. Log in as the Oracle Access Manager user.
3. Click the **System Configuration** tab
4. Expand **Access Manager Settings - SSO Agents - OAM Agents**.
5. Click the open folder icon, then click **Search**.
6. You should see the WebGate agents `Webgate_IDM`, `Webgate_IDM_11g` and `IAMSuiteAgent`.

10.8.3 Validating Oracle Directory Services Manager (ODSM)

This section describes how to validate the Application Tier configuration.

10.8.3.1 Validating Browser Connection to ODSM Site

Follow these steps to validate that you can connect the Oracle Directory Services Manager site in a browser:

1. In a web browser, verify that you can connect to Oracle Directory Services Manager (ODSM) at:

   `http://`*`HOSTNAME`*`.mycompany.com:`*`port`*`/odsm`

   For example, on IDMHOST1, enter this URL, where `7005` is *`ODSM_PORT`*

   `http://IDMHOST1.mycompany.com:7005/odsm`

   and on IDMHOST2, enter this URL:

   `http://IDMHOST2.mycompany.com:7005/odsm`

2. In a web browser, verify that you can access ODSM through the load balancer address:

   `http://ADMIN.mycompany.com/odsm`

10.8.3.2 Validating ODSM Connections to Oracle Internet Directory

Validate that Oracle Directory Services Manager can create connections to Oracle Internet Directory.

Create a connection to the Oracle Internet Directory on each ODSM instance separately. Even though ODSM is clustered, the connection details are local to each node. Proceed as follows:

1. Launch Oracle Directory Services Manager from IDMHOST1:

   `http://IDMHOST1.mycompany.com:7005/odsm`

2. Create a connection to the Oracle Internet Directory virtual host by providing the following information in ODSM:
   - Server: `OIDSTORE.mycompany.com`
   - Port: `636` (*`LDAP_LBR_SSL_PORT`*)
   - Enable the SSL option
   - User: `cn=orcladmin`
   - Password: *`ldap-password`*
3. Launch Oracle Directory Services Manager from IDMHOST2.

   Follow Step 3 to create a connection to Oracle Internet Directory from IDMHOST2

   `http://IDMHOST2.mycompany.com:7005/odsm`

4. Create a connection to the Oracle Internet Directory virtual host by providing the corresponding information in ODSM

> **Note:** Accept the certificate when prompted.

10.8.4 Validating Oracle Identity Manager

This section describes how to validate Oracle Identity Manager.

10.8.4.1 Validating the Oracle Internet Directory Instances

To validate the Oracle Internet Directory instances, ensure that you can connect to each Oracle Internet Directory instance and the load balancing router using these commands:

> **Note:** Ensure that the following environment variables are set before using `ldapbind`:
>
> - *`ORACLE_HOME`* (set to *`IDM_BASE`*`/products/dir/idm`)
> - *`OID_ORACLE_INSTANCE`*
> - *`PATH`* - The following directory locations should be in your *`PATH`*:
>
>   *`ORACLE_HOME`*`/bin`
>
>   *`ORACLE_HOME`*`/ldap/bin`
>
>   *`ORACLE_HOME`*`/ldap/admin`

```
ldapbind -h LDAPHOST1.mycompany.com -p 3060 -D "cn=orcladmin" -q
ldapbind -h LDAPHOST1.mycompany.com -p 3131-D "cn=orcladmin" -q -U 1
ldapbind -h LDAPHOST2.mycompany.com -p 3060 -D "cn=orcladmin" -q
ldapbind -h LDAPHOST2.mycompany.com -p 3131-D "cn=orcladmin" -q -U 1

ldapbind -h OIDIDSTORE.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h OIDIDSTORE.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
```

Note: The -q option prompts the user for a password. LDAP Tools have been modified to disable the options -w *password* and -P *password* when the environment variable LDAP_PASSWORD_PROMPTONLY is set to TRUE or 1. Use this feature whenever possible.

10.8.4.2 Validating the Oracle Virtual Directory Instances

To validate the Oracle Virtual Directory instances, ensure that you can connect to each Oracle Virtual Directory instance and the load balancing router using these ldapbind commands:

```
ldapbind -h LDAPHOST1.mycompany.com -p 6501 -D "cn=orcladmin" -q
ldapbind -h LDAPHOST2.mycompany.com -p 6501 -D "cn=orcladmin" -q
ldapbind -h IDSTORE.mycompany.com -p 389 -D "cn=orcladmin" -q

ldapbind -h LDAPHOST1.mycompany.com -p 7501 -D "cn=orcladmin" -q -U 1
ldapbind -h LDAPHOST2.mycompany.com -p 7501 -D "cn=orcladmin" -q -U 1
```

10.8.4.3 Validating SSL Connectivity

You can manually verify that the SSL connection has been set up correctly by generating a wallet and then using that wallet to access Oracle Internet Directory. Proceed as follows:

Execute the command

```
cd IDM_BASE/products/dir/oracle_common/bin
./SSLClientConfig.sh -component cacert
```

providing the following inputs:

- LDAP host name: Name of the Oracle Internet Directory server containing the Domain Certificate
- LDAP port: Port used to access Oracle Internet Directory (*OID_LDAP_PORT*), for example: 3060
- LDAP User: Oracle Internet Directory admin user, for example: cn=orcladmin
- Password: Oracle Internet Directory admin user password
- SSL Domain for CA: This is IDMDomain.
- Password for truststore: This is the password you want to assign to your wallet.

When the command executes, it generates wallets in the directory *IDM_BASE*/products/dir/idm/rootCA/keystores/common

Now that you have a wallet, you can test that authentication is working by executing the command:

```
ldapbind -h LDAPHOST1.mycompany.com -p 3131 -U 2 -D cn=orcladmin -q -W "file:IDM_
BASE/products/dir/idm/rootCA/keystores/common" -Q
```

You will be prompted for your Oracle Internet Directory password and for the wallet password. If the bind is successful, the SSL connection has been set up correctly.

10.8.4.4 Validating Oracle Identity Manager

Validate the Oracle Identity Manager Server Instance by bringing up the Oracle Identity Manager Console in a web browser. at:

`https://SSO.mycompany.com:443/oim`

Log in using the `xelsysadm` username and password.

10.8.4.5 Validating Oracle SOA Suite Instance from the Web Tier

Validate Oracle SOA Suite by accessing the URL:

`http://IDMINTERNAL.mycompany.com:80/soa-infra`

and logging in using the `xelsysadm` username and password.

10.8.4.6 Validating Oracle Identity Manager Instance

Validate the Oracle Identity Manager Server Instance by bringing up the Oracle Identity Manager Console in a web browser at:

`https://SSO.mycompany.com/oim`

Log in using the `xelsysadm` username and password.

> **Note:** When you log in for the first time, you are prompted to setup Challenge Questions. Please do so before proceeding further.

Validate Oracle SOA Suite using the URL:

`http://IDMINTERNAL.mycompany.com/soa-infra`

Log in as the `weblogic_idm` user.

10.8.5 Validating WebGate and the Oracle Access Manager Single Sign-On Setup

To validate that WebGate is functioning correctly, open a web browser and go the OAM console at: `http://ADMIN.mycompany.com/oamconsole`

You now see the Oracle Access Manager Login page displayed. Enter your OAM administrator user name (for example, `oamadmin`) and password and click **Login**. Then you see the Oracle Access Manager console displayed.

To validate the single sign-on setup, open a web browser and go the WebLogic Administration Console at `http://ADMIN.mycompany.com/console` and to Oracle Enterprise Manager Fusion Middleware Control at: `http://ADMIN.mycompany.com/em`

The Oracle Access Manager Single Sign-On page displays. Provide the credentials for the `weblogic_idm` user to log in.

10.9 Managing the Topology for an Oracle Identity Management Enterprise Deployment

This section describes the operations that you can perform after you have set up the Oracle Identity Management topology.

10.9.1 Starting and Stopping Components

This section describes how to start, stop and restart the various components of the Oracle Enterprise Deployment for Oracle Identity Management.

This section contains the following topics:

- Section 10.9.1.1, "Startup Order"

- Section 10.9.1.2, "Starting and Stopping Servers."

10.9.1.1 Startup Order

When starting up your entire infrastructure, start the components in the following order, (ignoring those not in your topology):

1. Database(s)
2. Database Listener(s)
3. Oracle Internet Directory
4. Oracle Virtual Directory
5. Node Manager
6. Oracle Access Manager Server(s)
7. WebLogic Administration Server
8. Oracle HTTP Server(s)
9. Oracle SOA Suite Server(s)
10. Oracle Identity Manager Server(s)

10.9.1.2 Starting and Stopping Servers

During provisioning, scripts were created in the *SHARED_ROOT*/config/scripts directory to start and stop all the servers in the environment. Two of the scripts are available for you to use from the command line to start and stop all Oracle Identity Management servers. The remaining scripts are used internally and must not be invoked from the command line.

Note: These scripts do NOT stop or start the database.

10.9.1.2.1 Starting All Servers Provisioning created a file called `startall.sh`, which is used to start all of the components on a particular server. To start everything in the correct order run the command on hosts in the following order:

- LDAPHOST1
- LDAPHOST2
- IDMHOST1
- IDMHOST2
- WEBHOST1
- WEBHOST2

If you want to start the services on a single host, execute the command on that host.

Before invoking this script, set `JAVA_HOME` to *JAVA_HOME*.

During exectution you will be prompted to enter the Weblogic and Node Manager administrator passwords.

The script starts the servers in the following order:

1. Node Manager1
2. AdminServer

3. wls_ods1
4. wls_soa1
5. wls_oim1
6. wls_oam1
7. wls_oif1
8. ohs1
9. oid1
10. oid2
11. ohs2
12. Node Manager 2
13. wls_ods2
14. wls_soa2
15. wls_oim2
16. wls_oam2
17. wls_oif2

10.9.1.2.2 Stopping All Servers: The script to stop all servers is `stopall.sh`.

Before invoking this script, set `JAVA_HOME` to *`JAVA_HOME`*.

During execution you will be prompted to enter the Weblogic and Node Manager administrator passwords.

10.9.2 About Oracle Identity Management Console URLs

Table 10–1 lists the administration consoles used in this guide and their URLs.

Table 10–1 Console URLs

Domain	Console	URL
IDMDomain	WebLogic Administration Console	`http://ADMIN.mycompany.com/console`
IDMDomain	Enterprise Manager FMW Control	`http://ADMIN.mycompany.com/em`
IDMDomain	OAM Console	`http://ADMIN.mycompany.com/oamconsole`
IDMDomain	ODSM	`http://ADMIN.mycompany.com/odsm`

10.9.3 Performing Backups During Installation and Configuration

It is an Oracle best practices recommendation to create a backup after successfully completing the installation and configuration of each tier, or at another logical point. Create a backup after verifying that the installation so far is successful. This is a quick backup for the express purpose of immediate restoration in case of problems in later steps. The backup destination is the local disk. You can discard this backup when the enterprise deployment setup is complete. After the enterprise deployment setup is complete, you can initiate the regular deployment-specific Backup and Recovery process.

For more details, see the *Oracle Fusion Middleware Administrator's Guide*.

For information on database backups, refer to the *Oracle Database Backup and Recovery User's Guide*.

This section contains the following topics:

- Section 10.9.3.1, "Backing Up Middleware Home"
- Section 10.9.3.2, "Backing Up LDAP Directories"
- Section 10.9.3.3, "Backing Up the Database"
- Section 10.9.3.4, "Backing Up the WebLogic Domain"
- Section 10.9.3.5, "Backing Up the Web Tier"

10.9.3.1 Backing Up Middleware Home

Back up the Middleware homes whenever you create a new one or add components to it. The Middleware homes used in this guide are Oracle Identity Management and Oracle Identity and Access Management.

10.9.3.2 Backing Up LDAP Directories

Whenever you perform an action which updates the data in LDAP, back up the directory contents.

This section contains the following topics:

- Section 10.9.3.2.1, "Backing up Oracle Internet Directory"
- Section 10.9.3.2.2, "Backing up Oracle Virtual Directory"
- Section 10.9.3.2.3, "Backing Up Third-Party Directories"

10.9.3.2.1 Backing up Oracle Internet Directory To back up an Oracle Internet Directory instance:

1. Shut down the instance using `opmnctl` located under the *`OID_ORACLE_INSTANCE`*`/bin` directory:

   ```
   OID_ORACLE_INSTANCE/bin/opmnctl stopall
   ```

2. Back up the Database hosting the Oracle Internet Directory data and the Oracle Internet Directory instance home on each host.
3. Start up the instance using `opmnctl` located under the *`OID_ORACLE_INSTANCE`*`/bin` directory:

   ```
   OID_ORACLE_INSTANCE/bin/opmnctl startall
   ```

10.9.3.2.2 Backing up Oracle Virtual Directory To back up an Oracle Virtual Directory instance:

1. Shut down the instance using `opmnctl` located under the *`OVD_ORACLE_INSTANCE`*`/bin` directory:

   ```
   OVD_ORACLE_INSTANCE/bin/opmnctl stopall
   ```

2. Back up the Oracle Virtual Directory Instance home on each LDAP host.
3. Start up the instance using `opmnctl` located under the *`OVD_ORACLE_INSTANCE`*`/bin` directory:

```
OVD_ORACLE_INSTANCE/bin/opmnctl startall
```

10.9.3.2.3 Backing Up Third-Party Directories Refer to your operating system vendor's documentation for information about backing up directories.

10.9.3.3 Backing Up the Database

Whenever you create add a component to the configuration, back up the IDMDB database. Perform this backup after creating domains or adding components such as Access Manager or Oracle Identity Manager.

10.9.3.4 Backing Up the WebLogic Domain

To back up the WebLogic domain, perform these steps:

1. Shut down the WebLogic administration server and any managed servers running in the domain as described in Section 10.9.1, "Starting and Stopping Components."
2. Back up the *ASERVER_HOME* directory from shared storage.
3. Back up the *MSERVER_HOME* directory from each host.
4. Restart the WebLogic Administration Server and managed servers.

10.9.3.5 Backing Up the Web Tier

To back up the Web Tier, perform these steps:

1. Shut down the Oracle HTTP Server as described in Section 10.9.1, "Starting and Stopping Components."
2. Back up the Oracle HTTP Server.
3. Start the Oracle HTTP Server as described in Section 10.9.1, "Starting and Stopping Components."

10.10 What to Do Next

Go to Chapter 11 which describes common problems that you might encounter when using Oracle Identity Management Provisioning and explains how to solve them.

11

Troubleshooting Oracle Identity Management Provisioning

This chapter describes common problems that you might encounter when using Oracle Identity Management Provisioning and explains how to solve them.

In addition to this chapter, review the *Oracle Fusion Middleware Error Messages Reference* for information about the error messages you may encounter.

This chapter contains the following sections:

11.1 Getting Started with Troubleshooting

This section describes how to use the log files and how to recover from provisioning failures. It contains the following topics:

11.1.1 Using the Log Files

To monitor provisioning using the wizard, click the icon under the **Log** field from any phase screen to see the logs for the current phase. The logs are searchable using the search box at the top of this new window. The log window does not refresh on its own, so click **Refresh** besides the search box at the top of this window to refresh the logs.

To check why a phase failed when the wizard is not running, check the corresponding logs files present under the logs directory using the following commands.

On Linux:
INSTALL_APPCONFIG_DIR/provisioning/logs/*hostname*.

On Windows:

INSTALL_APPCONFIG_DIR\provisioning\logs*hostname*.

11.1.2 Recovering From Oracle Identity Management Provisioning Failure

Oracle Identity Management Provisioning does not have any backup or recovery mechanism, so you must to start from the beginning in case of a failure.

If you perform a workaround that requires you to rerun Oracle Identity Management Provisioning, you must clean up the environment before rerunning it. Do the following:

1. Reboot the hosts to ensure that all running Oracle Identity Management processes are stopped.
2. Delete the content of the following directories on all hosts:
   - `Software Install Location`
   - `Shared Configuration Location`
   - `Local Configuration Location`
3. Drop the database schema using Oracle Fusion Middleware RCU. While dropping the schema, ensure that you select the ODS schema. Oracle Identity Management Provisioning will fail when you run it the next time. By default, all schemas except ODS schema are selected.
4. Create the database schema using Oracle Fusion Middleware RCU.

11.2 Resolving Common Problems

This section describes common problems and solutions. It contains the following topics:

11.2.1 Provisioning Fails

Problem

Provisioning fails.

Solution

Check the provisioning logs located in the directory:

INSTALL_APPCONFIG_DIR`/provisioning/logs/`*hostname*

where *hostname* is the host where the provisioning step failed.

11.2.2 OID Account is Locked

Problem

Investigation into the OID logs shows that the OID account is locked.

This is generally caused by the load balancer. The load balancer is continually polling OID to see if it is available using the given credentials. During setup, this can cause the account to become locked.

Solution

Disable the OID load balancer monitor during preconfiguration. Then enable it when provisioning is complete. Another alternative is to reduce the check frequency.

11.2.3 Missing ODSM Instance Directory on Second Node

Problem

After you run the Oracle Identity Management Provisioning Wizard, only one instance directory for Oracle Directory Services Manager is installed.

Solution

The absence of the ODSM instance directory on the second node does not result in any loss of function.

11.2.4 Null Error Occurs When WebLogic Patches Are Applied

Problem

During Oracle Identity Management Provisioning, patches are applied to all products provisioned, including WebLogic. This entails running the Smart Update `bsu` command. This command may fail without producing a detailed error message.

Cause

In this case, the failure is likely caused by directory paths that are longer than what the `bsu` command supports. You can verify this by running the `bsu` command manually, passing it the `-log` option, and looking for a stack trace containing a message such as the following:

```
java.lang.IllegalArgumentException:
Node name
?a?very?long?path?which?may?cause?problems?leading?to?an?IDMTOP?products?dir?utils
?bsu?cache_dir too long
```

For more information, see the chapter "Using the Command Line Interface" in *Oracle Smart Update Applying Patches to OracleWebLogic Server*.

Solution

When planning the Oracle Identity Management deployment, ensure that the `IDM_TOP` path is 45 characters or fewer in length.

11.2.5 Oracle Identity Management Patch Manager Progress Command Shows Active Session After Provisioning

Problem

If you run the Oracle Identity Management Patch Manager `progress` command after Oracle Identity Management Provisioning completes, the output shows an active session specific to Oracle Identity Management Provisioning, which is listed as ACTIVE, and contains a set of PLANNED steps.

Solution

You can safely ignore this output. The provisioning-driven patch session is complete, and all steps which needed to run have run. Creating a new patch session will silently replace this special session without error.

11.2.6 False OPatch Error Messages Printed to Log During Install Phase

Problem

During the install phase of provisioning, you may see a message `Starting binary patching for all-binary-patch components ...`, followed by a series of OPatch failure messages prefaced with the string `prepatch` within the provisioning log. These errors contain the string `Failed to load the patch object`.

Solution

These messages are harmless and can be safely ignored.

11.2.7 Oracle Identity Management Provisioning Wizard Hangs (Linux and UNIX)

Problem

The Oracle Identity Management Provisioning Wizard hangs. Neither the **Next** nor the **Back** button is active.

Cause

This problem is due to stale Network File System (NFS) file handles.

Solution

On Linux or UNIX, issue the following command:

```
df -k
```

Record the output of the `df` command, even if it is successful, in case further analysis is necessary. For example, take a screenshot.

If the `df` command hangs or is unsuccessful, work with your system administrator fix the NFS problem.

After the NFS problem has been resolved and the `df` command finishes successfully, run provisioning again.

11.2.8 Provisioning Fails During Install Phase (Linux)

Problem

Provisioning fails during the Install phase.

Cause

Some 32-bit libraries such as `crt1.o` are missing.

Solution

There are two ways to fix this. Do one of the following:

- Copy the 32-bit libraries `gcrt1.o`, `crtn.o`, `crti.o`, `crt1.o`, `Scrt1.o`, and `Mcrt1.o` from `/usr/lib/` on another machine running the same version.
- Install the missing package `glibc-devel.i686`

11.2.9 Oracle Identity Management Provisioning Wizard Install Fails Due to Oracle Internet Directory Configuration Failure (Windows)

Problem

The Oracle Internet Directory configuration fails on the Windows 2008 Server R2 +SP1, causing the Identity Management Provisioning Wizard to fail.

Solution

After the installation of the Oracle Identity Management Provisioning Wizard has finished, do the following:

1. Edit the `sqlnet.ora` file in the Oracle Internet Directory environment folder located at: `%ORACLE_HOME%\network\admin`.
2. Set the `ADR_BASE` parameter to a folder other than the Oracle home, for example, C:\temp.
3. If it does not exist already, add an `sqlnet.ora` file to that folder and ensure that it contains the `ADR_BASE` parameter, set to the same value as in Step 1.

11.2.10 Provisioning Fails if Installer Repository Location Is a UNC Path (Windows)

Problem

Provisioning fails at install time on Microsoft Windows with an error message similar to this:

```
[logStatus] STATE=BUILD_STARTED!TIMESTAMP=2013-03-26 04:56:28
MDT!TARGET=installwls!
CATEGORY=Weblogic!DOMAIN=NONE!HOSTNAME=slc02jqf!PRODUCT
FAMILY=orchestration!PRODUCT=orchestration!TASK=install!TASKID=orchestration.orche
stration.NONE.installwls.
NONE!MESSAGE=Starting install for weblogic for
C:\idmtop/products/dir!DETAIL=!BUILDFILE=c:\idminstaller\Oracle_
IDMLCM1\provisioning\idm-provisioning-build\idm-commonbuild.
xml!LINENUMBER=33!
[2013-03-26T04:56:30.693-06:00] [runIDMProvisioning-install]
[NOTIFICATION]
[] [runIDMProvisioningt-install] [tid: 12] [ecid:
0000JqaLtN_B1FH5Ivt1if1HKNuO000003,0] [exec]
```

```
java.lang.ClassNotFoundException:
com.bea.cie.gpr.internal.model.DelegateHomeListHelper
```

Cause

This error occurs because you are accessing the Software Repository using a UNC path. That is, you are using a path of the form \\server\share.

Solution

To resolve this issue, map the share to a local disk and then specify the repository location using the local disk path.

11.2.11 Oracle Identity Management Provisioning Fails During Preconfigure Phase (Windows)

Problem

Oracle Identity Management provisioning fails during the Preconfigure phase, with the following error:

```
TASKID=orchestration.orchestration.BUILD_ERROR.NONE.installNodeManager!MESSAGE
=Error exit code 1069 from C:\Windows\system32\sc.exe!DETAIL=Error exit code
1069 from C:\Windows\system32\sc.exe!
```

Cause

Node Manager fails to start due to a password error.

Solution

Perform the steps described in Section 5.3.1.7, "Set Up Required User (Windows)."

11.2.12 Error When Starting Oracle Access Manager Managed Servers (Windows)

Problem

After you complete Oracle Identity Management Provisioning, you will see an error similar to the following when you start the Oracle Access Manager Managed Servers on Windows:

```
Caused by: java.net.SocketException: Address family not supported by protocol
family: bind
```

Solution

Edit `setDomainEnv.cmd` and add the following parameters to the environment variable `EXTRA_JAVA_PROPERTIES`:

```
-DuseIPv6Address=false -Djava.net.preferIPv6Addresses=false
```

Restart the Administration Server and all Managed Servers that are running.

11.3 Using My Oracle Support for Additional Troubleshooting Information

You can use My Oracle Support (formerly MetaLink) to help resolve Oracle Fusion Middleware problems. My Oracle Support contains several useful troubleshooting resources, such as:

- Knowledge base articles

- Community forums and discussions
- Patches and upgrades
- Certification information

> **Note:** You can also use My Oracle Support to log a service request.

You can access My Oracle Support at https://support.oracle.com.

11.4 What To Do Next

Go to Chapter 12 which describes the process of creating a response file for a new Oracle Fusion Applications environment using the Provisioning Wizard interview process.

Part VI

Provisioning Oracle Fusion Applications

This part describes Oracle Fusion Applications provisioning.

Part VI contains the following chapters:

12

Creating a Response File

This chapter describes the process of creating a response file for a new Oracle Fusion Applications environment using the Provisioning Wizard interview process.

This chapter includes the following sections:

12.1 Introduction to Creating a Response File

Oracle Fusion Applications Provisioning orchestrates the physical installation and configuration of the product offerings that you choose and deploys those offerings and their dependent middleware components to a predetermined Oracle WebLogic Server Domain. To perform the installation tasks, Provisioning requires the provisioning repository of installers, the provisioning framework, and a response file.

When you create a response file, you choose provisioning configurations and specify the configuration details for the product offerings and their dependent middleware components. You save the response file and specify its location when you are ready to use it to provision a new environment.

12.1.1 How Does the Response File Work?

You must have downloaded the provisioning repository, installed the provisioning framework, and installed a database and the identity management components before you can create a response file. See Section 5.3.2, "Preparing the Oracle Fusion Applications Server" for provisioning prerequisites.

After the prerequisite setup is complete, you run the Provisioning Wizard and select the **Create a New Applications Environment Response File** option. During the interview process, you choose product offerings to install. The wizard "knows" which middleware dependencies must be installed for each product offering, and which host must be provisioned first. It detects common products that each offering relies on, as well as the presence of the transaction database and identity-related components, and prompts for the appropriate configuration parameters.

Using a question and answer interview format, the wizard collects information about:

- Provisioning configurations (product offerings)

- Node Manager credentials and installation and configuration directories
- Database connections and schema passwords
- Host names and ports for the offerings and their middleware dependencies
- Common configuration details for components, such as web tier, virtual hosts, email, and identity management

After you complete the response file, save it. Then, when you are ready to perform the physical installation, choose the **Provision a New Environment** option from the Provisioning Wizard and indicate the location of the response file. The wizard uses the details in the response file as a guide to what must be retrieved from the provisioning repository.

12.1.2 Selecting Product Offerings

An installation of Oracle Fusion Applications is logically broken up into groups of features known as **product offerings**, which represent the highest-level collection of functionality that you can license and implement. A **provisioning configuration** is a collection of one or more product offerings.

Product offerings have interdependencies on companion applications (for example Oracle Fusion Human Capital Management relies on Oracle Financials payroll), as well as middleware dependencies (for example, Oracle SOA Suite) required for runtime execution. The wizard prompts for applications and middleware configuration details at the domain level during Domain Topology Configuration.

When you select individual product offerings within a configuration instead of selecting all offerings within the configuration, the wizard starts the Managed Servers *only for the offerings that you selected*. However, because the interdependent details for the entire configuration are included in the response file, you can activate additional functionality later by using the Oracle Fusion Applications Functional Setup Manager to start the other Managed Servers. See *Oracle Fusion Functional Setup Manager User's Guide*.

The provisioning configurations are as follows:

- Oracle Fusion Customer Relationship Management (Sales and Marketing)
- Oracle Fusion Financials (Financials, Oracle Fusion Procurement, and Oracle Fusion Projects)
- Oracle Fusion Human Capital Management (Workforce Deployment, Workforce Development, and Compensation Management)
- Oracle Fusion Supply Chain Management (Product Management, Order Orchestration, Material Management and Logistics)

You can also choose several standalone product offerings. For this group of offerings, only the direct dependencies are installed, configured, and deployed:

- Customer Data Hub
- Enterprise Contracts
- Oracle Fusion Accounting Hub
- Oracle Fusion Incentive Compensation

12.1.3 Wizard Actions for Oracle Identity Management Components

During the Provisioning Wizard interview process, the wizard collects information that is necessary to connect to the Oracle Identity Management components you have previously installed and configured. This information includes:

- The user designated as the Super User. This user must already exist in the policy store.
- The existence of the system administrators group. This information determines if the group was created during the Oracle Identity Management component installation and configuration process, or if it must be created during provisioning.
- The distinguished name (DN) of the system administrators group (if it exists).
- The authenticator that will serve as the LDAP identity store: Oracle Internet Directory (OIDAuthenticator) or Oracle Virtual Directory (OVDAuthenticator).

12.1.4 Creating Installation-Specific Response Files

There are numerous scenarios for the environments you can create — from a small demonstration system, to a full production system provisioned on multiple hosts. The Provisioning Wizard can accommodate the creation of response files for specific environments so that you can create a separate response file for each type of environment. Note that all occurrences of a `hostname` should use the same name in the response file.

12.1.5 Updating a Response File

Frequently, details for a response file are not final, and so cannot be specified during a single pass through the Provisioning Wizard interview. Or, a completed response file has not been implemented, and requires changes before it is. The wizard options include the choice to save a partially completed response file and update it later. Note that a response file is not complete or available for provisioning until you click **Finish** on the **Summary** screen.

However, after you select product offerings and save them in a response file, regardless of whether it is partially or fully complete, you cannot update or change the product offerings in that response file. To add or change the mix of offerings, you must create a new response file and specify the new or additional offerings.

12.2 Prerequisites to Creating a Response File

Before you create a response file, you must have completed the following tasks:

1. Read and understand the concepts in Chapter 1.
2. Perform the prerequisite tasks outlined in Chapter 5.
3. Install a transaction database as described in Chapter 8.
4. Complete Oracle Identity Management provisioning. See Chapter 10.
5. If you plan to enable load balancer as described in Section 12.3.9, "Load Balancer Configuration", ensure that you complete the load balancer configuration as described in Section 4.1.3, "Planning Load Balancer Requirements" before proceeding.

12.3 Creating a Response File

Complete the wizard interview screens and save the response file in a location that is accessible to the various installers. Record the location, as you must supply it when you provision the environment. Note that you should create your response file on the Primordial host, which is the host that contains the Administration Server of the Common domain.

Note: The wizard warns if it cannot connect to the database or any of the hosts specified in the response file and if any of the passwords are not valid. If this warning represents an exception, you can ignore it and continue creating the response file. However, you *must* fix all issues flagged in the warnings before you start to provision an environment. You cannot successfully run provisioning until all validations have passed.

12.3.1 Start the Provisioning Wizard

The Provisioning Wizard supports the following command line options:

Table 12–1 Provisioning Wizard Command Line Options

Command Line Option	Description	Default Value
`-invPtrLoc [inventory pointer file name]`	Location of the `oraInst.loc` file.	`/etc/oraInst.loc`
`-ignoreSysPrereqs [true|false]`	Disables validation for database, schema and hosts. Most validation errors will be ignored. **Note:** `-ignoreSysPrereqs true` is the same as `-ignoreSysPrereqs` with no value specified.	false
`-help`	Displays help text. **Note:** The `-multitenant` option is displayed when you use the `-help` option. This option is not available for 11*g* Release 8 (11.1.8) and is reserved for future use.	

Usage:

```
provisioningWizard.sh -invPtrLoc <inventory pointer location
file>

-ignoreSysPrereqs {true|false}

-help
```

Example 12–1

```
provisioningWizard.sh -invPtrLoc /oracle/oraInst.loc
-ignoreSysPrereqs
```

To start the Provisioning Wizard, do the following on the primordial host:

1. Set the *JAVA_HOME* environment variable to point to the JDK location in the provisioning repository, for example:

   UNIX:

   `export JAVA_HOME=repository_location/jdk6`

```
export PATH=$JAVA_HOME/bin:$PATH
```

AIX:

```
export JAVA_HOME=repository_location/jdk6
export PATH=$JAVA_HOME/bin:$PATH
export SKIP_ROOTPRE=TRUE
```

> **Note:** This environment variable is not required while creating a response file. However, it is required for provisioning an environment. See Section 13.5.1, "Starting the Wizard and Preparing to Install" for details.

Windows:

```
set JAVA_HOME=repository_location\jdk6
set PATH=%JAVA_HOME%\bin;%PATH%
```

2. Verify that the `LIBPATH` value is null.
3. On UNIX systems, set the DISPLAY environment variable to an active and authorized display.
4. Run the following command on the primordial host. For more information, see Section 1.5.1, "Types of Hosts in a Multiple-Host Environment".

   UNIX:

   ```
   cd framework_location/provisioning/bin
   ./provisioningWizard.sh
   ```

   Solaris:

   ```
   cd framework_location/provisioning/bin
   bash provisioningWizard.sh
   ```

   Windows:

   ```
   cd framework_location\provisioning\bin
   provisioningWizard.bat
   ```

> **Note:** Ensure that provisioning on Microsoft Windows platforms is performed from a **Run as Administrator** console. By default, the command prompt has the necessary privilege set. If not, you can run the Run as Administrator option by right clicking the Command Prompt from the Start menu.

12.3.2 Wizard Screens and Instructions

Table 12–2 shows the steps necessary to create a response file using the Provisioning Wizard. For help with any of the screens, click **Help** on any Provisioning Wizard screen.

> **Note:** If you do not input the correct values required, the error and warning messages are displayed at the bottom of the screen.

Table 12–2 Creating a Response File

Screen	Description and Action Required
Welcome	No action is required on this read-only screen. Click **Next** to continue.
Specify Central Inventory Directory	This screen displays only if one or more of the following conditions are not met: ■ The `-invPtrLoc` option is used to specify the central inventory location on non-Windows platforms, so the default value for your platform is not used. Note that the default for Linux and AIX platforms is `/etc/oraInst.loc` and for Solaris, it is `/var/opt/oracle/oraInst.loc`. ■ The Central Inventory Pointer File is readable. ■ The Central Inventory Pointer File contains a value for `inventory_loc`. ■ The `inventory_loc` directory is writable. ■ The `inventory_loc` directory has at least 150K of space. ■ `inventory_loc` is not a file. Specify the location of the **Central Inventory Directory** that meets the previous criteria. The `inventory_loc` directory can be created by the `createCentralInventory.sh` script and does not have to exist at the time you specify its location. For non-Windows platforms, in the **Operating System Group ID** field, select or enter the group whose members will be granted access to the inventory directory. All members of this group can install products on this host. Click **OK** to continue. The **Inventory Location Confirmation** dialog prompts you to run the *`inventory_directory`*`/createCentralInventory.sh` script as root, to confirm that all conditions are met and to create the default inventory location file, such as `/etc/oraInst.loc`. After this script runs successfully, return to the interview and click **OK** to proceed with the installation. If you do not have root access on this host but want to continue with the installation, select **Continue installation with local inventory** and click **OK** to proceed with the installation. For Windows platforms, this screen displays if the inventory directory does not meet requirements. For more information about inventory location files, see "Oracle Universal Installer Inventory" in the *Oracle Universal Installer and OPatch User's Guide*. Click **Next** to continue.
Installation Options	Presents the list of valid installation actions that you can perform using the wizard. Select **Create a New Applications Environment Response File**. Click **Next** to continue.

Table 12–2 (Cont.) Creating a Response File

Screen	Description and Action Required
Specify Security Updates	Set up a notification preference for security-related updates and installation-related information from My Oracle Support. You can receive the notifications in two ways: ■ **Email**: Enter your email address to have updates sent by email. ■ **I wish to receive security updates via My Oracle Support**: Select this option to have updates sent directly to your My Oracle Support account. You must enter your **My Oracle Support Password** if you select this option. **Note:** If you provide invalid My Oracle Support (MOS) credentials, a dialog box is displayed informing that you will be anonymously registered. You must complete the following steps before you continue with provisioning the new environment: 1. Cancel and exit the Provisioning Wizard. 2. Obtain the correct MOS credentials. 3. Restart the Provisioning Wizard to update the provisioning response file with the correct MOS credentials or uncheck the checkbox next to **I wish to receive security updates via My Oracle Support**. Save the provisioning response file and then exit the Provisioning Wizard. 4. Restart the Provisioning Wizard to provision the Oracle Fusion Applications environment. Click **Next** to continue.
Provisioning Configurations	Select one or more offerings, either within a configuration, or from the list of standalone product offerings. **Tip: This value is available in the** *Oracle Fusion Applications Installation Workbook* **- Provisioning tab -> Fusion Applications Offerings.** Click **Details** in the message pane to see a breakdown of servers for each offering. After you click **Next**, you cannot change the selections on this screen. To make changes, click **Cancel**, open a new wizard session, and create a new response file.
Response File Description	Enter information to describe this response file. This description is not associated in any way with the executable plan file, or the summary file, that you save when you finish creating this response file. ■ **Response File Name**: Specify a name to identify this response file. ■ **Response File Version**: Assign a version number to this response file. The version is intended for documentation only. ■ **Created By**: Defaults to the operating system user who invoked the wizard. Set when the response file is initially created and cannot be modified for the current response file. ■ **Created Date**: Defaults to the date that the response file was initially created and saved. Set when the response file was initially created and cannot be modified for the current response file. ■ **Response File Description**: Provide a description of this response file. To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.
Installation Location	Specify credentials for the Node Manager and supply the location of the various directories required for installation and configuration actions. To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.

Table 12–2 (Cont.) Creating a Response File

Screen	Description and Action Required
System Port Allocation	Accept the default values or set a custom value for the **Applications Base Port**. The application domain port ranges are derived from this value. If you change the base port value, the domain port ranges adjust accordingly. Ranges must not overlap and must be set in ascending order. Ports listed under **Other Ports** are not derived from the **Applications Base Port** value. These "individual" ports can be defined using custom port values. To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.
Database Configuration	Enter the database parameters that you established when you installed Oracle Database. The wizard validates whether the database you installed is a single instance of Oracle Database or Oracle Real Application Clusters (Oracle RAC). If a **Single Instance Database**, enter: ■ **User Name (SYSDBA Role)**: The user name of the `sysdba` role. This user name is used to upgrade schemas during the configuration phase. Note that the `sysdba` fields are not validated, so ensure that you enter the correct values. ■ **Password**: The password of the `sysdba` role. ■ **Host Name**: The name of the host where the database is installed. ■ **Port**: The listening port for the database. ■ **Service Name:** The global database name for the database that you installed. Used to distinguish this database instance from other instances of Oracle Database running on the same host. If you have installed Oracle RAC, select **Real Application Clusters Database** and enter the **Service Name** that you specified when you installed this database. Click **Add** to create a new row in the table for each instance. Select a row and click **Remove** to delete it. Enter the following values for the previously installed database: ■ **User Name (SYSDBA Role)**: The user name of the `sysdba` role. This user name is used to upgrade schemas during the configuration phase. Note that the `sysdba` fields are not validated, so ensure that you enter the correct values. ■ **Password**: The password of the `sysdba` role. ■ **Host Name**: The name of the host for each Oracle RAC instance. ■ **Port**: The listening port of the database. ■ **Instance Name**: The name of the Oracle RAC instance used to manage this database. Due to a limitation in the Oracle Data Integrator (ODI) installer, if you select Real Application Clusters Database, you must enter at least two rows in the table. See Section 14.6.2. Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> FA Transactional Database. To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.

Table 12–2 (Cont.) Creating a Response File

Screen	Description and Action Required
Schema Passwords	The database that you installed contains preloaded schemas required for runtime execution. Select one of the following options and enter the database schema passwords set up when you ran the Oracle Fusion Applications Repository Creation Utility. For more information, see Table 10–1, " Running the Oracle Fusion Applications Repository Creation Utility". ■ **Use the same password for all accounts**: Select this option if you set up a single password for all accounts. Enter the value in the **Password** field. This option is the default. ■ **Use a different password for each account**: Select this option if you set up individual passwords for each **Account**. Password values were set up for Oracle Fusion Applications and AS Common Schemas. Enter those values in the **Password** field. To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.
ODI Password Configuration	Enter and confirm your ODI Supervisor **Password**. The ODI Supervisor Password is the Supervisor Password that you entered on the **Custom Variables** page during execution of Oracle Fusion Applications RCU under the Master and Work Repository component. To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.
Domain Topology Configuration	To determine the flow for the remaining wizard interview screens, choose one of the options. The types of possible topologies are: ■ **Basic Topology**: One host for all domains ■ **Medium Topology**: One host per domain ■ **Advanced Topology**: One host per application and middleware component Note that all hosts must use the same operating system; that is, you cannot install "domain1" on Windows and "domain2" on Linux. Note that you should **not use** any of the Oracle Identity Management hosts as the host in the Domain Topology Configuration because installing Oracle Identity Management and Oracle Fusion Applications on the same host is not a supported topology. See Section 12.3.5, "Domain Topology Configuration" for details. To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.

Table 12–2 (Cont.) Creating a Response File

Screen	Description and Action Required
Common Domain	**Note**: Individual domain screens appear only if you selected the **One host per application and middleware component** option on the **Domain Topology Configuration** screen. Specify values for this domain and its middleware dependencies. All hosts must use the same operating system and share a common mount point for network storage. The host specified for the Admin Server is the default for all servers. You can change the default. ▪ **Host Name**: Specify the host where you want to install and configure the Managed Servers for this domain. Note that this host cannot be the same Oracle Identity Management host. ▪ **Port**: Port for internal communications only. The wizard assigns values based on values on the **System Port Allocation** screen. You can edit port values. However, they must be unique within the domain and fall within the range previously specified. For example, in a range of 7401 to 7800, a value of 8444 generates an error. ▪ **UCM Intradoc Server Port**: Port where the Universal Content Management Server listens. ▪ **InBound Refinery Server Port**: Used for calling top-level services. To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.
Product Family Domains	**Note**: Individual domain screens appear based on which options you select on the **Domain Topology Configuration** screen. For example, the **Incentive Compensation Domain** screen does not appear unless you selected that product offering for installation. All product family domain screens prompt for the same types of values. Specify values for this domain and its middleware dependencies. All hosts must use the same operating system and share a common mount point for network storage. The host specified for the Admin Server is the default for all servers. You can change the default. ▪ **Host Name**: Specify the host where you want to install and configure the Managed Servers for this domain. Note that this host cannot be the same Oracle Identity Management host. ▪ **Port**: Port for internal communications only. The wizard assigns values based on values on the **System Port Allocation** screen. You can edit port values. However, they must be unique within the domain and fall within the range previously specified. For example, in a range of 7401 to 7800, a value of 8444 generates an error. **Note**: See Section 12.3.6, "Oracle Business Intelligence Configuration" for Oracle Business Intelligence configuration requirements. To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.
Web Tier Configuration	Use this screen to configure Oracle HTTP Server and choose a virtual host type. You can deploy the web tier to a host inside the firewall, or outside the firewall (demilitarized zone, known as DMZ). See Section 12.3.7, "Web Tier Configuration" for the list of parameters. To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.

Table 12–2 (Cont.) Creating a Response File

Screen	Description and Action Required
Virtual Hosts Configuration	Provisioning determines the application domains to be deployed based on your product offering choices and lists them on this screen. Specify domain-specific values for the type of virtual host mode that you selected on the **Web Tier Configuration** screen. See Section 12.3.8, "Virtual Hosts Configuration" for the list of parameters. To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.
Load Balancer Configuration	Load balancing enables you to distribute a workload evenly across two or more hosts, network links, CPUs, hard drives, or other resources. Check **Load Balancing Enabled** to take advantage of this feature, and specify: ▪ **Internal Load Balancer Configuration**: The host and port for the internal Virtual IP (VIP). ▪ **External Load Balancer Configuration**: The host and port for external Virtual IP (VIP). It must have a publicly available address to be usable. To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.
Web Proxy Configuration	Create **Proxy Settings** to enable users who want to use a proxy server to connect to the Internet. See Section 12.3.10, "Web Proxy Configuration" for details. Take note of the special instructions for Oracle Customer Relationship Management customers. To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.
IDM Properties File	When you are creating a response file or updating an incomplete response file without updates to this page, you will be able to select the IDM properties file to load IDM configuration data. After you select the file, you can review the content and decide if you want to proceed with this file. **WARNING:** You can review the file and select a different file if required on this screen. You cannot select an IDM properties file after you click **Next**, as the screen will display read-only fields. **Do not load IDM Configuration from IDM Properties file:** Select this option if you do not want to load the IDM configuration data from the IDM properties file. **Load IDM Configuration from IDM Properties file**: Select this option if you want the values on the Identity Management Configuration screen and the Access and Policy Management Configuration screen to default to the values in the IDM properties file (for example, `idmsetup.properties`). **IDM Properties file**: Enter the location of the file, for example, *`SHARED_CONFIG_DIR`*`/fa/idmsetup.properties`, where *`SHARED_CONFIG_DIR`* is the shared configuration location that you selected in the Install Location Configuration page of the Oracle Identity Management Provisioning Wizard. **IDM Properties file contents**: If you have selected a valid IDM properties file, the contents will be displayed. This field is read-only and cannot be modified. Click **Next** to continue.

Table 12–2 (Cont.) Creating a Response File

Screen	Description and Action Required
Identity Management Configuration	Provisioning loads roles, policies, and application IDs that you created during the prerequisite Oracle Identity Management installation. To share the identity management environment across multiple Oracle Fusion Applications installations, and make the policies and roles accessible to all environments, you must populate identity management configuration details during the first installation. See Section 12.3.13, "Identity Management Configuration" for the list of parameters. See also Section 12.3.11, "Distinguished Names" for information about Distinguished Names conventions. To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.
Access and Policy Management Configuration	Configure Oracle Fusion Applications for integration with existing Oracle Access Manager components. See Section 12.3.14, "Access and Policy Management Configuration" for the list of parameters. To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.
IDM Database Configuration	Enter the configuration details that you specified when you installed the database for Oracle Identity Manager. See Section 12.3.15, "IDM Database Configuration" for the list of parameters. To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.
Summary	Displays the applications and middleware components that will be installed when you perform a physical installation using this response file. Includes details such as required disk space and the installation locations. See Section 12.3.16, "Summary" for a description of the parameters. Click **Finish** to save the response file. The response file is complete and can be used as the basis for provisioning of a new environment.

12.3.3 Oracle WebLogic Server Node Manager Credentials and Installation Locations

Specify credentials for the Node Manager and supply the location of the various directories required for installation and configuration actions on the **Installation Location** screen. The credentials provided will be used to configure the NodeManager, secure WebLogic Server and OWSM keystores and wallets on the file system.

Ensure that you use the specified user name and password to connect to the NodeManager for starting and stopping servers.

Node Manager Credentials

- **User Name**: Specify a user name for the Node Manager role.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Identity Management tab -> Identity Store / Policy Store -> FA Node Manager Username.

- **Password**: Specify a password for the Node Manager and retype it in the **Confirm Password** field.

Installation and Configuration

Provide locations of various directories that the administrator needs access to. For non-Windows platforms, you must enter the full file path in the Provisioning Wizard UI when asked to provide any file path, such as Oracle Fusion Applications Home, Applications Configuration Directory, and so on. Using symbolic link paths will cause provisioning to fail in later phases.

- **Installers Directory Location**: Enter the path to the *repository_location* directory where you extracted the Oracle Fusion Applications software obtained from the media pack downloaded from the Oracle Software Delivery Cloud Portal. For Windows, the location must be a symbolically linked directory. See Section 5.3.2.21 for additional details. Note that a symbolic link is not necessary if the repository and the database are on the same node.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Storage tab -> Temporary Shared Storage -> Installers Directory Location.

- **Applications Base**: Enter the directory path to the applications base directory. The top-level directory for the Oracle Fusion Applications binaries is the applications base and is referred to as the *APPLICATIONS_BASE* directory (`net/mount1/appbase`). See Section 2.3.7.2 for additional details.

  The applications base directory must not be set to the system root directory or set to the root directory of a logical drive. Some lifecycle management tools compute directory names by backing up one directory level from the applications base directory and then appending the appropriate subdirectory name. These tools will fail if the applications base directory is set to the system root directory or set to the root directory of a logical drive because it is not possible to back up one directory level from the system root directory or from the root directory of a logical drive.

  During creation of a provisioning plan in a UNIX environment, ensure that the absolute file path of the *APPLICATIONS_BASE* directory does not exceed 59 characters before provisioning a new application environment.

  In a Windows environment, this name cannot exceed eight characters, and must be a symbolically linked directory. See Section 5.3.2.21 for additional details.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Storage tab -> Install Directories -> FA Applications Base.

- **Applications Configuration**: This directory is automatically populated based on the value you specify in the **Applications Base** field. It is the path to the directory where the configuration files for the domain will be written. You can specify a different location of your choice instead of using the location automatically populated by the UI. This directory must be empty.

  For Windows, the location must be a symbolically linked directory. See Section 5.3.2.21 for additional details.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Storage tab -> Install Directories -> FA Applications Configuration Location.

- **Enable Local Applications Configuration**: Select this checkbox to run the Managed Servers from a non-networked (local) disk on the host, visible only to the processes running on that host. If you enable this option, the wizard copies the domain configuration from the shared location and places it on the local disk you

specify. This configures all Managed Servers to run from the non-networked location.

- **Local Applications Configuration**: Specify the location for the local domain directory you want to set up. This field is required if you selected **Enable Local Applications Configuration**. The specified directory must exist and initially be empty on every host that participates in the domain topology. You must ensure the directory has sufficient disk space. During the Preverify phase, provisioning displays an error if the local configuration directory does not have sufficient disk space.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Storage tab -> Install Directories -> FA Local Applications Configuration Location.

Middleware Dependencies

- **Font Directory**: Appears only if you have selected Oracle Sales, Oracle Marketing, or Oracle Financials offerings. Enter the directory where the TrueType fonts are installed. The location varies on different operating systems, but is typically found here:
  - **Microsoft Windows x64 (64-bit)**: `C:\WINDOWS\Fonts`
  - **Linux x86-64**: `/usr/X11R6/lib/X11/fonts/TTF`
  - **Oracle Solaris**: `/usr/X11R6/lib/X11/fonts/TrueType`
  - **IBM AIX on POWER Systems (64-bit)**: `/usr/X11R6/lib/X11/fonts/TrueType`

  Some systems may not have TrueType fonts installed. If you cannot locate the fonts on your system, verify that they have been installed. In addition, you can use the fonts directory shipped as part of the JRE installed in the repository. Regardless of which path you specify, you must have access to.ttf files.

Oracle Business Intelligence Repository Password

RPD Password: Specify and **Confirm** a password to allow access to the metadata repository (RPD) for both Oracle Business Intelligence Applications and Oracle Transactional Business Intelligence. The password must be between 8 and 30 characters and contain at least one digit. It can include letters, numbers, pound sign (#), dollar sign ($), or underscore (_). If you want to include two consecutive dollar signs ($$) in the RPD password, enter one additional dollar sign ($) as the escape character before the second dollar sign in the password. This means you need to enter three dollar signs ($$$) for this field in the Provisioning Wizard to indicate two consecutive dollar signs. Provisioning sets up this password, but does *not* actually access the repository.

If the environment created is Windows-based, the wizard prompts for these values:

- ***Windows Domain\Windows User Name***: Specify a user name to use for running provisioning.
- ***Windows Domain Password***: Specify a password for running provisioning. Retype the password to **Confirm** it.

12.3.4 System Port Allocation

Accept the default values or set a custom value for the **Applications Base Port**. The application domain port ranges are derived from this value. If you change the base

port value, the domain port ranges adjust accordingly. Ranges must not overlap and must be set in ascending order.

> **Tip:** This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Fusion Applications Port Numbers -> Fusion Applications Base.

Ports listed under **Other Ports** are not derived from the Applications Base Port value. These "individual" ports can be defined using custom port values.

> **Tip:** Node Manager: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Fusion Applications Port Numbers -> FA Node Manager.
>
> Informatica Identity Resolution License Server: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Fusion Applications Port Numbers -> Informatica Identity Resolution License Server.

To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment. Click **Next** to continue.

If you have other software running on the provisioning hosts, ensure that the system port allocation value in the provisioning response file is not a port already used by other software. The system port allocation cannot be changed after you start provisioning a new Oracle Fusion Applications environment. If a port conflict is detected during provisioning phases, you have to restart provisioning from the beginning with a correct set of system port allocation. See Section 13.2, "Installation Phases and Types of Hosts in a Multiple-Host Environment" for more information.

To display a list of network connections including the port numbers and process identifier holding the ports, run these commands:

UNIX: `netstat -anp`

Windows: `netstat`

12.3.5 Domain Topology Configuration

To determine the flow for the remaining wizard interview screens, choose one of the topology types. Note that all occurrences of a `hostname` should use the same name in the response file. A machine name could be a logical or virtual host name. It can either be in fully qualified form, `mymachine.mycompany.com`, or short form, `myMachine`, if it is consistent throughout the response file. For more information, see Section 5.3.2.11, "Edit Host Names (UNIX)".

The types of possible topologies are:

- **Basic Topology**: One host for all domains
- **Medium Topology**: One host per domain
- **Advanced Topology**: One host per application and middleware component

> **Note:** You must install Oracle Identity Management and Oracle Fusion Applications on different hosts. Installing Oracle Identity Management and Oracle Fusion Applications on the same host is not a supported topology.

- **One host for all domains**: Select this option to specify the **Host Name** to provision all applications domains and their middleware dependencies on a single host. The wizard continues the interview at the **Web Tier Configuration** screen when you click **Next**.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Environment tab -> Environment Info -> FA Topology Type:

  For Basic topology, **Select One Host For All Domains**.

  This value is available in the *Oracle Fusion Applications Installation Workbook* - Topology tab -> Component Assignment:

  All Components below must have the same node # in the *Oracle Fusion Applications Installation Workbook*, use the abstract hostname (or real hostname if absract is blank) that corresponds to that node # in the Topology table:

  - FA Common Domain
  - FA CRM Domain
  - FA Financials Domain
  - FA HCM Domain
  - FA IC Domain
  - FA Procurement Domain
  - FA Projects Domain
  - FA Supply Chain Domain
  - FA Business Intelligence Domain

- **One host per domain**: Select this option and then select a **Host Name** for each domain to be created. Provisioning installs and configures the Managed Servers for each **Application Domain** and the middleware dependencies on the host that you specify. The wizard continues the interview at the **Web Tier Configuration** screen when you click **Next**.

Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Environment tab -> Environment Info -> FA Topology Type:

For Enterprise topology, select **One Host Per Domain**.

This value is available in the *Oracle Fusion Applications Installation Workbook* - Topology tab -> Component Assignment:

Use the abstract hostname (or real hostname if abstract is blank) that corresponds to the node # for the following components in the Topology table:

- FA Common Domain
- FA CRM Domain
- FA Financials Domain
- FA HCM Domain
- FA IC Domain
- FA Procurement Domain
- FA Projects Domain
- FA Supply Chain Domain
- FA Business Intelligence Domain

- **One host per application and middleware component**: Select this option to specify the host for each application and middleware component individually. The wizard displays the **Common Domain** screen when you click **Next**, and includes all domain-specific screens in the interview.

Note: This topology is not covered in the *Oracle Fusion Applications Installation Workbook* by default, but you can use it as part of an Enterprise or Enterprise HA example topology.

If you select the last option, you cannot change the selections on this screen after you click **Next**. You must click **Cancel**, open a new wizard session, and create a new response file to change the configuration domain topology later.

12.3.6 Oracle Business Intelligence Configuration

Oracle Business Intelligence products are integrated with, and accessible from, Oracle Fusion Applications. Products include:

- Oracle Business Intelligence Enterprise Edition
- Oracle Business Intelligence Applications
- Oracle Transactional Business Intelligence
- Oracle Essbase
- Oracle Business Intelligence Publisher
- Oracle Real-Time Decisions

Enter the **Host** where you want Oracle Business Intelligence products to be installed. You specified an **RPD** password on the **Installation Location** screen. Provisioning

creates this password and makes it available so that Oracle Business Intelligence Applications and Oracle Transactional Business Intelligence can access the metadata repository in your new environment.

> **Note:** The Oracle Fusion Applications installation and provisioning process installs the Oracle BI Applications software components in the Business Intelligence Oracle home but does no further setup. To finish setting up Oracle BI Applications, you must follow the instructions in the "Setting Up Oracle Business Intelligence Applications" chapter of the *Oracle Business Intelligence Applications Installation Guide.*

12.3.7 Web Tier Configuration

You can create virtual hosts on a single web tier. There are three options (IP-based, name-based, and port-based) for each domain that is created during installation. The values assigned during installation are derived from the default HTTP port that you name on this screen. Note that all occurrences of a `hostname` should use the same name in the response file. A machine name could be a logical or virtual host name. It can either be in fully qualified form, `mymachine.mycompany.com`, or short form, `myMachine`, if it is consistent throughout the response file. For more information, see Section 5.3.2.11, "Edit Host Names (UNIX)".

Web Tier

- **Install Web Tier in DMZ**: Select this option if you set up a separate host for web tier installation as a demilitarized zone (DMZ). This host does not have access to the shared file system. It cannot be used for any other host deployed, regardless of domain. See Section 6.4.

  > **Tip:** This value is available in the *Oracle Fusion Applications Installation Workbook* - Topology tab: Verify if the DMZ(Yes/No) column has the value **Yes** for the node that corresponds to the component FA WebTier.

- **Host**: Enter the name of the host where Oracle HTTP Server will be installed and configured.

  > **Tip:** This value is available in the *Oracle Fusion Applications Installation Workbook* - Topology tab: Use the abstract hostname (or real hostname if abstract is blank) for the node that corresponds to the component FA WebTier.

- **Virtual Host Mode**: Select one of the following:
  - **IP Based**: Created on the basis of an IP or IP:host combination (the default).
  - **Name Based**: Create new DNS entries, such as `fin.example.com` and `crm.example.com` to use as virtual hosts.
  - **Port Based**: Created based on the internal and external port for each domain.

Note: In the Provisioning Wizard, do not choose the Name Based virtual host mode if you are planning to specify Load Balancer Configuration details on the next page. This combination is not recommended as it requires manual changes during Oracle Fusion Applications Provisioning. Setting up Name Based virtual hosts is not recommended if you are using a Load Balancer.

Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> WebTier Virtual Host Mode -> FA WebTier -> Mode.

- **Domain Name**: Specify a domain name (using the format *my.example.com*) to configure the domain in which Oracle Fusion Applications will receive requests. This value is also used as the default domain name for name-based virtual hosts.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Environment tab -> Environment Info -> Domain name.

- **HTTP Port**: The default port for the web tier. UNIX: Do not specify a port that requires operating system administrator privileges.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Fusion Applications Port Numbers -> FA Oracle HTTP Server.

- **HTTPS (SSL) Port**: Secure port for the web tier. UNIX: Do not specify a port that requires operating system administrator privileges.

  Note: On UNIX platforms, using a port below 1024 requires root privileges and Provisioning is not run as root user, so you should not specify a HTTP/HTTPS port below 1024.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Fusion Applications Port Numbers -> FA Oracle HTTP Server SSL.

SMTP Server

- **Host**: Specify the host for email marketing. This field appears only if you selected the Oracle Fusion Customer Relationship Management offering.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Environment tab -> Email Server -> SMTP Server Host.

- **Port**: Default port for the SMTP server.

12.3.8 Virtual Hosts Configuration

Specify the configuration parameters for the domains to be installed on the virtual hosts that you selected on the Web Tier Configuration page. Note that all occurrences

of a `hostname` should use the same name in the response file. A machine name could be a logical or virtual host name. It can either be in fully qualified form, `mymachine.mycompany.com`, or short form, `myMachine`, if it is consistent throughout the response file.

If you selected **IP Based**, specify the following information for each application domain listed:

> **Tip:** These values are available in the *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> FA WebTier Virtual Hosts.

- **Internal Name**: The host name where the web tier listens on the internal virtual host for this domain. The host name can consist of letters A through Z (upper or lower case), digits 0 through 9, minus sign (-) and period (.). The first character must be a letter and the last character must not be a minus sign or a period.
- **Internal Port**: The port for this internal virtual host. Visible only from inside the firewall.
- **External Name**: The host name for the external virtual host for this domain or middleware dependency. The host name can consist of letters A through Z (upper or lower case), digits 0 through 9, minus sign (-) and period (.). The first character must be a letter and the last character must not be a minus sign or a period. The host:port should be visible from outside the firewall.
- **External Port**: The port to be used for this external virtual host. The `host:port` should be visible from outside the firewall.

If you selected **Name Based**, specify the following information for each domain listed:

- **Internal.Name**: The DNS name for this internal virtual host. For example, for Oracle Fusion Financials, the name might be `fin-internal`.
- **External.Name**: The DNS name for this external virtual host. For example, for Oracle Fusion Financials, the name might be `fin`.

If you selected **Port Based**, specify the following information for each domain listed:

- **Internal Port**: The port that is visible only from inside the firewall for this domain.
- **External Port**: The port that is visible from outside the firewall for this domain.

12.3.9 Load Balancer Configuration

Load balancing enables you to distribute a workload evenly across two or more hosts, network links, CPUs, hard drives, or other resources.

Load Balancing Enabled: This checkbox is selected by default. Keep it checked if you use load balancer in front of the Oracle Fusion Applications environment. Ensure that you have completed the load balancer configuration as described in Section 4.1.3, "Planning Load Balancer Requirements" before proceeding and then specify the following:

- **Internal Load Balancer Configuration**: The host and port for the internal Virtual IP (VIP).

> **Tip:** This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints.

- **External Load Balancer Configuration**: The host and port for external Virtual IP (VIP). It must have a publicly available address to be usable.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Virtual Hosts tab -> HTTP LBR Endpoints.

To stop creating this response file and resume later, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment.

Click **Next** to continue.

12.3.10 Web Proxy Configuration

Create **Proxy Settings** to enable users who want to use a proxy server to connect to the Internet.

Tip: These values are available in the *Oracle Fusion Applications Installation Workbook* - Environment tab -> Web Proxy.

- **Enable Web Proxy**: Select to enable proxy-related values to set up access to the Internet. **Note**: If you are a Oracle Fusion CRM customer and have a web proxy for external HTTP(S) traffic, you must select **Enable Web Proxy** on this screen and specify your web proxy configuration.
- **Web Proxy Host**: Enter the name of the host where the proxy server is installed.
- **Web Proxy Port**: The listening port assigned to the proxy server.
- **Enable Secure Web Proxy**: Select to have the proxy server SSL-enabled. If you select this checkbox, the **Secure Web Proxy Host** and **Secure Web Proxy Port** fields are enabled and become mandatory.
- **Secure Web Proxy Host**: Enter the SSL host used for secure communications.
- **Secure Web Proxy Port**: Enter the SSL port used for internal communications.
- **No Proxy Hosts**: Defaults to hosts that are connected directly. If there are multiple hosts, they are listed and separated by a vertical bar (`|`). You can use a wildcard character (*) to specify hosts that should be bypassed. For example, `*.example.com` would bypass all hosts whose name ends with `.example.com`.
- **Proxy Server Requires Authentication**: To enable authentication for the proxy server, select this option.
- **User Name**: Enter the user name that you set up for accessing the proxy server.
- **Password**: Enter the password that you set up for accessing the proxy server.

12.3.11 Distinguished Names

A Distinguished Name (DN) identifies an entry in a Lightweight Directory Access Protocol (LDAP) directory. Because directories are hierarchical, DNs identify the entry by its location as a path in a hierarchical tree (much as a path in a file system identifies a file). Generally, a DN begins with a specific common name, and proceeds with increasingly broader areas of identification until the country name is specified.

Table 18–3 provides definitions for distinguished name components (defined in the X.520 standard).

Table 12–3 Distinguished Name Components

Component	Definition
Common Name (CN)	Identifies the person or object defined by the entry. For example, `cn=John Doe`. Or `cn=corpDirectory.example.com`.
Organizational Unit (OU)	Identifies a unit within the organization. For example, `ou=scm`.
Organization (O)	Identifies the organization where the entry resides. For example, `o=My Corporation`.
Locality (L)	Identities the place where the entry resides. The locality can be a city, county, township, or any other geographic region. For example, `l=Your City`.
State of Province Name (ST)	Identifies the state or province in which the entry resides. For example, `st=Your State`.
Country (C)	Identifies the name of the country where the entry resides. For example, `c=US`
Domain Component (DC)	Identifies the components of a domain. For example, if the domain is `example.com`, the domain components would be: `dc=example, dc=com`.

12.3.12 Oracle Identity Management Properties File

When you are creating a response file or updating an incomplete response file without updates to this page, you will be able to select the IDM properties file to load Oracle Identity Management configuration data. After you select the file, you can review the content and decide if you want to proceed with this file.

WARNING: You can review the file and select a different file if required on this screen. You cannot select an IDM properties file after you click Next, as the screen will display read-only fields.

- **Do not load IDM Configuration from IDM Properties file**: Select this option if you do not want to load the IDM configuration data from the IDM properties file.
- **Load IDM Configuration from IDM Properties file:** Select this option if you want the values on the Identity Management Configuration screen and the Access and Policy Management Configuration screen to default to the values in the IDM properties file (for example, `idmsetup.properties`). For more information about the IDM properties file, see Section 10.7.2, "Passing Configuration Properties File to Oracle Fusion Applications".
- **IDM Properties file:** Enter the location of the file, for example, *`SHARED_CONFIG_DIR`*`/fa/idmsetup.properties`, where *`SHARED_CONFIG_DIR`* is the shared configuration location that you selected on the **Install Location Configuration** page of the Oracle Identity Management Provisioning Wizard.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Identity Management tab -> IDM Provisioning Files -> IDM Properties File Location.

- **IDM Properties file contents:** If you have selected a valid IDM properties file, the contents will be displayed. This field is read-only and cannot be modified.

12.3.13 Identity Management Configuration

Enter the parameters necessary to integrate applications with a previously installed Oracle Identity Management infrastructure. If you chose to use the values in the IDM properties file (`for example,idmsetup.properties`) on the **IDM Properties File** screen, they appear as defaults in the corresponding fields. You can replace the default values if your original configuration has changed.

- **Super User Name**: Enter the name of an existing user that should be granted administrator and functional setup privileges. The `uid` attribute must be set to be the same as the `cn` attribute.

  > **Tip:** This value is available in the *Oracle Fusion Applications Installation Workbook* - Identity Management tab -> Identity Store / Policy Store -> FA Super User Name.

- **Create Administrators Group**: Indicate whether you created an "Administrators" group, whose members have specialized privileges for all Oracle Fusion Middleware components. If you do not already have this group present in the identity store, this box should be checked.
- **Create Monitors Group**: Indicate whether you created a "Monitors" group, whose members have read-only administrative privileges to Oracle WebLogic Server domains. If you do not already have this group present in the identity store, this box should be checked.
- **Create Operators Group**: Indicate whether you created an "Operators" group, whose members have Monitors privileges to Oracle WebLogic Server domains. If you do not already have this group present in the identity store, this box should be checked.
- **Identity Store Server Type**: Indicate the type of identity store that you set up: OID (Oracle Internet Directory) or OVD (Oracle Virtual Directory). If you select OVD, then the **Default to Identity Store** checkbox in Oracle Platform Security Services Configuration must be unchecked and the policy store cannot be the same instance as the identity store (they must be different instances in this case). Using OVD for policy store is not currently supported.

  > **Tip:** This value is available in the *Oracle Fusion Applications Installation Workbook* - Identity Management tab -> Identity Store / Policy Store -> ID Store type (OID/OVD).

- **Use SSL to Communicate With Identity Store**: This feature is not enabled in this release.
- **Identity Store Host**: Enter the host or DNS name for your identity store LDAP service. This can be the host name of the identity server or the host name for the load balancer endpoint load balancing multiple identity servers.
- **Identity Store Port**: The port assigned to the identity store. This can be the port of the identity server or the port for the load balancer endpoint load balancing multiple identity servers.

  > **Tip:** The value for the Identity Store Port is available in the *Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Identity Management Port Numbers and will depend on the Identity Store Server Type defined previously (OID or OVD).

- **Identity Store Secure Port**: The SSL port assigned to the identity store. This feature is not enabled for this release. This can be the secure port of the identity server or the secure port for the load balancer endpoint load balancing multiple identity servers.
- **Identity Store User DN**: Enter the Distinguished Name of the user that you set up with read-write access to the LDAP.
- **Identity Store Password**: Enter the password that you set up for the user with read-write access to the LDAP.
- **Identity Store Read-only User DN**: Enter the Distinguished Name (DN) of the user that you set up with read-only access to the Identity Store LDAP.
- **Identity Store Read-only Password**: Enter the password that you set up for the identity store read-only user.
- **Identity Store User Name Attribute**: Choose the type of user name attribute that you configured in the identity store. Valid values are: user ID (uid), common name (CN), or email address.
- **Identity Store User Base DN**: Enter the root Distinguished Name assigned to the upload of applications user data. This is the root for all the user data in your identity store.
- **Identity Store Group Base DN**: Enter the root Distinguished Name for all the group data in your identity store.
- **OIM Admin Server Host**: Enter the name of the host where the OIM Administration Server is installed.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook*:

  For Basic topology: Topology tab -> Topology -> Abstract Hostname (or Real if abstract is blank) for node that corresponds the IDM Identity and Access component.

  For Enterprise/ Enterprise HA topology: Network - Virtual Hosts tab -> AdminServer Virtual Hosts/VIPs -> IDMDomain AdminServer.

- **OIM Admin Server Port**: The port where the Oracle Identity Management Administration Server listens.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Identity Management Port Numbers ->IDMDomain AdminServer.

- **OIM Administrator User Name**: Enter the name you set up as the Oracle Identity Management Domain administrator.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Identity Management tab -> Identity Store / Policy Store -> IDM Super User Name.

- **OIM Administrator Password**: Enter the password you set up for the Oracle Identity Management Domain administrator.
- **OIM Managed Server Host**: Enter the virtual or real host name of the Oracle Identity Manager Managed Server where SPML callback and other OIM services are running.

Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Topology tab -> Topology -> Abstract Hostname (or Real if abstract is blank) for node that corresponds to the IDM Identity and Access component.

- **OIM Managed Server Port**: Enter the virtual or real port where the Oracle Identity Manager Managed Server listens.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Identity Management Port Numbers -> IDMDomain OIM.

- **OIM HTTP Internal Endpoint URL**: The internal access point on the Oracle HTTP Server for Oracle Identity Manager services in an Oracle Identity Management enterprise deployment, or the Oracle Identity Manager Managed Server access point for a non-enterprise deployment. This URL is used for HTTP communication between Oracle Fusion Applications and Oracle Identity Manager.

  Enter the HTTP termination address of Oracle Identity Manager, using the following format: `http://host:port`. It terminates at either a load balancer or the Oracle HTTP Server or the Oracle Identity Manager Managed Server.

- **OIM HTTP(S) External Endpoint URL**: The access point to use for accessing the Oracle Identity Manager application using a browser. Note that a non-secure URL is used unless you provide an HTTPS URL.

  Enter the HTTP(S) termination address of Oracle Identity Manager, using the following format: `http(s)://host:port`. It terminates at either a load balancer or the Oracle HTTP Server or the Oracle Identity Management Managed Server.

Note: The wizard warns if the Identity Store credentials are not valid and do not allow a connection to the database. If this warning represents an exception, you can ignore it and continue creating the response file. However, you *must* fix all issues before you start to provision an environment. You cannot successfully run provisioning until all validations have passed.

Tip: This value is available in the *Oracle Fusion Applications Installation Workbook*:

For Basic topology: Topology tab -> Topology -> Abstract Hostname (or real if abstract is blank) for node corresponding to the IDM Identity and Access component.

For Enterprise/Enterprise HA: Network - Virtual Hosts tab -> HTTP LBR Endpoints -> IDM.

12.3.14 Access and Policy Management Configuration

Enter the parameters necessary to integrate applications with a previously installed Oracle Identity Management infrastructure. If you chose to use the values in the IDM properties file (for example, `idmsetup.properties`) on the **IDM Properties File** screen, they appear as defaults in the corresponding fields. You can replace the default values if your original configuration has changed.

Oracle Access Manager Configuration

- **OAM Admin Server Host:** Enter the name of the host where the Administration Server for Oracle Access Manager exists.

Tip: This value is available in the *Oracle Fusion Applications Installation Workbook*:

For Basic topology: Topology tab -> Topology -> Abstract Hostname (or real if abstract is blank) for node corresponding to the IDM Identity and Access component.

For Enterprise/Enterprise HA: Network -Virtual Hosts tab -> AdminServer Virtual Hosts/VIPs ->IDMDomain AdminServer.

- **OAM Admin Server Port:** Enter the port number for the Oracle Access Manager Administration Server.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Identity Management Port Numbers -> IDMDomain AdminServer.

- **OAM Administrator User Name**: Enter the name you assigned this user when you installed Oracle Access Manager.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Identity Management tab -> OAM -> OAM Administrator User Name.

- **OAM Administrator Password**: Enter the password you assigned this user when you installed Oracle Access Manager.
- **OAM AAA Server Host:** Enter the name of the proxy host where the Oracle Access Manager is installed.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Topology tab -> Topology -> Abstract Hostname (or Real if abstract is blank) for node corresponding to the IDM Identity and Access component.

- **OAM AAA Server Port:** The port number for the Oracle Access Manager listener on the OAM proxy host.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Network - Ports tab -> Identity Management Port Numbers -> IDMDomain OAM AAA Server Port.

- **Access Server Identifier:** Name used to identify the Oracle Access Server.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Identity Management tab -> OAM -> Access Server Identifier.

- **Enable Second Primary Oracle Access Manager**: Select this checkbox to name a second Primary Oracle Access Manager for high availability.
- **Second Access Server Identifier**: This defaults to `aaa2`, the name of the second Primary Oracle Access Manager Server.

  Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Identity Management tab -> OAM -> Second Access Server Identifier.

- **Webgate Password**: Specify a password for the Resource WebGate. It must contain at least eight alphanumeric characters and at least one digit or punctuation mark. Retype to **Confirm** the password. If seeding of security data is disabled, the password must be the existing WebGate password.

Oracle Platform Security Services Configuration

- **Default to Identity Store:** The default values of this section depend on whether this field is enabled. If the checkbox is unchecked, which is the default, the **OPSS Policy Store Host, OPSS Policy Store Read-Write User Name** and **OPSS Policy Store Password** fields are empty by default and do not inherit values from your identity store. **OPSS Policy Store Port** defaults to 3060 and **OPSS Policy Store Secure Port** defaults to 3131.

  Note: If you check this checkbox, the Identity Store Server Type cannot be OVD and must be OID. Using OVD for policy store is currently not supported.

  If you check this checkbox, the following fields inherit values from your identity store: **OPSS Policy Store Host**, **OPSS Policy Store Port**, and **OPSS Policy Store Secure Port**.

  A description of related fields follows:

  – **Use SSL to communicate with OPSS Policy Store**: This feature is not enabled in this release.

  – **OPSS Policy Store Host**: Enter the host name for the OID where Oracle Platform Security Services (OPSS) policies are to be seeded if **Default to Identity Store** is unchecked. If **Default to Identity Store** is checked, this value defaults from your identity store. This can be the host name of the policy server or the host name for the load balancer endpoint load balancing multiple policy servers.

  – **OPSS Policy Store Port**: The number of the OID port for the OPSS policy store defaults to 3060 if **Default to Identity Store** is unchecked. If **Default to Identity Store** is checked, this value defaults from your identity store. This can be the port of the policy server or the port for the load balancer endpoint load balancing multiple policy servers.

  – **OPSS Policy Store Secure Port**: The number of the secure port for OID defaults to 3131 if **Default to Identity Store** is unchecked. If **Default to Identity Store** is checked, this value defaults from your identity store. This feature is not enabled for this release. This can be the secure port of the policy server or the secure port for the load balancer endpoint load balancing multiple policy servers.

- **OPSS Policy Store Read-Write User Name**: Enter the Distinguished Name of the user that you set up with write privileges to the OPSS policy store. Check if the common name, `cn=PolicyRWUser`, has already been seeded into Identity Management. If so, enter 'cn=PolicyRWUser,*replace_your_choice_of_identity_store_user_base_distinguish_name_here*'.

- **OPSS Policy Store Password**: Enter the password that you set up for the OPSS policy store user with read-write privileges.

- **OPSS Policy Store JPS Root Node**: This is the Distinguished Name of the node to be used as the OPSS policy root for Oracle Fusion Applications. This field is read-only and the default value is set as cn=FAPolicies.

> **Tip:** This value is available in the *Oracle Fusion Applications Installation Workbook* - Identity Management tab -> LDAP -> FA JPS Root DN.

- **Create OPSS Policy Store JPS Root Node**: Select this option to create the OPSS JPS Root Node. For this release, this option must be enabled.

Identity Management Keystore Configuration

The IDM Keystore file and password value fields are enabled if either the Identity Store, the OPSS Store, or the OIM endpoint is SSL-enabled. These fields are populated by the values from the IDM properties file (`for example,idmsetup.properties`), if you have this file that contains these values. You can also edit these values if the fields are enabled.

- **IDM Keystore File**: Enter the location of the JKS keystore containing the certificates for the Oracle Identity Management components.
- **IDM Keystore Password**: Enter the password that you set up for the IDM Keystore File.

Note: The wizard warns if the OPSS Policy Store LDAP connection and the Keystore connection information is not valid and does not allow a connection to the database. If this warning represents an exception, you can ignore it and continue creating the response file. However, you *must* fix all issues before you start to provision an environment. You cannot successfully run provisioning until all validations have passed.

12.3.15 IDM Database Configuration

Enter the database parameters you established when you installed Oracle Database for the Oracle Identity Manager (OIM). The wizard validates whether the database you installed is a single instance of Oracle Database or Oracle Real Application Clusters (Oracle RAC). For a **Single Instance Database**, enter:

> **Tip:** These values are available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> IDM Database.

- **Host Name**: The name of the host where the OIM database is installed.
- **Port**: The listening port for the database.
- **Service Name**: A unique Oracle Fusion Applications name for the OIM database.

If you have installed Oracle RAC, select **Real Application Clusters Database** and enter the **Service Name** that you specified when you installed this database.

Click **Add** to create a new row for each instance. Select a row and click **Remove** to delete the row. Enter the following information for each instance:

- **Host Name**: The name of the host for each Oracle RAC instance.
- **Port**: The listening port of the database.
- **Instance Name**: The name of the Oracle RAC instance used to manage this database.

Enter the database schema owner and password that you set up to store the Oracle Metadata Services (MDS) Repository data for the Oracle Web Services Policy Manager.

- **Schema Owner**: The owner of the MDS schema in the OIM database that is to be used by the Oracle Web Services Policy Manager.

Tip: This value is available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> IDM Database -> IDM DB Prefix (Value is made up of prefix + _MDS).

- **Schema Owner Password**: The password for the MDS schema.

12.3.16 Summary

Verify that the installation represented on this screen is what you expect. Click **Back** to return to the interview screens that require changes. If you are satisfied with the details presented here, complete the following information:

- **Response File Name**: Specify a unique file name for this response file. This is the executable file that you supply to the wizard when prompted.
- **Provisioning Summary**: Specify a unique name for the summary details file. You cannot use this file to execute the response file.
- **Directory**: Enter the directory where you want to save this response file and the summary file. Choose a location that is visible to all servers accessing shared storage. Ensure that the location is not read-only.

Record the name of the response file and its location. You may want to supply it to your system administrator to use when performing system maintenance tasks.

12.4 Updating an Existing Response File

During the response file creation process, you can create a **partial response file**, which contains an incomplete set of configuration details. To create a partial response file, click **Save** at any point during the interview. When you are ready to continue with the creation of the response file, start the wizard and select **Update an Existing Response File** from the **Installation Options** screen. Page through the screens and continue where you left off.

Clicking **Cancel** is another way to create a partial response file, or, alternatively, exit the wizard without saving any response file details:

1. Start the Provisioning Wizard and choose **Create a New Applications Environment Response File** from the **Installation Options** screen.
2. Begin the interview process and continue to the point where you want to end the session. Click **Cancel**.
3. Choose one of the following options:
   - **Save and Exit**: Save the details that you have created for this response file. Creates a partial response file.
   - **Exit**: Exits the wizard without saving any details. Does not create a partial response file.
   - **Cancel**: Does not exit the wizard and keeps you on the page that you are. You can continue with the interview by returning to the **Welcome** screen in the wizard interview. Does not save the details that you entered and does not create a partial response file.
4. Choose **Save and Exit**. The partial response file is saved in the directory where you started the wizard.

5. When you are ready to add more details to the response file, start the Provisioning Wizard and choose **Update an Existing Response File**. Specify the **Response File** location, or click **Browse** to navigate to the partial response file.
6. Page through the interview screens until you come to the point where you stopped the last session and move through the rest of the interview as described in Table 12–2 until you finish the process.

You can save a partial response file and return to the wizard as many times as necessary to complete it. The wizard does not recognize a response file as being complete or valid until you have clicked **Finish** on the **Summary** screen.

You can also update a completed response file if it has not been implemented. Note that after you select product offerings for a partial or completed response file, you cannot change the mix by updating the response file. You must start a new wizard session and create a new response file.

12.5 What to Do Next

After you have saved the response file, you can return to the **Installation Options** screen and select the **Provision an Applications Environment** option to perform the physical installation. Or, you can create another response file to use for another type of installation, for example, to create a test or demonstration environment.

- To create another response file, repeat the tasks in Section 12.3, "Creating a Response File". Save the new response file.
- To use a response file to provision a new environment, go to Chapter 13.

13

Provisioning a New Oracle Fusion Applications Environment

This chapter describes in detail the tasks necessary to perform a physical installation, configuration, and deployment of the product offerings that you specified in your response file.

This chapter includes the following sections:

13.1 Introduction to Provisioning a New Oracle Fusion Applications Environment

In the response file that you created, you specified the configuration details necessary to run a physical installation of Oracle Fusion Applications product offerings. For full-scale environments, typically the offerings must be provisioned on multiple hosts, and the installation must be run from a shared drive that is accessible to all hosts.

The installation process is run in phases, in an assigned order. You must complete each phase, in order, on each host, before you move to the next phase. All phases must be completed successfully on all the hosts in your environment to create a fully operational applications environment.

13.2 Installation Phases and Types of Hosts in a Multiple-Host Environment

Provisioning provides scripts that read from the response file and take action for each installation **phase** (target). As each phase is run, its progress is tracked on a related screen in the Provisioning Wizard user interface.

Note:

- Run the Provisioning Wizard on the primordial host to create a provisioning response file. If you run the Provisioning Wizard on a non-primordial host to create a provisioning response file, the validation assumes that the host is the primordial host. Ensure that you interpret the validation errors correctly as they may not be applicable to the non-primordial host.
- When provisioning a new environment, you should only run the Provisioning Wizard on the primordial host and the Provisioning Command-line Interface on non-primordial hosts.

Installation phases and the names of the tracking screens are as follows:

- **Preverify**: Checks to see that all prerequisites are present. Tracked on the **Prerequisite Checks** screen.
- **Install**: Installs applications, middleware, and database components. Creates the applications Oracle home directory. Tracked on the **Installation** screen.

  Note: The Install phase must be run sequentially starting with the primordial host then one by one on the other provisioning hosts. A file locking error is displayed if you run the Install phase in parallel from the provisioning hosts because `oraInventory` is shared by the provisioning hosts.

  The database schema owner password complexity check will be run at the end of the Install phase. See Section 8.6.2.2.1, "Database Schema User Password Complexity Rule".

- **Preconfigure**: Prepares application and middleware components for deployment and creates `appid` users and groups. Modifies the Oracle Application Development Framework (Oracle ADF) configuration file to use the database, based on Oracle Metadata Services (MDS) in the applications enterprise archive (EAR) files. Also updates the connections.xml file in all applications EAR files with endpoint information. Tracked on the **Preconfigure** screen.
- **Configure**: Creates and configures Oracle WebLogic Server domains, Managed Servers, and clusters; applies templates; creates and configures data sources, queues, and topics; configures middleware (wiring); and deploys applications product offerings to domains. Tracked on the **Configure** screen.
- **Configure-secondary**: Performs the configure actions on a primary or secondary host or both. If there is no primary or secondary host, or if there is only a primary host, this phase runs, but takes no action. Tracked on the **Configure Primary/Secondary** screen.
- **Postconfigure**: Performs online tasks, such as configuring the Node Manager, deploying the service-oriented architecture (Oracle SOA Suite) composite, establishing Oracle HTTP Server wiring, seeding policies, and setting up postdeployment security configuration. Tracked on the **Postconfigure** screen.
- **Startup**: Starts the Administration Server and Managed Servers for each domain on the host where you are running this phase. Tracked on the **Startup** screen.

- **Validate**: Performs a variety of postprovisioning validations, such as server and application availability, successful loading of identity credentials, and validation of data source. Tracked on the **Validation** screen.

> **Note:** Actions related to Oracle Identity Management components are performed only in specific phases. See Section 10.3.2, "Installation Phase Actions for Oracle Identity Management Components" for details.

A cleanup and restore phase runs automatically if a failure occurs:

Cleanup: Shuts down processes started during a failed phase and performs the necessary cleanup actions. If the automated cleanup fails, you must manually stop all processes except the Node Manager on all hosts including OPMN and Java EE processes before you can run the restore action. Note, however, that you must stop *all* processes if you are running the cleanup action on the configure phase.

Restore: The necessary restore actions required for a given provisioning phase. This action deletes and restores the instance directory, and, if necessary (and available), restarts the Common domain Administration Server and Oracle HTTP Server.

See Section 14.4, "Recovery After Failure" for more information about cleanup and restore actions.

The number of hosts and their purpose determines the order in which you provision the applications environment.

- **Primordial host**: Location of the Common domain (specifically the Administration Server of the Common domain). Only one primordial host exists in each environment.
- **Primary host**: Location where the Administration Server for a domain runs. Only one primary host exists in a domain.
- **Secondary host**: Location where the Managed Servers for any application reside when they are not on the same host as the Administration Server of the same domain. The term, secondary host, is meaningful when a domain spans across more than one physical server. The server(s) that does not have the administration server is(are) called secondary host(s).
- **DMZ host**: A host that cannot access the shared storage within the firewall is said to be in a demilitarized zone (DMZ). Typically used to install Oracle HTTP Server so that restrictions on communication with components within the firewall can be enforced. See Section 6.4, "Setting Up a Demilitarized Zone (DMZ) for the Web Tier" for more information.

> **Note:**
>
> - Run the Provisioning Wizard on the primordial host to create a provisioning response file. If you run the Provisioning Wizard on a non-primordial host to create a provisioning response file, the validation assumes that the host is the primordial host. Ensure that you interpret the validation errors correctly as they may not be applicable to the non-primordial host.
> - When provisioning a new environment, you should only run the Provisioning Wizard on the primordial host and the Provisioning Command-line Interface on non-primordial hosts.

13.3 Prerequisites to Provisioning a New Oracle Fusion Applications Environment

Before you begin the physical installation, ensure that you have completed:

- All setup details as described in Chapter 5
- All installation tasks associated with your transaction database as described in Chapter 8
- A response file with the required configuration details as described in Chapter 12

For Linux and Solaris platforms only:

Copy the required GCC library for your hardware platform to the *repository_location*/installer/webgate directory.

For SUSE Linux Enterprise Server 11 (Linux x86-64 SLES 11), you must ensure the following 32-bit libraries are available before provisioning a new environment. Otherwise, the user will encounter an error during installation:

- glibc-devel-32bit-2.9-13.2
- libgcc43-4.3.3_20081022
- libstdc++43-4.3.3_20081022-11.18
- gcc-32bit-4.3
- libaio-32bit-0.3.104
- libaio-devel-32bit-0.3.104
- libstdc++43-32bit-4.3.3_20081022
- libstdc++43-devel-32bit-4.3.3_20081022

In addition, you also must be able to use terminal sessions, which will enable you to alternate between running each phase on the primordial host (using the Provisioning Wizard) and running the phases on the primary and secondary hosts (using the command line).

13.4 Provisioning a New Environment on Multiple Hosts

To provision a new environment, you start the Provisioning Wizard on the primordial host, make a selection from the options menu, and indicate the location of the response file. The wizard presents a review of the details in the response file on a series of interview screens.

You can make changes to most of the response file details on the interview screens. However, you cannot make any changes to the product offerings. You must create a new response file to change the offering mix.

After you have completed the preverify phase successfully on all the hosts in your environment, and clicked **Next** to start the install phase on the primordial host, you can no longer modify any sections of the response file.

You must run the phases *in order*, and complete *each* phase on *all* hosts in your environment before you begin the next phase. The Provisioning Wizard enables you to monitor the progress and success of each phase across all hosts.

> **Note:** If you set up a separate DMZ host for your web tier, you must open a separate terminal session for that host and run all provisioning phases (except the preverify phase). To ignore preverify phase errors, use the command line argument '-ignoreSysPrereqs true' in the runProvisioning command. You cannot view the build processes on the DMZ host on the primordial host interface because the DMZ host does not have access to the shared network drive.

For example, if you have three hosts — Host A (primordial host), Host B (primary host) and Host C (secondary host) — the process of provisioning those hosts works like this:

1. Open a terminal session on Host A, Host B, and Host C. Log in to each host.
2. Start the Provisioning Wizard on Host A, select **Provision an Applications Environment**, and specify the location of the response file.
3. Page through the wizard screens and make any necessary changes to the response file details displayed. If you selected to view individual domain details on the **Provisioning Configuration** screen, those screens are also added to the interview. Review the summary of installation actions that will be taken for this response file.
4. When you click **Next** on the **Summary** screen, the wizard initiates the preverify phase on Host A and displays the **Prerequisite Checks** screen. You can track the progress of this phase on this screen.
5. From the command line on the Host B and Host C terminal sessions, enter the syntax to run the preverify phase. (You do not have to wait for a phase to run to completion on the primordial host before you start the same phase on any of the other hosts.)
6. View the results of the preverify phase for all hosts on the **Prerequisite Checks** screen. The **Next** button will not be enabled until the preverify phase has been completed successfully on all hosts. Click **Back** to navigate through previous screens to fix errors. You must resolve all errors before you can continue.

> **Note:** After you click **Next** to move to the **Installation** screen (the **install** phase), you can no longer go back to previous screens.

7. When there are no errors, click **Next** to initiate the install phase on Host A.
8. From the command line on the Host B and Host C terminal sessions, enter the syntax to run the install phase.
9. View the results on the **Installation** screen on Host A. When the phase has been completed successfully on all hosts, click **Next** on the Installation screen to initiate the next phase and display the next tracking screen. The phases are listed in Section 13.2, "Installation Phases and Types of Hosts in a Multiple-Host Environment".
10. Repeat this process for the remaining phases until all have been completed successfully.

> **Note:** A full backup of the provisioning and configuration state is performed automatically at the end of each successfully completed phase. The backup is saved in *APPLICATIONS_BASE*/restart/.

13.5 Performing the Installation

To provision your environment, start the Provisioning Wizard and page through the installation screens to initiate each phase and monitor the build processes. Note that Oracle Fusion Middleware Oracle homes and Oracle Fusion Applications Oracle home are read-only, and customers are not expected to update or install any components manually to these home directories. These home directories can be updated only by Oracle Fusion Applications lifecycle tools, such as Provisioning, RUP Installer, and Patch Manager.

Note: If you ignored any warnings during the creation of the response file, you must fix all issues stated in the warnings before you can successfully provision an environment. You can make those changes in this installation interview. The wizard saves the changes to your original response file and proceeds with the new instructions. All validations must pass before you can run the **install** phase.

13.5.1 Starting the Wizard and Preparing to Install

Ensure that you created the inventory pointer file (`oraInst.loc`) when you installed the provisioning framework. If you created the file in `/etc`, you can ignore the `-invPtrLoc` command line argument. If you created the file in another location, you must add the `-invPtrLoc` argument to the command line syntax and indicate the location of the inventory. See Section 13.5.6.

To start provisioning your new environment:

1. Open a terminal session and log in to the primordial host.
2. Open a terminal session and log in to each of the other hosts in your environment, including the DMZ host (if present).
3. Set the *JAVA_HOME* environment variable to point to the JDK location in the provisioning repository. For example:

   UNIX:

   ```
   export JAVA_HOME=repository_location/jdk6
   export PATH=$JAVA_HOME/bin:$PATH
   ```

   AIX:

   ```
   export JAVA_HOME=repository_location/jdk6
   export  PATH=$JAVA_HOME/bin:$PATH
   export  SKIP_ROOTPRE=TRUE
   export  SKIP_SLIBCLEAN=TRUE
   ```

   Windows:

   ```
   set JAVA_HOME=repository_location\jdk6
   set  PATH=%JAVA_HOME%\bin;%PATH%
   ```

Note: Verify the system path (PATH) to ensure the reference to the directory "Program Files (x86)" is replaced with its corresponding short path name so that the required tools pick it up properly. If there are references to "Program Files (x86)" (due to the extra space), the Provisioning Configure phase will fail on Microsoft Windows 7 and Windows 2008 Server R2.

4. Verify that the LIBPATH value is null.
5. On UNIX systems, set the DISPLAY environment variable to an active and authorized display.
6. Run the following command on the primordial host:

   UNIX:

   ```
   cd framework_location/provisioning/bin
   ./provisioningWizard.sh
   ```

   On Solaris, use `bash provisioningWizard.sh` instead of `./provisioningWizard.sh`.

   Windows:

   ```
   cd framework_location\provisioning\bin
   provisioningWizard.bat
   ```

Note: Ensure that provisioning on Microsoft Windows platforms is performed from a **Run as Administrator** console. By default, the command prompt has the necessary privilege set. If not, you can run the **Run as Administrator** option by right-clicking the Command Prompt from the Start menu.

Note: For Microsoft Windows platforms, ensure that the Provisioning Wizard is started from the following location: *framework_location*`\provisioning\bin`. If the Provisioning Wizard is not run from this location, you will encounter errors for backup operations initiated during the provisioning process.

13.5.2 Installing Oracle Fusion Applications

Table 13–1 illustrates the steps required to provision a new environment on multiple hosts. Notice that after you run the first phase (preverify) on all hosts, the steps to run the remaining phases are the same. Move to each subsequent phase, in the assigned order.

Note: In the table, UI denotes a step performed in the Provisioning Wizard, and CLI denotes a step performed on the command line.

For help with any of the Provisioning Wizard screens, click **Help** on any Provisioning Wizard interview screen.

Note: When you are running the Provisioning Wizard to provision an applications environment and any issue occurs during provisioning, the error and warning messages are displayed at the bottom of the screen.

Note: Ensure that provisioning on Microsoft Windows platforms is performed from a Run as Administrator console. By default, the command prompt has the necessary privilege set. If not, you can run the Run as Administrator option by right-clicking the Command Prompt from the Start menu.

Table 13–1 Provisioning a New Applications Environment

Interface (UI or CLI)	Action Required
UI: Welcome Screen	No action is required on this read-only screen. Click **Next** to continue.
UI: Specify Central Inventory Location	This screen displays only if one or more of the following conditions are not met: ■ The `-invPtrLoc` option is used to specify the central inventory location on non-Windows platforms, so the default value for your platform is not used. Note that the default for Linux and AIX platforms is `/etc/oraInst.loc` and for Solaris, it is `/var/opt/oracle/oraInst.loc`. ■ The Central Inventory Pointer File is readable. ■ The Central Inventory Pointer File contains a value for `inventory_loc`. ■ The `inventory_loc` directory is writable. ■ The `inventory_loc` directory has at least 150K of space. ■ `inventory_loc` is not a file. Specify the location of the **Central Inventory Directory** that meets the previous criteria. The `inventory_loc` directory can be created by the `createCentralInventory.sh` script and does not have to exist at the time you specify its location. For non-Windows platforms, in the **Operating System Group ID** field, select or enter the group whose members will be granted access to the inventory directory. All members of this group can install products on this host. Click **OK** to continue. The **Inventory Location Confirmation** dialog prompts you to run the *`inventory_directory`*`/createCentralInventory.sh` script as root, to confirm that all conditions are met and to create the default inventory location file, such as `/etc/oraInst.loc`. After this script runs successfully, return to the interview and click **OK** to proceed with the installation. If you do not have root access on this host but want to continue with the installation, select **Continue installation with local inventory** and click **OK** to proceed with the installation. Note that the directory specified for `inventory_loc` in the `oraInst.loc` file must be created already. Otherwise, the preverify phase reports this as an error and you must correct it by creating the directory in the file system before you can continue. For Windows platforms, this screen displays if the inventory directory does not meet requirements. For more information about inventory location files, see "Oracle Universal Installer Inventory" in the *Oracle Universal Installer and OPatch User's Guide*. Click **Next** to continue.
UI: Installation Options Screen	Presents the list of valid installation options that you can perform using the Provisioning Wizard. Select **Provision an Applications Environment**. Enter the path in the **Response File** field to the response file you want to use to provision the environment. Or click **Browse** to navigate to the response file location. Click **Next** to continue.

Table 13–1 (Cont.) Provisioning a New Applications Environment

Interface (UI or CLI)	Action Required
UI: Response File Description Screen	This is the information you entered when you initially created the response file. It is not associated in any way with the executable plan file, or the summary file, that you saved when you finished creating this response file. You can change the response file name, version, and description before you run provisioning, if you like. ■ **Response File Name**: Specify a name to identify this response file. ■ **Response File Version**: Assign a version to this response file. Version numbers are intended only for documentation purposes. ■ **Created By**: Defaults to the operating system user who invoked the wizard. Set when the response file is initially created and cannot be modified for the current response file. ■ **Created Date**: Defaults to the date that the response file was initially created and saved. Set when the response file was initially created and cannot be modified for the current response file. ■ **Response File Description**: Provide a description of this response file. Click **Next** to continue.
UI: Installation Location Screen	Displays the credentials for the Node Manager and the directory locations you entered in the response file. If these values have changed, make corrections on this screen. See Section 13.5.3, "Installation Location Details" for details. Click **Next** to continue.
UI: Review Provisioning Configuration Screen	Lists the wizard interview screens where you originally specified domain-specific parameters for this response file. You can make changes to this information if necessary. **Note**: If you ignored any warnings during the creation of this response file, you must fix all issues stated in the warnings before you can successfully provision an environment. Select any of the screens displayed here to make changes for a product domains with warnings. All validations must pass before you can run the **install** phase. You cannot add or delete product offerings to this response file. To change product offerings, you must create a new response file. Select one or more options from the list. When you click **Next**, the screens you select are added to the flow. Note that if you return to this screen after running the preverification checks, those verification checks are invalidated. You must run the preverify phase again. Click **Next** to continue.
UI: Summary Screen	Review the information displayed to ensure that the installation details are what you intend. To make changes, click **Back** to return to previous screens in the interview. Click **Next** to initiate the **preverify** phase on the primordial host. The wizard displays the **Prerequisite Checks** screen. It also creates a current copy of this response file and saves it in the directory indicated in the message pane. Click **Next** to continue.

Table 13–1 (Cont.) Provisioning a New Applications Environment

Interface (UI or CLI)	Action Required
UI: Prerequisite Checks Screen	The **preverify** phase performs prerequisite checks for Oracle Fusion Applications provisioning on the primordial host. The host is marked with a **Home** symbol in the **Host** column. The **Domains** column lists the domains that are being deployed. After you initiate this phase on the primary and secondary hosts (from the command line), the build processes for those hosts are also shown. The **Status** column indicates the progress of each phase for each host: ■ **Block**: Processing has not yet started on this host for the named phase. ■ **Clock**: Performing the build for a phase. ■ **Check mark**: The build was completed successfully. ■ **x mark**: The build has failed for this phase. You must correct the errors before you can continue. ■ **Restricted** symbol: The validation process has stopped due to a failure within another process. Click an **x** or a **Restricted** symbol to display messages about failures. Click the host-level **Log** file for details about this phase. Click a build **Log** file to see details specific to that build. You can make changes to the interview screens and rerun the **preverify** phase as many times as it is necessary. Note that when you make changes to the response file and rerun **preverify**, Oracle Fusion Applications Provisioning requires that the application configuration directory be empty. Click **Retry** to rerun this phase if errors are reported. You must fix all errors before you continue. Section 14.5, "Troubleshooting Preverify Phase Errors".
CLI and UI: Run the preverify phase on primary and secondary hosts from the command line and monitor progress in the UI.	In the terminal session for the primary and secondary host, run the **preverify** phase with this command: UNIX: *path_to_script*`/runProvisioning.sh -responseFile` *provisioning_response_file_location* `-target preverify` Windows: *path_to_script*`\runProvisioning.bat -responseFile` *provisioning_response_file_location* `-target preverify` **Note**: The same provisioning phases can be run in parallel on all hosts simultaneously if the provisioning process has been started in the primordial host first. However, each new provisioning phase must be run in the specific order listed in Section 13.2, "Installation Phases and Types of Hosts in a Multiple-Host Environment"; that is, you cannot start a new phase until the previous one has been completed successfully on all the hosts in your environment. Monitor the progress of the preverify phase using the **Prerequisite Checks** screen on the primordial host. Click **Retry** to rerun this phase if errors are reported. See Section 14.5, "Troubleshooting Preverify Phase Errors" for details. When this phase is complete with no errors on all hosts, click **Next**. The wizard starts the install phase on the primordial host and displays the Installation screen. When the preverify phase is successful on the primoridal host, place a copy of the response file and the generated provisioning plan (*APPLICATIONS_BASE*`/provisioning/plan/provisioning.plan`) on the DMZ host. **Note:** After you click **Next**, you can no longer modify the response file.
UI: Installation Screen	Displays the progress of the **install** phase on the primordial host. Build messages and **Log** icons track the progress for all phases in the same manner as described for the preverify phase.
CLI and UI: Run the install phase on the primary, secondary, and DMZ (if present) hosts and monitor the progress in the UI.	In the terminal session, run the **install** phase on the primary, secondary, and the DMZ host (if present) with this command: UNIX: *path_to_script*`/runProvisioning.sh -responseFile` *provisioning_response_file_location* `-target install` Windows: *path_to_script*`\runProvisioning.bat -responseFile` *provisioning_response_file_location* `-target install` Monitor the progress on the Installation screen on the primordial host.

Table 13–1 (Cont.) Provisioning a New Applications Environment

Interface (UI or CLI)	Action Required
CLI and UI: Copy the webtier_dmz_artifacts.zip file to the DMZ host (if present).	After the **install** phase response files complete, copy the webtier_dmz_artifacts.zip file from *APPLICATIONS_BASE/* directory on the non-DMZ host to *APPLICATIONS_BASE/* directory on the DMZ host (if present). Click **Next** to initiate the **preconfigure** phase on the primordial host. The wizard displays the **Preconfigure** screen.
UI: Preconfigure Screen	Displays the progress of the **preconfigure** phase on the primordial host.
CLI and UI: Run the preconfigure phase on the primary, secondary, and DMZ (if present) hosts and monitor the progress in the UI.	In the terminal session, run the **preconfigure** phase on the primary, secondary, and the DMZ host (if present) with this command: UNIX: *path_to_script*/runProvisioning.sh -responseFile *provisioning_response_file_location* -target preconfigure Windows: *path_to_script*\runProvisioning.bat -responseFile *provisioning_response_file_location* -target preconfigure Monitor the progress on the **Preconfiguration** screen on the primordial host.
UI and CLI: Initiate the remaining phases (in order) on the primordial, primary, secondary, and DMZ (if present) hosts.	After the **preconfigure** phase reports a successful completion on each host in your environment, return to the primordial host and click **Next** to initiate the next phase. As each new phase is started on the primordial host, on the command line, enter the command to run that phase on the primary, secondary, and DMZ host (if present) on the command line. See Table 13–4 for a list of all the phases, and the command-line syntax. The associated screens, in phase order, are as follows: ▪ **Configure** (**configure** phase) ▪ **Configure Primary/Secondary** (**configure-secondary** phase) ▪ **Postconfigure** (**postconfigure** phase) ▪ **Startup** (**startup** phase) After the phases are complete with no errors, click **Next** on the **Startup** screen to initiate the **validate** phase and then start this phase on the other hosts.
UI: Validation	When the validate phase is complete with no errors on all hosts, click **Next**.
UI: Installation Complete	This screen displays the configuration of the new environment. Click **Finish**. The wizard automatically saves a summary file that describes this installation. The file is saved to the response file directory as follows: *framework_location*/provisioning/provisioning-responseFile/*provisioning_response_file_name-timedate*.summary.

Note that if you are provisioning a new environment on a single host, you can ignore the steps that run from the command line. Each phase starts automatically on the primordial host when you click **Next**.

13.5.3 Installation Location Details

The wizard displays the Node Manager credentials and the locations of the various directories you entered when you created this response file. You can change these values, if necessary.

Node Manager Credentials

- **User Name**: Specify a user name for the Node Manager role.
- **Password**: Specify a password for the Node Manager and retype it in the **Confirm Password** field.

Provide locations of various directories that the administrator needs access to.

Installation and Configuration

- **Installers Directory Location**: Enter the path to the *repository_location* directory you created when you downloaded the provisioning repository. For

Windows, the location must be a symbolically linked directory. See Section 5.3.2.21, "Set Up the Server and the Shared Area Permissions (Windows x64)" for additional details. Note that a symbolic link is not necessary if the repository and the database are on the same node.

- **Applications Base**: Enter the directory path to the Oracle home that you specified when you installed the provisioning framework. This is the Oracle Fusion Applications Oracle home. It is the `root` directory for all Oracle Fusion Applications and Oracle Fusion Middleware products.

  The applications base directory must not be set to the system root directory or set to the root directory of a logical drive. Some lifecycle management tools compute directory names by backing up one directory level from the applications base directory and then appending the appropriate subdirectory name. These tools will fail if the applications base directory is set to the system root directory or set to the root directory of a logical drive because it is not possible to back up one directory level from the system root directory or from the root directory of a logical drive.

  In a UNIX environment, this name cannot exceed 59 characters.

  In a Windows environment, this name cannot exceed eight characters, and must be a symbolically linked directory.

- **Applications Configuration**: This directory is automatically populated based on the value you specify in the **Applications Base** field. It is the path to the directory where the configuration files for the domain will be written. For Windows, the location must be a symbolically linked directory. See Section 5.3.2.21, "Set Up the Server and the Shared Area Permissions (Windows x64)" for additional details.

- **Enable Local Applications Configuration**: Select this checkbox to run the Managed Servers from a non-networked (local) disk on the host, visible only to the processes running on that host. If you enable this option, the wizard copies the domain configuration from the shared location and places it on the local disk you specify. This configures all Managed Servers to run from the non-networked location.

- **Local Applications Configuration**: Specify the location for the local domain directory you want to set up. This field is required if you selected **Enable Local Applications Configuration**. The specified directory must initially be empty.

Middleware Dependencies

- **Font Directory**: Appears only if you have selected Oracle Sales, Oracle Marketing, or Oracle Financials offerings. Enter the directory where the TrueType fonts are installed. The location varies on different operating systems, but is typically found here:

  - **Microsoft Windows x64 (64-bit)**: `C:\WINDOWS\Fonts`
  - **Linux x86-64**: `/usr/X11R6/lib/X11/fonts/TTF`
  - **Oracle Solaris**: `/usr/X11R6/lib/X11/fonts/TrueType`
  - **IBM AIX on POWER Systems (64-bit)**: `/usr/X11R6/lib/X11/fonts/TrueType`

  Some systems may not have TrueType fonts installed. If you cannot locate the fonts on your system, verify that they have been installed. In addition, you can use the fonts directory shipped as part of the JRE installed in the repository. Regardless of which path you specify, you must have access to .ttf (.TTF) files.

Oracle Business Intelligence Repository Password

RPD Password: Specify and **Confirm** a password to allow access to the metadata repository (RPD) for both Oracle Business Intelligence Applications and Oracle Transactional Business Intelligence. The password must be between 8 and 30 characters and contain at least one digit. It can include letters, numbers, pound sign (#), dollar sign ($), or underscore (_). If you want to include two consecutive dollar signs ($$) in the RPD password, enter one additional dollar sign ($) as the escape character before the second dollar sign in the password. This means you need to enter three dollar signs ($$$) for this field in the Provisioning Wizard to indicate two consecutive dollar signs. Provisioning sets up this password, but does *not* actually access the repository.

If the environment created is Windows-based, the wizard prompts for these values:

- ***Windows Domain\Windows User Name***: Specify a user name to use for running provisioning.
- ***Windows Domain* Password**: Specify a password for running provisioning. Retype the password to **Confirm** it.

13.5.4 Oracle Fusion Applications Post-Installation Checklist

This checklist is in addition to the automated validation that takes place during the validate phase of Oracle Fusion Applications Provisioning. For more information, see "Perform Validation Steps" in the *Oracle Fusion Applications Cloning and Content Movement Administrator's Guide*.

The Oracle Fusion Applications Administrator should also perform a final environment validation of the entire stack. Table 13–2 gives a high-level list of such tasks.

Table 13–2 Technical Stack Validation

Component	Task	Expected Outcome
WLS Console (Oracle Identity Management)	Connect to the WLS Console of the IDMDomain using a browser (point directly at the WLS AdminServer port).	You should be able to connect successfully and check the status of the servers in the domain.
EM Console (Oracle Fusion Applications)	Connect to the EM Console of each Fusion Applications Domain using a browser (point directly at the WLS AdminServer port).	You should be able to connect successfully and check the status of the Fusion Middleware components (including BI, WebCenter, ESS, SOA) as well all the Fusion Applications managed servers for each domain.
SSO/Home Page (Oracle Fusion Applications)	Open the Fusion Applications Homepage using a browser (point at the CommonDomain OHS host/port or LBR if your environment has one).	You should be redirected to the OAM SSO login screen. After logging in you should see the Fusion Applications Homepage and no error messages. If you see error message, attempt to refresh the page as they may simply be timeouts since this is the first time the page is being accessed.
Functional Setup	Navigate to Setup and Maintenance page using the Navigator Menu.	You should see the Setup and Maintenance page with no error messages.
Scheduled Jobs	Navigate to the Scheduled Jobs page using the Navigator Menu. *	You should see the Scheduled Jobs page with no error messages.
Reports and Analytics	Navigate to the Reports and Analytics page using the Navigator Menu. *	You should see the Reports and Analytics page with no error messages. Click on the folders to display the available reports.

* If the Scheduled Jobs or Reports and Analytics links do not appear in the Navigator Menu, you will have to enable them in Functional Setup:

- Navigate to **Setup and Maintenance** using the Navigator Menu.

- Use the Search box to search for the **Work Menu**. The results will display on the right and should include **Manage Menu Customizations**.
- Click on **Go to Task** (next to Manage Menu Customizations).
- Find the **Scheduled Jobs** or **Reports and Analytics** menu items on the tree and make sure they are configured as visible/rendered.
- For more information see the *Oracle Fusion Applications Extensibility Guide*.

13.5.5 Performing a Manual Backup

You may want to perform a manual backup, for example, if the automated backup after a phase should fail.

Note: Run these commands for each phase, preverify through postconfigure, and for each host in the environment.

For Linux x86-64:

```
/bin/tar -C $APPLICATIONS_CONFIG/instance -cf $APPLICATIONS_CONFIG/restart/backup_
phase_name/instance.tar
```

If local configuration is enabled, also run these commands for each host:

```
/bin/tar -C $LOCAL_CONFIG/domains -cf $APPLICATIONS_CONFIG/restart/backup_local_
phase_name/hostname/domains/localdomains.tar

/bin/tar -C $LOCAL_CONFIG/applications -cf $APPLICATIONS_CONFIG/restart/backup_
local_phase_name/hosthame/applications/localapplications.tar

/bin/tar -C $LOCAL_CONFIG/biinst -cf $APPLICATIONS_CONFIG/restart/backup_local_
phase_name/hostname/biinst/BIInstance.tar
```

For Microsoft Windows x64 (64-bit):

```
cd $APPLICATIONS_CONFIG/instance
$REPOSITORY\provisioning\util\zip.exe -r $APPLICATIONS_CONFIG\restart\backup_
phase_name\instance.zip
```

If local configuration is enabled, also run these commands for each host:

```
cd $APPLICATIONS_CONFIG\domains\
$REPOSITORY\provisioning\util\zip.exe -r $APPLICATIONS_CONFIG\restart\backup_
local_phase_name\hostname\domains\localdomains.zip

cd $APPLICATIONS_CONFIG/applications\
$REPOSITORY\provisioning\util\zip.exe -r $APPLICATIONS_CONFIG\restart\backup_
local_phase_name\hostname\applications\localapplications.zip

cd $APPLICATIONS_CONFIG/biinst\
$REPOSITORY\provisioning\util\zip.exe -r $APPLICATIONS_CONFIG\restart\backup_
local_phase_name\hostname\biinst\BIInstance.zip
```

For Oracle Solaris:

```
/bin/tar -cEf $APPLICATIONS_CONFIG/restart/backup_phase_name/instance.tar -C
$APPLICATIONS_CONFIG/instance
```

If local configuration is enabled, also run these commands for each host:

```
/bin/tar -cEf $APPLICATIONS_CONFIG/restart/backup_local_phase_
name/hostname/domains/localdomains.tar -C $LOCAL_CONFIG/domains

/bin/tar -cEf $APPLICATIONS_CONFIG/restart/backup_local_phase_
name/hostname/applications/localapplications.tar -C $LOCAL_CONFIG/applications

/bin/tar -cEf $APPLICATIONS_CONFIG/restart/backup_local_phase_
name/hostname/biinst/BIInstance.tar -C $LOCAL_CONFIG/biinst
```

For IBM AIX on POWER Systems (64-bit):

```
cd $APPLICATIONS_CONFIG
/usr/bin/pax -wEf $APPLICATIONS_CONFIG/restart/backup_phase_name/instance.pax -x
pax $APPLICATIONS_CONFIG/instance
```

If local configuration is enabled, also run these commands for each host:

```
/usr/bin/pax -wEf $APPLICATIONS_CONFIG/restart/backup_local_phase_
name/hostname/domains/localdomains.pax -x pax $LOCAL_CONFIG/domains

/usr/bin/pax -wEf $APPLICATIONS_CONFIG/restart/backup_local_phase_
name/hostname/applications/localapplications.pax -x pax $LOCAL_CONFIG/applications

/usr/bin/pax -wEf $APPLICATIONS_CONFIG/restart/backup_local_phase_
name/hostname/biinst/BIInstance.pax -x pax $LOCAL_CONFIG/biinst
```

13.5.6 Using the Command-Line Interface for Installations on the Primary and Secondary Hosts

The installation phases on the primary and secondary hosts are run from the command line, using specific arguments to further define the necessary actions.

13.5.6.1 Adding Arguments to Phase Commands

Table 13–3 shows valid arguments used when running installation phases.

Table 13–3 Command-Line Syntax for Phase Arguments

Syntax	Description
path_to_script	Directory path to the location of the build scripts. This directory was set up when you installed the provisioning framework, for example *framework_location*/provisioning.
-responseFile	You must provide the location of a previously saved response file. Input is: *response_file_location*
-target	Indicates that the script should run a specific installation phase (target). Any *phase_name* is a valid argument, for example, -target perverify.

Table 13–3 (Cont.) Command-Line Syntax for Phase Arguments

Syntax	Description
-ignoreSysPrereqs	Options: true | false Default: false. -ignoreSysPrereqs true is the same as -ignoreSysPrereqs with no value. Adding this argument disables validation for database, schema, and hosts, and enables you to progress to the **install** phase without having to fix failure issues. Checks continue to be performed, but failures are ignored. Can be used as an argument with both the provisioningWizard and the runprovisioning commands. If specified with runprovisioning -target install, the Oracle Universal Installer exceptions are ignored. If you specify this argument for the **preverify** phase, you must specify it for all the remaining phases (**install**, **preconfigure**, **configure**, **configure-secondary**, **postconfigure**, **startup**, and **validate**). If it is not specified for the remaining phases, a phase guard exception will be raised.
-invPtrLoc	Specifies the location of the Oracle Inventory directory, which is used by the installers to keep track of which Oracle products are installed on a host. For example, the runProvisioning command with this argument would be: UNIX: *path_to_script*/runProvisioning.sh -invPtrLoc /home/oracle/oraInst.loc or Windows: *path_to_script*\runProvisioning.bat -invPtrLoc \home\oracle\oraInst.loc.

Note that the -plan argument in previous releases was replaced by the -responseFile argument.

13.5.6.2 Running the Installation Phases

Table 13–4 shows the command-line syntax for running the various installation phases. Ensure that provisioning on Microsoft Windows platforms is performed from a Run as Administrator console. By default, the command prompt has the necessary privilege set. If not, you can run the **Run as Administrator** option by right-clicking the Command Prompt from the Start menu.

> **Note:** In the command syntax, ensure that path_to_script is a local drive and not an UNC path.

Table 13–4 Installation Phase Syntax

Phase (Target)	Command Syntax
Preverify	UNIX: *path_to_script*/runProvisioning.sh -responseFile *provisioning_response_file_location* -target preverify Windows: *path_to_script*\runProvisioning.bat -responseFile *provisioning_response_file_location* -target preverify
Install	UNIX: *path_to_script*/runProvisioning.sh -responseFile *provisioning_response_file_location* -target install Windows: *path_to_script*\runProvisioning.bat -responseFile *provisioning_response_file_location* -target install

Table 13–4 (Cont.) Installation Phase Syntax

Phase (Target)	Command Syntax
Preconfigure	UNIX: *path_to_script*/runProvisioning.sh -responseFile *provisioning_response_file_location* -target preconfigure Windows: *path_to_script*\runProvisioning.bat -responseFile *provisioning_response_file_location* -target preconfigure
Configure	UNIX: *path_to_script*/runProvisioning.sh -responseFile *provisioning_response_file_location* -target configure Windows: *path_to_script*\runProvisioning.bat -responseFile *provisioning_response_file_location* -target configure
Configure-secondary	UNIX: *path_to_script*/runProvisioning.sh -responseFile *provisioning_response_file_location* -target configure-secondary Windows: *path_to_script*\runProvisioning.bat -responseFile *provisioning_response_file_location* -target configure-secondary
Postconfigure	UNIX: *path_to_script*/runProvisioning.sh -responseFile *provisioning_response_file_location* -target postconfigure Windows: *path_to_script*\runProvisioning.bat -responseFile *provisioning_response_file_location* -target postconfigure
Startup	UNIX: *path_to_script*/runProvisioning.sh -responseFile *provisioning_response_file_location* -target startup Windows: *path_to_script*\runProvisioning.bat -responseFile *provisioning_response_file_location* -target startup
Validate	UNIX: *path_to_script*/runProvisioning.sh -responseFile *provisioning_response_file_location* -target validate Windows: *path_to_script*\runProvisioning.bat -responseFile *provisioning_response_file_location* -target validate
Cleanup-*phase_name*	UNIX: *path_to_script*/runProvisioning.sh -responseFile *provisioning_response_file_location* -target cleanup-*phase_name* Windows: *path_to_script*\runProvisioning.bat -responseFile *provisioning_response_file_location* -target cleanup-*phase_name* **Note:** Substitute *phase_name* with the appropriate provisioning phase (install, preconfigure, configure, configure-secondary, or postconfigure) to perform a cleanup action.
Restore-*phase_name*	UNIX: *path_to_script*/runProvisioning.sh -responseFile *provisioning_response_file_location* -target restore-*phase_name* Windows: *path_to_script*\runProvisioning.bat -responseFile *provisioning_response_file_location* -target restore-*phase_name* **Note:** Substitute *phase_name* with the appropriate provisioning phase (install, preconfigure, configure, configure-secondary, or postconfigure) to perform a restore action.

13.6 What to Do Next

After you have completed provisioning a new Oracle Fusion Applications environment, you can proceed to Chapter 14 for troubleshooting instructions.

14

Troubleshooting Your Oracle Fusion Applications Environment

This chapter describes how to troubleshoot your Oracle Fusion Applications environment.

14.1 Introduction to Troubleshooting Your Oracle Fusion Applications Environment

There are various resources available to help with errors that occur during the provisioning of a new Oracle Fusion Applications environment.

14.2 General Troubleshooting Tips

This section describes general troubleshooting tips:

- Oracle Fusion Applications release notes may contain additional information about the latest updates.
- This release of Oracle Fusion Applications relies on certified versions of supported platforms documentation for Oracle Fusion Applications for details about hardware and software, minimum disk space and memory requirements, required system libraries, packages, or patches, and minimum database requirements.
- If you entered incorrect information on one of the installation screens, return to that screen by clicking **Back** until you see the screen.
- When you provision an environment, provisioning writes debug information to the debug directory (*APPLICATIONS_BASE*`/provisioning/debug`).

- Do not delete any files from this directory.
- You can troubleshoot errors using the files in this directory.

14.3 Provisioning Log Files

Log files contain information about both normal and problematic events. They can help you diagnose and address some problems yourself. For example, log messages that state that a service cannot be reached might indicate a hardware failure.

If you discover a more complex issue, My Oracle Support personnel may use log files to trace the execution code paths of relevant requests as part of diagnosing the problem. Log files are particularly helpful if your Oracle Fusion Applications environment contains custom code that needs debugging, especially when using a debugger is not feasible (such as on a production system).

During each provisioning phase, the Provisioning Wizard writes the actions of the build processes to a log file created for each domain. Click the **Log** file icon to see details and error messages. In the log file, you can search for a specific text string, or move forward and backward through the content. The wrap feature enables text to be easily printed, or even forwarded by email.

Provisioning writes log files to the following location:

UNIX:

APPLICATIONS_BASE/logs/provisioning/*host_name*

Windows:

APPLICATIONS_BASE\logs\provisioning*host_name*

This shared location is accessible from all hosts, and contains the following log files:

- `runProvisioning-default-main.log`: The main log file.
- `runProvisioning-`*phase_name*`.log`: The main log file for a given phase, containing the output and error streams. These logs are used by the wizard to keep track of internal information. For example, for runProvisioning-preverify.log, each provisioning thread then writes its own log to runProvisioning-*product_family-phase_name*.log.
- `runProvisioning-`*product_family-phase_name*`.log`: Displayed in the Provisioning Wizard as a **Log** icon for preconfigure, configure, configure-secondary, postconfigure, and startup phases. The files contain detailed information about the phase. For example, runProvisioning-fin-preverify.log contains information about the preverify actions taken while creating the Oracle Fusion Financials domain.

> **Note:** Because all reference roles must be provided in each product log file, you should expect to see duplicate reference role entries.

Provisioning also relies on the Oracle Universal Installer (OUI), which writes log files as follows:

UNIX:

Oracle_Inventory_Location/logs

Windows:

C:\Program Files\Oracle\Inventory\logs.

If you do not know the location of the Oracle Inventory directory, you can find it at:

UNIX: `/etc/oraInst.loc` or

Windows: `C:\Program Files\Oracle\Inventory\logs`. For Windows, if the `Oracle` folder is not present in the program files, the inventory log files are generated under the Oracle Home for the database that is started.

Note that *`APPLICATIONS_BASE`* is the root directory under which the provisioned environment resides. Except for the web tier host, this physical location must be on a shared drive.

In addition to log file locations discussed in this section, note these log file locations associated only with the preconfigure, configure, configure-secondary, postconfigure, and startup phases:

- Oracle WebLogic Server:

  UNIX: *`app.config.dir`*`/domains/`*`host_name/domain_name`*`/servers/`*`server_name`*`/logs`

  Windows: *`app.config.dir`*`\domains\`*`host_name\domain_name`*`\servers\`*`server_name`*`\logs`

- Oracle WebLogic Server Node Manager:

  UNIX: *`APPLICATIONS_BASE`*`/fusionapps/wlserver_10.3/common/nodemanager/`*`host_name/`*

  Windows: *`APPLICATIONS_BASE`*`\fusionapps\wlserver_10.3\common\nodemanager\`*`host_name\`*

14.3.1 Modifying the Default Log Level

The default log level for provisioning is TRACE:1 and NOTIFICATION:1 for messages written to provisioning log files and console, respectively. The definition of loggers controlling the log level for provisioning log files and console are described as:

```
<logger name="runProvisioning-default-main" level="TRACE:1">
   <handler name="default-main"></handler>
  </logger>


 <logger name="runProvisioning-console" level="NOTIFICATION:1">
   <handler name="prov-cons-handler"></handler></logger>
 </loggers>
```

To change the log level, modify the corresponding logger definition in the *`framework_location`*`/provisioning/bin/prov-logging-config.xml` file.

For more information about log level attributes, see "Setting the Level of Information Written to Log Files" in the *Oracle Fusion Middleware Administrator's Guide*.

14.3.2 Default Log Level for Managed Servers

The default log level for standard out, that is, output to the command line console, for managed servers is set to `NOTIFICATION` to provide additional information when investigating issues, particularly around start up for managed servers.

14.4 Recovery After Failure

The wizard performs automated cleanup and recovery actions. If those processes cannot clean up and restore your session, you can perform the actions manually.

See "Starting and Stopping Components in the Oracle Fusion Applications Environment" in *Oracle Fusion Applications Administrator's Guide* for complete instructions for stopping and starting components.

14.4.1 Automated Cleanup and Recovery

Recovery is intended to be systemwide. If a failure occurs on one server, cleanup and recovery steps must be performed on all servers, including the hosts on which the phase completed successfully. During the installation, errors may occur during the running of any of the installation phases. If you must use the abort feature, you may need to perform some cleanup tasks as well.

A **Retry** button is available on each provisioning phase interview screen to initiate cleanup on the primordial host for that phase, or on a non-primordial host if that is where you started provisioning. Initiating the retry operation affects the full phase, beginning with the primordial host or the host from which you started provisioning. The Retry UI explicitly tells you on which hosts you should execute cleanup, and specifies the command to use to run cleanup. A message displays that tells you which host the cleanup target is being run on. If additional cleanup is required on other hosts, those host names are specified after the cleanup target completes. The wizard indicates what cleanup tasks are required, enables the **Continue** button, and waits for you to click **Continue** after you complete the additional cleanup. Clicking **Continue** initiates a process to confirm whether the cleanup is complete. If no additional cleanup is required, the **Continue** button remains disabled, and the wizard starts executing the restore action.

When the restore completes on the current host, a message again displays that tells you which hosts you must execute restore, along with the command to run. The **OK** button is enabled when the restore is done on the current host. When you click **OK**, a process checks again to confirm whether the restore is complete and an error message displays if the restore is not complete. When the restore is done, the phase restarts on the current host if needed. If the phase does not need to run, the retry window closes and the information from the previous run of the phase displays. In the hosts table at the top of the screen, all hosts that were either in a failed or aborted state before you started the retry, will be reset when the retry window closes. Then you must restart the phase from the command line for all hosts with a reset status.

The wizard detects hosts that require cleanup and displays a message informing you of the host names. You must perform the cleanup action from the command line on these hosts before you can initiate any restore action. Command-line syntax for the cleanup action takes the following form:

UNIX: *path_to_script*`/runProvisioning.sh -responseFile` *provisioning_response_file_location* `-target cleanup-`*phase_name*

Windows: *path_to_script*`\runProvisioning.bat -responseFile` *provisioning_response_file_location* `-target cleanup-`*phase_name*

The command-line syntax for the restore action takes the following form:

UNIX: *path_to_script*`/runProvisioning.sh -responseFile` *provisioning_response_file_location* `-target restore-`*phase_name*

Windows: *path_to_script*`\runProvisioning.bat -responseFile` *provisioning_response_file_location* `-target restore-`*phase_name*

These actions are available for the preverify, install, preconfigure, configure-secondary, postconfigure, startup, and validate phases. They are also available for shutdown and deinstall actions.

14.4.2 Running Cleanup and Restore

When a failure occurs during one of the provisioning phases, you must fix the cause of the error and then retry the provisioning phase on the hosts that previously failed using the Provisioning Wizard and the provisioning command-line interface if the failed hosts are primary or secondary hosts.

To retry a provisioning phase, you initiate it starting with the primordial host by clicking **Retry** on the Provisioning Wizard. The wizard starts the cleanup phase on the primordial host.

- When prompted, you must execute a cleanup phase from the command line on each of the hosts that failed the provisioning phase. You can do so simultaneously on all failed hosts.
- After the cleanup phase completes successfully on all the hosts, continue with the restore phase followed by a retry of the provisioning phase. You must start the restore phase first from the primordial host through the Provisioning Wizard, and run the restore phase from the command line on the other hosts from the terminal session. You can do so simultaneously on all hosts.
- After the restore phase is successful on all hosts, you can rerun the failed provisioning phase.

When a failure occurs during one of the provisioning phases, do the following:

1. Click **Retry** to run the cleanup action on the primordial host (Common domain host).
2. If your environment contains additional hosts, the wizard displays a message giving you the names of the other hosts.
3. Run the cleanup action from the command line on the other hosts in the terminal session. This can be done in parallel.

   UNIX: *path_to_script*`/runProvisioning.sh -responseFile` *provisioning_response_file_location* `-target cleanup-`*phase_name*

   Windows: *path_to_script*`\runProvisioning.bat -responseFile` *provisioning_response_file_location* `-target cleanup-`*phase_name*
4. Click **Continue**. If all cleanup steps are completed on **all** hosts where required, the wizard starts the restore action on the primordial host or prompts you to complete steps that have not been completed. Click **Continue** again when finished to start the restore action on the primordial host.
5. If your environment contains other hosts, the wizard displays a message giving you the names of the other hosts.

   Note: On Windows, do not open files in the top-level provisioning directory or any of its descendent directories before you run the restore action.

6. Run the restore action from the command line on the other hosts from the terminal session for each host. This action can run in parallel.

UNIX: *path_to_script*/runProvisioning.sh -responseFile *provisioning_response_file_location* -target restore-*phase_name*

Windows: *path_to_script*\runProvisioning.bat -responseFile *provisioning_response_file_location* -target restore-*phase_name*

7. Click **OK** on the primordial host to start the next phase. The wizard displays the same messages as described in Step 4 if all additional hosts have not been restored.

14.4.3 Handling Cleanup Failures

The automated cleanup and restore actions cannot handle every type of failure. Sometimes manual steps are needed. This is true, for example, when the configure phase fails and any of the following situations exists:

- Node Manager is not yet configured
- Node Manager is configured with an invalid trust key
- Administration Server is not yet registered with the Node Manager
- Administration Server is not running

Under any of these circumstances, the Node Manager will not be able to shut down the Administration Server and the Managed Servers during cleanup-*phase_name*. You must manually shut down all servers before you continue with the restore-*phase_name*.

1. Shut down Web Tier processes, if any, with this command:

   UNIX: *WT_CONFIG*/bin/opmnctl shutdown. To remove the Windows Service, run C:\sc delete OracleProcessManager_CommonDomain_webtier.

   Note: Applies to cleanup-configure, cleanup-configure-secondary, and cleanup-postconfigure.

2. Shut down Oracle Business Intelligence processes, if any, by running:

   UNIX: *BI_CONFIG_HOME*/bin/opmnctl shutdown. To remove the Windows Service, run C:\sc delete OracleProcessManager_BIInstance.

   Note: This applies to cleanup-configure, cleanup-configure-secondary, and cleanup-postconfigure.

3. Shut down Global Order Promising (GOP) (if provisioned) with this command:

   UNIX: *gop_instance_base*/bin/opmnctl shutdown. To remove the Windows service, run: sc delete GlobalOrderPromisingServer1.

   Note: This applies to cleanup-postconfigure.

4. Shut down Informatica Identity Resolution (IIR) processes, if any, by running these two scripts **in the order listed**:

   a. *APPLICATIONS_BASE*/informaticaIR/bin/idsdown

   b. *APPLICATIONS_BASE*/informaticaIR/bin/lidown

   Note: This applies to cleanup-postconfigure, if IIR is provisioned.

5. Shut down Java EE applications using the method recommended for the Oracle WebLogic Server. See "Starting and Stopping Java EE Applications Using WLST" in *Oracle Fusion Applications Administrator's Guide* for details.

   Note: This applies to cleanup-configure, cleanup-configure-secondary, and cleanup-postconfigure.

6. Shut down Node Manager only if it was not configured correctly.

Errors during cleanup of a target produce messages that inform you of the error and display the contents of the associated log file. If you scroll through a message, you can view additional messages, including the manual steps that you should take to fix the problem.

Note that failures during `cleanup-install` require the following specific cleanup tasks:

1. Run the Oracle Universal Installer deinstall process for each component against the same `oraInventory` that provisioning uses. See the Oracle Universal Installer and OPatch User's Guide for information.
2. Delete the install phase guards. You can find them under *`APPLICATIONS_CONFIG`*`/provisioning/phaseguards/`.
3. Windows: Delete the following key from the Windows registry before re-running provisioning:

   `HKEY_LOCAL_MACHINE/SOFTWARE\Wow6432Node\oblix\oblixNetPoint\10.1.4\WebGate\`*`install_directory`*

   If this step is not completed, WebGate will not be installed properly and will generate the following error during the configure-secondary phase:

   `webgate-build.xml:928: The directory` *`appbase`*`\webgate\access\oblix\apps\common\bin does not exist.`

14.4.4 Handling Remnant Processes

Provisioning cannot reliably stop all grandchild processes associated with failures during the running of a phase. Occasionally, remnant processes are present after a failure. Oracle recommends that you manually check and stop all remnant processes that start from the *`APPLICATIONS_BASE`* and the *`framework_location`*`/provisioning` folder, except for Node Manager and the Provisioning Wizard.

Take this action after you complete the cleanup action for any phase, and before you run a restore action for that phase. Without this additional cleanup action, you may experience unwanted interference with the restore action and subsequent rerun logic. This is especially true for long-running child processes such as LDAP policy migration.

You can identify remnant processes in the *APPLICATIONS_BASE* as follows:

Linux: `ps -ef | grep` *`APPLICATIONS_BASE/folder_name`*

Windows: `wmic process get Processid,Commandline,Description | find` *`APPLICATIONS_BASE/folder_name`*

You can identify remnant processes in the *`framework_location`*`/provisioning` folder as follows:

Linux: `ps -ef | grep` *`framework_location`*`/provisioning/`*`folder_name`*

Windows: `wmic process get Processid,Commandline,Description | find` *`framework_location/provisioning/folder_name`*

Remember, do *not* stop the Node Manager and UI processes.

14.4.5 Handling Restore Failures

If the automated restore operation fails, you must complete these manual steps for all phases, except as noted:

1. Delete the restart phase guard (*phase_name*.grd) file associated with the failure. It is located under *APPLICATIONS_BASE*/restart/.
2. You must restore the instance directory from the backup, located as follows:

   UNIX: *APPLICATIONS_BASE*/restart/backup_*phase_name/*instance.tar

   Windows: *APPLICATIONS_BASE* \restart\backup_*phase_name*\instance.zip

   IBM AIX on POWER Systems (64-bit): *APPLICATIONS_BASE*/restart/backup_*phase_name/*instance.pax

   Execute the following commands to restore the instance directory:

   UNIX:

   rm -rf *CONFIG_HOME*

   mkdir *CONFIG_HOME*

   tar -xfv *path_to_instance*.tar/instance.tar -C *CONFIG_HOME*

   Windows:

   rm -rf *CONFIG_HOME*

   mkdir *CONFIG_HOME*

   cd *CONFIG_HOME*

   framework_location\provisioning\util\unzip.exe *path_to_instance*.zip\instance.zip -d .

   IBM AIX on POWER Systems 64-bit:

   rm -rf *CONFIG_HOME*

   mkdir *CONFIG_HOME*

   cd $*CONFIG_HOME*

   pax -rEf *path_to_instance*.pax/instance.pax -x pax -*p e*

3. When a local application configuration has been enabled, you must manually restore the localdomains and localapplications configuration directories on every *local_application_config_host*:

   UNIX: *APPLICATIONS_BASE*/restart/backup_*phase_name/local_application_config_host*/localdomains.tar and...

   UNIX: *APPLICATIONS_BASE*/restart/backup_*phase_name/local_application_config_host*/localapplications.tar

   Windows: *APPLICATIONS_BASE*\restart\backup_*phase_name**local_application_config_host*\localdomains.zip and...

   Windows: *APPLICATIONS_BASE*\restart/backup_*phase_name**local_application_config_host*\localapplications.zip

   IBM AIX on POWER Systems 64-bit: *APPLICATIONS_BASE*/restart/backup_*phase_name/local_application_config_host*/localdomains.pax

   IBM AIX on POWER Systems 64-bit: *APPLICATIONS_BASE*/restart/backup_*phase_name/local_application_config_host*/localapplications.pax

In addition, restore the following file related to Oracle Business Intelligence:

UNIX: *APPLICATIONS_BASE*/restart/backup_*phase_name*/*local application_config_host*/biinst/BIInstance.tar

Windows: *APPLICATIONS_BASE*\restart\backup_*phase_name**local application_config_host*\biinst\BIInstance.zip

IBM AIX on POWER Systems 64-bit: *APPLICATIONS_BASE*/restart/backup_*phase_name*/*local application_config_host*/biinst/BIInstance.pax

4. For `restore-configure-secondary` and `restore-postconfigure` only, start the CommonDomain Administration Server. See "Starting an Administration Server Using WLST and Node Manager" in Table 4-1 of *Oracle Fusion Applications Administrator's Guide* for complete instructions for stopping and starting components.
5. For `restore-postconfigure` only, start Oracle HTTP Server by running *WT_CONFIG_HOME*/bin/opmnctl startall. Oracle HTTP Server must be started from the host where it is installed. It cannot be started from any other host.
6. For `restore-configure` and `restore-postconfigure`, check the restore logs to see if the Oracle Business Intelligence schema restore operation is complete. Perform the restore operation for the database contents first.
7. To restore the Oracle Business Intelligence schema from backup, perform the following actions:
   a. Drop all tables in `FUSION_BIPLATFORM`, if you have not done so already. Drop only the tables — not the schema user.
   b. Run the following stored procedure as the `FUSION_BIPLATFORM` user. For `restore-configure`, use biplatform-preconfigure.dmp as the *v_dump_file_name*. For `restore-postconfigure`, use biplatform-configure-sec.dmp:

```
DECLARE
v_schema_name VARCHAR2(30) := 'FUSION_BIPLATFORM';
v_directory VARCHAR2(30) := 'FUSIONAPPS_PROV_RECOVERY_DIR';
v_dump_file_name VARCHAR2(30) := <biplatform-preconfigure.dmp or
biplatform-configure-sec.dmp>;
v_unique_job_name VARCHAR2(50) := <unique identifying job name e.g. Manual
BI
Schema Restore>;
v_temp_schema_name VARCHAR2(40) := 'IN (''' ||  v_schema_name || ''')';
v_handle NUMBER;
v_job_state VARCHAR2(30);
BEGIN
v_handle :=
DBMS_DATAPUMP.open('IMPORT','TABLE',NULL,v_unique_job_name,'COMPATIBLE');
DBMS_DATAPUMP.add_file(v_handle,v_dump_file_name,v_directory);
DBMS_DATAPUMP.metadata_filter(v_handle,'SCHEMA_EXPR',v_temp_schema_name);
DBMS_DATAPUMP.start_job(v_handle);
DBMS_DATAPUMP.wait_for_job(v_handle,v_job_state);
DBMS_DATAPUMP.detach(v_handle);
END;
```

If LDAP cleanup fails, perform the following manual tasks:

1. For the preconfigure phase, complete these tasks:.
   - Undo member assignments on Administrators, Operators, and Monitors group nodes.

- Remove AppIDUsers node under user base distinguished name.
- Remove AppIDGroups node under group base distinguished name.
- Remove FusionGroups node under group base distinguished name.
- Remove Administrators, Operators, and Monitors groups under group base distinguished name (if you created them in the response file).
- Remove jpsroot (if you enable it in the response file).

2. For the configure phase, remove the `cn=JPSContext` node (with its children) under the jpsroot node from the policy store LDAP if seeding is enabled. Perform this task on the primordial host.
3. For the postconfigure phase, remove all nodes under jpsroot and recreate the container nodes as well as OPSS credentials that were created in the configure phase:
   - Remove all nodes under jpsroot node.
   - Create a temporary bootstrap domain and bring up its Administration Server.
   - Run `reassociateSecurityStore` for that domain with `join=false` to create a fresh policy domain on LDAP.
   - Since the work completed in the configure phase is undone by the deletion of the policy domain during cleanup, seed OPSS credentials.
   - Bring down the bootstrap domain's Administration Server and delete the domain from the file system.
   - You cannot register this domain with Node Manager. Use the command line to bring up this server.

   Rerun `restore-postconfigure` after you fix any issues. If this does not resolve the issues, you should start from the beginning.

   If you need to manually start Node Managers on the provisioning hosts, for example, when the hosts are restarted due to error or maintenance, refer to Task 3 in "Starting an Oracle Fusion Applications Environment"of *Oracle Fusion Applications Administrator's Guide* for complete instructions for starting Node Manager. The Node Manager is started by provisioning at the beginning of a configure phase. You need to ensure that the Node Manager is running before performing a cleanup/restore action for configure-secondary and later phases.

14.5 Troubleshooting Preverify Phase Errors

You may encounter some errors during the preverify phase. This section details troubleshooting information for the preverify phase errors.

14.5.1 Preverify Phase Prerequisite Condition Failed on Red Hat Enterprise 6

The following error message is displayed during the preverify phase if you install Oracle Fusion Applications on the Red Hat Enterprise 6 platform:

```
[2013-03-22T12:13:01.241+05:30] [runProvisioning-preverify] [NOTIFICATION]
[] [runProvisioning-preverify] [tid: 10]
[ecid:0000JqGpNU12JRbptGc9yX1HIzpD000000,0]
[validateInstallersPrerequisite] Check Name:CertifiedVersions

[2013-03-22T12:13:01.243+05:30] [runProvisioning-preverify] [NOTIFICATION]
[] [runProvisioning-preverify] [tid: 10]
```

```
[ecid:0000JqGpNU12JRbptGc9yX1HIzpD000000,0]
[validateInstallersPrerequisite] Check Description:This is a prerequisite
condition to test whether the Oracle software is certified on the current
O/S or not.

[2013-03-22T12:13:03.175+05:30] [runProvisioning-preverify] [NOTIFICATION]
[] [runProvisioning-preverify] [tid: 10]
[ecid:0000JqGpNU12JRbptGc9yX1HIzpD000000,0]
[validateInstallersPrerequisite] Expected result: One of
oracle-6,oracle-5.6,enterprise-5.4,enterprise-4,enterprise-5,redhat-5.4,re
dhat-4,redhat-5,SuSE-10,SuSE-11

[2013-03-22T12:13:03.178+05:30] [runProvisioning-preverify] [NOTIFICATION]
[] [runProvisioning-preverify] [tid: 10]
[ecid:0000JqGpNU12JRbptGc9yX1HIzpD000000,0]
[validateInstallersPrerequisite] Actual Result: redhat-Red

[2013-03-22T12:13:03.180+05:30] [runProvisioning-preverify] [NOTIFICATION]
[] [runProvisioning-preverify] [tid: 10]
[ecid:0000JqGpNU12JRbptGc9yX1HIzpD000000,0]
[validateInstallersPrerequisite] Check complete. The overall result of
this check is: Failed <<<<

[2013-03-22T12:13:16.718+05:30] [runProvisioning-preverify] [NOTIFICATION]
[] [runProvisioning-preverify] [tid: 10]
[ecid:0000JqGpNU12JRbptGc9yX1HIzpD000000,0] [logStatus] STATE=BUILD_
ERROR!TIMESTAMP=2013-03-22 12:13:16
IST!TARGET=private-preverify-installers-prerequisite!CATEGORY=BUILD_
ERROR!DOMAIN=NONE!HOSTNAME=in-mum-orafus02.corp.capgemini.com!PRODUCTFAMIL
Y=orchestration!PRODUCT=orchestration!TASK=validateInstallersPrerequisite!
TASKID=orchestration.orchestration.BUILD_
ERROR.private-preverify-installers-prerequisite.validateInstallersPrerequi
site!MESSAGE=The OUI installer prerequisite check failed:: Product :
webtier Product : wc Product : soa Product : ecm_bucket2 Product: atgpf
Product : odi Product : fusionapps Product : gop !DETAIL=The OUI installer
prerequisite check failed :: Product : webtier|Product : wc|Product:
soa|Product : ecm_bucket2|Product : atgpf|Product : odi|Product :
fusionapps|Product :
gop|!BUILDFILE=/u04/prov/provisioning/provisioning-build/common-preverify-
build.xml!LINENUMBER=1354!

[2013-03-22T12:13:16.793+05:30] [runProvisioning-preverify] [ERROR]
[FAPROV-01045] [runProvisioning-preverify] [tid: 10]
[ecid:0000JqGpNU12JRbptGc9yX1HIzpD000000,0] *** Validation Error! ***[[]]

[2013-03-22T12:13:16.797+05:30] [runProvisioning-preverify] [ERROR] []
[runProvisioning-preverify] [tid: 10]
[ecid:0000JqGpNU12JRbptGc9yX1HIzpD000000,0] The OUI installer prerequisite
check failed :: Product : webtier[[Product : wc

Product : soa

Product : ecm_bucket2

Product : atgpf

Product : odi

Product : fusionapps

Product : gop
```

```
]]
```

This is caused by an error in the operating system validation. Apply the following workaround to resolve the issue:

1. Locate the file `common-preverify-build.xml` in provisioning framework location, *FRAMEWORK_LOCATION*`/provisioning/provisioning-build/common-preverify-build.xml`.
2. Comment out the following block of code by adding "<!-- comment out per workaround" at the beginning and "-->" at the end, as shown below.:

```
<if>

<isfalse
value="${provisioning.setup.common.core.disable.preverify.prerequisite}
"/>

<then>

<logStatus state="BUILD_STARTED" category="installers"
task="validateInstallersPrerequisite"/>


<!-- bug fix 12771983 -->

<if>

<os family="windows"/>

<then>

<antcall target="private-preverify-installers-prerequisite"/>

</then>

<else>

<trycatch property="error-message">

<try>

<envAntCall target="private-preverify-installers-prerequisite"
AdditionalAntOpts="-d64" RunWlstEnvScript="false"/>

</try>

<catch>

<simulateValidationError message="${error-message}"/>

</catch>

</trycatch>

</else>

</if>


<logStatus state="BUILD_COMPLETE" category="installers"
task="validateInstallersPrerequisite"/>

</then>

</if>
```

TO:

```
<!-- comment out per workaround

<if>

<isfalse value="${provisioning.setup.common.core.
disable.preverify.prerequisite}"/>

<then>

<logStatus state="BUILD_STARTED" category="installers"
task="validateInstallersPrerequisite"/>


<!-- bug fix 12771983 -->

<!-- comment out per workaround

<if>

<os family="windows"/>

<then>

<antcall target="private-preverify-installers-prerequisite"/>

</then>

<else>

<trycatch property="error-message">

<try>

<envAntCall target="private-preverify-installers-prerequisite"
AdditionalAntOpts="-d64" RunWlstEnvScript="false"/>

</try>

<catch>

<simulateValidationError message="${error-message}"/>

</catch>

</trycatch>

</else>

</if>


<logStatus state="BUILD_COMPLETE" category="installers"
task="validateInstallersPrerequisite"/>

</then>

</if>

-->
```

3. Save the file and retry the preverify phase.

14.5.2 Preverify Phase Not Displaying All Validation Errors on non-Primordial Hosts

When there is a build error in the preverify phase in the primordial host, not all validation errors in the non-primordial hosts will be accounted for in the Provisioning Wizard. This is because a build error, which is a much more severe error than validation, occurs in the primordial host before the logic to count validation errors.

After fixing the issue that caused the build error and rerunning preverify phase, the validation errors are counted and displayed correctly. This is normal and expected.

Resolve the issue that caused the build error in the primordial host first and rerun preverify phase to find out if there are other validation errors among the hosts. Fix the validation errors where appropriate until validation errors are resolved before proceeding to the next phase.

14.5.3 Preverify Phase Required Free Space is Higher than Actually Provisioned

During the preverify phase, you may see an error saying provisioning requires more free space for the local application configuration directory in the current host like the log below:

```
[2012-02-03T23:11:27.659-08:00] [runProvisioning-preverify]
[NOTIFICATION] [] [runProvisioning-preverify] [tid: 12]
[ecid: 0000JL7CzeGBDCAnv^n3F11FBDbj000003,0]
[logStatus] STATE=BUILD_ERROR!TIMESTAMP=2012-02-
03 23:11:27PST!TARGET=private-preverify-filesystem-Free-space!CATEGORY=BUILD_
ERROR!DOMAIN=NONE!HOSTNAME=adcdk16!PRODUCTFAMILY=orchestration!PRODUCT=orchestrati
on!TASK=validateFileSystem!TASKID=orchestration.orchestration.BUILD_
ERROR.private-preverify-filesystem-free-space.validateFileSystem!MESSAGE=The file
system /scratch/aime/rc4 only has 44271 MB, but 76800 MB is needed!
DETAIL=The file system /scratch/aime/rc4 only has 44271 MB, but 76800 MB is
needed!BUILDFILE=/net/adcgei13/scratch/aime/rc4/FAINTEG_MAIN_PLATFORMS_
120131.1600/provisioning/provisioning-build/common-preverify-build.xml!LINENUMBER=
1392!
[2012-02-03T23:11:27.698-08:00] [runProvisioning-preverify] [ERROR] [FAPROV-01045]
[runProvisioning-preverify] [tid: 12] [ecid: 0000JL7CzeGBDCAnv^n3F11FBDbj000003,0]
*** Validation Error! ***[[ ]]
```

After provisioning completes, you may find that only a fraction of the required file system is being used. This is normal. The 77 GB free space is the Oracle recommended value derived from the performance benchmark. It includes projection of disks required for storing diagnostic logs and other information in the local domain over a long period.

14.5.4 Preverify Phase Warning

If you are provisioning the Human Capital Management (HCM) application offerings, namely Workforce Development and Workforce Deployment, and the `/mnt/hwrrepo` directory (for Windows: `C:\mnt\hwrrepo`) does not exist, a warning message will be displayed.

- You can continue with the provisioning process if you do not need the Workforce Reputation (HWR) application.
- If the HWR application is required, you need to follow the instructions in Section 5.3.2.9 to prepare the shared mount. You can complete provisioning the environment first then prepare the shared mount before you start using the HWR application.

14.5.5 Preverify Phase Errors (AIX 7.1)

During the **Install** phase on IBM AIX 7.1 POWER systems (64-bit), the following warning from installation of WebGate appears in the provisioning log even if the provisioning host already meets the supported AIX platform requirement.

```
Copyright (c) 1999, 2011, Oracle and/or its affiliates. All rights reserved.
```

```
Reading response file.. Expected result: One of 5300.08,6100.02 Actual Result:
7100.00 Check complete. The overall result of this check is: Failed <<<< Problem:
This Oracle software is not certified on the current operating system.
Recommendation: Make sure you are installing the software on the correct platform.
Warning: Check:CertifiedVersions failed.
```

You can ignore the warning and continue with provisioning process.

14.5.6 Preverify Phase Errors (Windows)

You might encounter the following error while running the preverification phase on Windows systems:

```
"C:\repository_location/installers/database/Disk1/setup.exe": CreateProcess
error=740, The requested operation requires elevation at
java.lang.ProcessBuilder.start(ProcessBuilder.java:460)
```

If you receive this error, disable User Access Control (UAC) or log in as a Local Administrator to the machine where the Provisioning Wizard is not functioning properly.

See http://technet.microsoft.com/en-us/library/dd759070.aspx for information about disabling UAC.

14.5.7 ODI Offline Pre-Verification Fails (Windows)

On Microsoft Windows, if Oracle WebCenter Content Management is not installed properly, ODI Offline Preverification fails in Oracle Fusion Applications Release Update Patches (RUP) Installer.

Oracle WebCenter Content Management install fails with the following error:

```
[C\AT\fusionapps\ecm\ucm\Distribution\Kofax\Autorun.inf  (Access is
denied)]
```

Resolution:

1. Disable Prevent remote creation of autorun files from McAfee ePolicy Orchestrator (ePO) in the FusionApp Windows boxes before starting the RUP Installer.
2. When the install is done, enable it again.

14.5.8 OAM Validation Errors

During the provisioning of a new Oracle Fusion Applications environment, you might encounter the following errors in the provisioning log:

- OAM_Validation: Cannot perform OAM Validation as null
- OAM11G_OAM_ADMIN_USER : Could not validate OAM Admin user

For example, the error log will be displayed as follows:

```
[2012-04-23T10:36:36.040-07:00] [runProvisioning-preverify] [ERROR] [FAPROV-01045]
[runProvisioning-preverify] [tid: 13] [ecid: 0000JRWHGNRFk3A5JbWByf1F_P9m000004,0]
*** Validation Error! ***[[  ]]

[2012-04-23T10:36:36.040-07:00] [runProvisioning-preverify] [ERROR] []
[runProvisioning-preverify] [tid: 13] [ecid: 0000JRWHGNRFk3A5JbWByf1F_P9m000004,0]
List of failed Validation in OIM[[1. OAM_Validation : Cannot perform OAM
Validation as null]]
```

```
[logStatus] STATE=BUILD_ERROR!TIMESTAMP=2012-07-02 10:32:09
PDT!TARGET=common-preverify-security!CATEGORY=BUILD_ERROR!DOMAIN=CommonDomain!
HOSTNAME=<host>!PRODUCTFAMILY=fs!PRODUCT=Functional-Setup!TASK=validateOam!TASKID=
fs.Functional-Setup.BUILD_
ERROR.common-preverify-security.validateOam!MESSAGE=Error 1 : OAM11G_OAM_ADMIN_
USER :  Could not validate OAM Admin user. !DETAIL=Error 1 : OAM11G_OAM_ADMIN_USER
:  Could not validate OAM Admin user
```

Apply the following workaround:

1. Exit the current Provisioning Wizard.
2. Restart the Provisioning Wizard:

   `provisioningWizard.sh -ignoreSysPrereqs true`

   This allows you to proceed to the next provisioning phase after you have resolved all other errors identified by the preverify phase.

   If you also see this error on the non-primordial hosts, add the `-ignoreSysPrereqs true` option before running the `runProvisioning.sh` command.
3. You must use the `-ignoreSysPrereqs true` option in the `provisioningWizard.sh` and `runProvisioning.sh` commands for all subsequent provisioning phases.

14.6 Troubleshooting Install Phase Errors

This section includes troubleshooting information for install phase errors.

14.6.1 Cancelling an Installation in Progress

You can interrupt the installation process while it is in progress by clicking **Cancel**, or by clicking the **X** icon next to a build that has failed. If you click **Cancel**, all processes running in the background are terminated and put in a **Failed** status.

You can start the wizard again after you initiate a **Cancel** action. The wizard detects that the installation has been partially completed, and presents you with two options:

- Resume from where you left off. The wizard asks if you want to resume. Click **Yes**.

  The wizard takes you to the screen where you clicked **Cancel** and created the failure. Restart the installation at that point by clicking the **Retry** button. The wizard performs cleanup and recovery actions for you.
- Clean up the errors manually and rerun the **Provision a New Applications Environment** option for the response file from the beginning.

14.6.2 Install Phase Failed with INST-07221: Specified connect string is not in a valid format Error

When you create a provisioning response file using the Oracle Fusion Applications Provisioning Wizard, if you provide only one RAC node information for the Oracle Fusion Applications database, then you will get the following error during the install phase in the `runProvisioning-install.log`. The error is generated due to a limitation in the Oracle Data Integrator (ODI) installer and you must provide at least two RAC nodes.

```
[2012-08-21T10:40:21.365-04:00] [runProvisioning-install] [NOTIFICATION]
[] [runProvisioning-install] [tid: 31] [ecid: 0000J_9c8_
p7U8lCgvq2So1GCtIP00000M,0] Starting Oracle Universal Installer...[[
```

```
Checking if CPU speed is above 300 MHz. Actual 1600 MHz Passed

Checking Temp space: must be greater than 300 MB. Actual 7107 MB Passed

Checking swap space: must be greater than 512 MB. Actual 14527 MB Passed

Preparing to launch Oracle Universal Installer from
/tmp/OraInstall2012-08-21_10-40-14AM. Please wait ...Log:
/u01/app/oraInventory/logs/install2012-08-21_10-40-14AM.log

Copyright (c) 1999, 2011, Oracle and/or its affiliates. All rights
reserved.

Reading response file..

Verifying data......

[VALIDATION] [ERROR]:INST-07221: Specified connect string is not in a
valid format

[VALIDATION] [SUGGESTION]:Provide the value in the following format.
Format: hostname:port:servicename , For Real Application Cluster Database
hostname1:port1^hostname2:port2@servicename

installation Failed. Exiting installation due to data validation
failure.]]

[2012-08-21T10:40:21.387-04:00] [runProvisioning-install] [NOTIFICATION]
[] [runProvisioning-install] [tid: 10] [ecid: 0000J_
9V7RD7U8lCgvq2So1GCtIP000000,0] [logStatus] STATE=BUILD_
ERROR!TIMESTAMP=2012-08-21 10:40:21
EDT!TARGET=install!CATEGORY=none!DOMAIN=NONE!HOSTNAME=<host.com>!PRODUCTFA
MILY=orchestration!PRODUCT=orchestration!TASK=none!TASKID=orchestration.or
chestration.NONE.install.NONE!MESSAGE=An Error Occured: !DETAIL=The
following error occurred while executing this line:|<FRAMEWORK_
LOCATION>/provisioning/provisioning-build/orchestration-build.xml:3132:
The following error occurred while executing this line:|<FRAMEWORK_
LOCATION>/provisioning/provisioning-build/common-misc-build.xml:109: An
Error Occured: The following error occurred while executing this line:

|<FRAMEWORK_LOCATION>/provisioning/provisioning-build/
base-product-family-build.xml:85: The following error occurred while
executing this line:|<FRAMEWORK_
LOCATION>/provisioning/provisioning-build/fs-build.xml:281: The following
error occurred while executing this line:|<FRAMEWORK_
LOCATION>provisioning/provisioning-build/fs-build.xml:1448: The following
error occurred while executing this line:|<FRAMEWORK_
LOCATION>/provisioning/provisioning-build/base-techstack-build.xml:62: The
following error occurred while executing this line:|<FRAMEWORK_
LOCATION>/provisioning/provisioning-build/
odi-build.xml:326: OUI installer failed: <REPOSITORY_
LOCATION>/installers/odi/Disk1/runInstaller!
BUILDFILE=<FRAMEWORK_LOCATION>/provisioning/provisioning-build/
common-misc-build.xml!LINENUMBER=107!
```

Resolution

You must provide the information for at least two RAC nodes on the **Database Configuration** page of the Provisioning Wizard, save the response file, and then restart the provisioning process to deploy a new Oracle Fusion Applications environment as detailed in the following steps:

1. If the Provisioning Wizard is still active, close the window and exit.
2. Delete the entire contents of the `APPLICATIONS_CONFIG` folder including the folder. This is the location for Oracle Fusion Applications Home displayed on the **Installation Location** page of the Provisioning Wizard. If you enable Local Applications Configuration, ensure that the `Local Applications Configuration` directory and its contents are deleted.
3. Start the Provisioning Wizard and select the **Update an Existing Provisioning Response file** option. Select the existing Provisioning Response file.
4. Navigate to the **Database Configuration** page.
5. If you decide to use a single node RAC database, select **Single-Instance Database** and enter the database host, port and service name. If you decide to use a multi-node RAC database, ensure that the RAC nodes are available and enter the database host, port and service name. If you select **Real Application Clusters Database**, you must enter at least two rows in the table.
6. Complete the remaining steps to finish creating a response file.
7. Follow the instructions to begin provisioning a new Oracle Fusion Applications environment starting with the preverify phase. Note that you do not need to restore the Oracle Fusion Applications database instances or the Oracle Identity Management databases from backup because the provisioning framework does not update the databases at this time.

14.7 Troubleshooting Configure Phase Errors

During the Configure phase on the BI host, you may encounter the following error messages in the BI provisioning log (`runProvisioning-bi-configure.log`):

```
[2013-01-08T12:53:42.693-08:00] [runProvisioning-bi-configure]
[NOTIFICATION] [] [runProvisioning-bi-configure] [tid: 19]
[ecid:0000JkRaUlRFg4G_Ixg8yf1Gv74D00000A,0] <Jan 8, 2013 12:53:41 PM PST>
<Notice>

<Security> <BEA-090078> <User oraclesystemuser in security realm myrealm
has had 5 invalid login attempts, locking account for 30 minutes.> [[<Jan
8, 2013 12:53:42 PM PST> <Error> <oracle.wsm.resources.policymanager>
<WSM-02062> <Unable to retrieve credentials for the specified csf-key
FUSION_APPS_WSM_APPID-KEY oracle.wsm.policymanager.PolicyManagerException:
WSM-02062 : Unable to retrieve credentials for the specified csf-key
FUSION_APPS_WSM_APPID-KEY

at oracle.wsm.policymanager.BeanFactory.
getConfigFromCSF(BeanFactory.java:634)
at oracle.wsm.policymanager.BeanFactory.
populateProperties(BeanFactory.java:1035)
```

This is an incorrect error message which may be displayed intermittently. To continue, you should rerun the configure phase after completing the cleanup-configure phase followed by the restore-configure phase successfully.

14.8 Troubleshooting Postconfigure Phase Errors

The following section describes the steps to troubleshoot Postconfigure phase errors.

14.8.1 Postconfigure Phase Oracle SOA Suite Server Startup Errors

During the Postconfigure phase, you might encounter error messages in the provisioning log for a domain (for example, in `runProvisioning-crm-postconfigure.log`).

```
[2013-12-02T01:51:38.122-08:00] [runProvisioning-crm-postconfigure]
[NOTIFICATION] [] [runProvisioning-crm-postconfigure] [tid: 94]
[ecid:0000KAmi6CyEGRK5IVd9if1Ib5CC00001L,0] Starting serversoa_server1
.....................................................................
.....................................................................
.....................................................................
.....................................Exception while starting server
'soa_server1'[[No stack trace available.

This Exception occurred at Mon Dec 02 01:51:38 PST 2013.

weblogic.management.scripting.ScriptException: Error occured while
performing start : Server with name soa_server1 failed to be started

Problem invoking WLST - Traceback (innermost last):

File "/scratch/aime/FINS_IP/apptop/provisioning/debug/<host_
name>/postconfigure_02_12_13_01_29_43/nodeManagerStartServer_
CRMDomain4661859561054870083.py", line 329, in ?

File "/scratch/aime/FINS_IP/apptop/provisioning/debug/<host_
name>/postconfigure_02_12_13_01_29_43/nodeManagerStartServer_
CRMDomain4661859561054870083.py", line 187, in startServer

File "<iostream>", line 1279, in start

File "<iostream>", line 1847, in raiseWLSTException

WLSTException: Error occured while performing start : Error starting the
server : Error occured while performing start : Server with name soa_
server1 failed to be started

Use dumpStack() to view the full stacktrace
```

This can be because the ODI server and the domain admin server are on different hosts

and

either the ODI server is the last Oracle Fusion Middleware server to be configured

or

the ODI server is isolated on a separate host when you select the **Advanced Topology** option on the Domain Topology Configuration screenduring the creation of the Oracle Fusion Applications provisioning response file to specify the placement of each servers on the provisioning hosts.

Resolution

Follow these steps to resolve the issue.

1. Run `cleanup-postconfigure` and then `restore-postconfigure`.
2. Log in to the respective domain admin console for which server startup failed.
3. Fix the Node Manager details of the host being used by the ODI server. Change the Listen Address of the host to the ODI server address using the following steps:
   a. Select **Environment** -> **Machines** from the **Domain Structure** menu.

b. Click the machine name link.

c. In the **Settings for <a machine name>** window, select **Configuration** -> **Node Manager**.

d. Update the Listen Address by entering the host name of the ODI server address. Click **Lock & Edit** located in the top left corner of the Change Center panel.

e. Enter the host address, click **Save** and then click **Release Configuration**.

f. Continue rerunning the Postconfigure phase.

14.9 Troubleshooting Validate Phase Errors

The following section describes the steps to troubleshoot Validate phase errors.

14.9.1 Validate Phase WebGate Validation Errors

During the Validate phase, you will encounter WebGate validation errors and the error messages in the provisioning log are as follows:

```
[2012-11-18T19:06:13.323-08:00] [runProvisioning-validate] [NOTIFICATION]
[] [runProvisioning-validate] [tid: 11] [ecid:
0000JgMcCTD9lZOLIih8if1GeQ7k000002,0]  [logStatus] STATE=BUILD_
ERROR!TIMESTAMP=2012-11-18 19:06:13
PST!TARGET=private-validate!CATEGORY=BUILD_
ERROR!DOMAIN=CommonDomain!HOSTNAME=<host>!PRODUCTFAMILY=fs!PRODUCT=WebGate
!TASK=validate WebPageStatus!TASKID=fs.WebGate.BUILD_
ERROR.private-validate.validate WebPageStatus!MESSAGE=The HTTP request to
http://<host>:<port>/oberr.cgi?progid=1 returned status: 404.!DETAIL=The
HTTP request to http://<host>:<port>/oberr.cgi?progid=1 returned status:
404.!BUILDFILE=<framework_
location>/provisioning/provisioning-build/webgate-build.xml!LINENUMBER=992
!

[2012-11-18T19:06:52.116-08:00] [runProvisioning-validate] [NOTIFICATION]
[] [runProvisioning-validate] [tid: 11] [ecid:
0000JgMcCTD9lZOLIih8if1GeQ7k000002,0]  [logStatus] STATE=BUILD_
ERROR!TIMESTAMP=2012-11-18 19:06:51
PST!TARGET=private-validate!CATEGORY=BUILD_
ERROR!DOMAIN=FinancialDomain!HOSTNAME=<host>!PRODUCTFAMILY=fin!PRODUCT=Web
Gate!TASK=validateWebPageStatus!TASKID=fin.WebGate.BUILD_
ERROR.private-validate.validateWebPageStatus!MESSAGE=The HTTP request to
http://<host>:<port>/oberr.cgi?progid=1 returned status: 404.!DETAIL=The
HTTP request to http://<host>:<port>/oberr.cgi?progid=1 returned status:
404.!BUILDFILE=<framework_
location>/provisioning/provisioning-build/webgate-build.xml!LINENUMBER=992
!
```

These WebGate web page validation errors can be ignored. If there are any other validation errors, you must resolve them before proceeding to the Summary phase. If the **Next** button on the Provisioning Wizard is not enabled after resolving all validation errors, do the following from the command line to enable it:

1. `cd` *APPLICATIONS_CONFIG*`/provisioning/phaseguards`
2. `rm validate-<host>-FAILED.grd`

3. `touch validate-<host>-COMPLETED.grd`. **Note:** Use the same host name as specified in Step 2.

The **Next** button should be enabled on the Provisioning Wizard.

WARNING: Deleting and creating files in the phase guard directory is necessary as a workaround to resolve validation phase issues ONLY if none of the other options work. In any other case, you should never modify or make changes to the phase guard files.

14.9.2 Validate Phase Topology Manager Service Endpoint Invocation Error

During the Validate phase, you may encounter the following errors:

`INFO: WSM-09004 Component auditing cannot be initialized error` and

```
SEVERE: Error while invoking endpoint
"http://<host>:<7004>/topologyManagerService/ProvisionConfigurationService
" from client.
```

The log messages in the `runProvisioning-fs-postconfigure.log` files are as follows:

```
[2012-12-11T01:24:08.130-08:00] [runProvisioning-fs-postconfigure] [TRACE]
[] [runProvisioning-fs-postconfigure] [tid: 402] [ecid:
0000Ji9Ho1B3r2GLIyT4if1GljTr000069,0] [SRC_CLASS:
oracle.apps.fnd.provisioning.ant.taskdefs.util.logger.ProvisioningLogger]
[SRC_METHOD: log] Attempt 1 of 20 for importProvisionDeployedInfo

[2012-12-11T01:24:10.767-08:00] [runProvisioning-fs-postconfigure] [ERROR]
[] [runProvisioning-fs-postconfigure] [tid: 403] [ecid:
0000Ji9Hp6F3r2GLIyT4if1GljTr00006A,0] INFO: WSM-09004 Component auditing
cannot be initialized.

[2012-12-11T01:24:10.772-08:00] [runProvisioning-fs-postconfigure] [ERROR]
[] [runProvisioning-fs-postconfigure] [tid: 403] [ecid:
0000Ji9Hp6F3r2GLIyT4if1GljTr00006A,0] INFO: WSM-09004 Component auditing
cannot be initialized.

[2012-12-11T01:24:11.676-08:00] [runProvisioning-fs-postconfigure] [ERROR]
[] [runProvisioning-fs-postconfigure] [tid: 403] [ecid:
0000Ji9Hp6F3r2GLIyT4if1GljTr00006A,0] SEVERE: Error while invoking
endpoint
"http://<host>:<port>/topologyManagerService/ProvisionConfigurationService
" from client.
```

This error message occurs when the validation is initiated by the provisioning framework before the Oracle Web Service Manager (OWSM) is fully initialized. The provisioning framework will retry up to a predetermined number of times, therefore such error messages can be ignored. However, if validation fails after 20 attempts, you should investigate the issue.

14.9.3 Validate Phase Group Not Found in OVD

During the Validate phase, you will encounter an `ldapSearch` validation error and the `runProvisioning-validate.log` file will contain the following error messages:

```
[2013-06-04T21:33:25.523-07:00] [runProvisioning-validate] [NOTIFICATION]
[FAPROV-01042] [runProvisioning-validate] [tid: 11] [ecid:
0000JwIb1v20rmG5Izt1if1Hffxu000002,0] [arg: /tmp/clean-559114674.ldif]
```

```
Validating user and group entries in the LDIF file
'/tmp/clean-559114674.ldif' ...

[2013-06-04T21:33:26.249-07:00] [runProvisioning-validate] [NOTIFICATION]
[] [runProvisioning-validate] [tid: 11] [ecid:
0000JwIb1v20rmG5Izt1if1Hffxu000002,0]  [logStatus] STATE=BUILD_
ERROR!TIMESTAMP=2013-06-04 21:33:26
PDT!TARGET=common-validate-global-identities!CATEGORY=BUILD_
ERROR!DOMAIN=CommonDomain!HOSTNAME=slc00veq!PRODUCTFAMILY=fs!PRODUCT=Funct
ional-Setup!TASK=validateLDIFEntries!TASKID=fs.Functional-Setup.BUILD_
ERROR.common-validate-global-identities.validateLDIFEntries!MESSAGE=ldapSe
arch encountered an error while validating the group 'cn=PER_EXECUTIVE_
MANAGER_ABSTRACT,cn=FusionGroups,cn=Groups,dc=us,dc=oracle,dc=com' [LDAP:
error code 32 - LDAP Error 32 : No Such Object] url
-ldap://<host>:<port>!DETAIL=ldapSearch encountered an error while
validating the group 'cn=PER_EXECUTIVE_MANAGER_
ABSTRACT,cn=FusionGroups,cn=Groups,dc=us,dc=oracle,dc=com' [LDAP: error
code 32 - LDAP Error 32 : No Such Object] url
-ldap://<host>:<port>!BUILDFILE=/scratch/aime/ST5REPO/provisioning/provisi
oning-build/common-validate-build.xml!LINENUMBER=1010!

[2013-06-04T21:33:26.264-07:00] [runProvisioning-validate] [ERROR]
[FAPROV-01045] [runProvisioning-validate] [tid: 11] [ecid:
0000JwIb1v20rmG5Izt1if1Hffxu000002,0] *** Validation Error! ***[[  ]]

[2013-06-04T21:33:26.264-07:00] [runProvisioning-validate] [ERROR] []
[runProvisioning-validate] [tid: 11] [ecid:
0000JwIb1v20rmG5Izt1if1Hffxu000002,0] ldapSearch encountered an error
while validating the group 'cn=PER_EXECUTIVE_MANAGER_
ABSTRACT,cn=FusionGroups,cn=Groups,dc=us,dc=oracle,dc=com' [LDAP: error
code 32 - LDAP Error 32 : No Such Object] url -ldap://<host>:<port>

[2013-06-04T21:33:26.264-07:00] [runProvisioning-validate] [NOTIFICATION]
[FAPROV-01046] [runProvisioning-validate] [tid: 11] [ecid:
0000JwIb1v20rmG5Izt1if1Hffxu000002,0] *** The 'Defer On Error' validation
mode is enabled. ***

[2013-06-04T21:33:26.264-07:00] [runProvisioning-validate] [ERROR]
[FAPROV-01002] [runProvisioning-validate] [tid: 11] [ecid:
0000JwIb1v20rmG5Izt1if1Hffxu000002,0] *** Will continue processing of the
next validation task (if any). ***
```

This validation error occurs because the abstract role, `PER_EXECUTIVE_MANAGER_ABSTRACT`, does not have a description in LDAP. This does not have any functional impact. You can ignore this validation error.

14.10 What to Do Next

To prepare your Oracle Fusion Applications installation for functional implementation, you must perform several configuration tasks, some of which are common for all Oracle Fusion Applications or multiple product families, and some are specific to the individual product families or products. The configuration tasks could either be mandatory or conditional, depending on the requirement.

Note: Most of these tasks are not applicable to Oracle Cloud implementations.

Go to Part VII, "Completing Oracle Fusion Applications Post-Installation Tasks" for detailed information about post-installation tasks.

Part VII

Completing Oracle Fusion Applications Post-Installation Tasks

To prepare Oracle Fusion Applications for functional implementation, you must perform several configuration tasks of which some are common for all Oracle Fusion Applications or multiple product families, and some are specific to the individual product families or products. The configuration tasks could either be mandatory or conditional, depending on the requirement.

Note: Most of these tasks are not applicable to Oracle Cloud implementations.

Post-Installation Tasks Checklist

To help keep track of the post-installation tasks, you can print this checklist from the PDF version of this guide. This checklist is also available in the *Oracle Fusion Applications Installation Workbook*.

Section	Task	Applies To	Task Requirement	Task Execution Criteria
Section 15.2	Applying Patches to Your New Environment	All Product Families	Mandatory	N/A
Section 15.3	Upgrading LDAP Users for Single Sign-on	All Product Families	Mandatory	N/A
Section 15.4	Adding Privileges to IDStore and Policy Store Entities	All Product Families	Mandatory	N/A
Section 15.5	Updating the MDS Schema Database Statistics	All Product Families	Mandatory	N/A
Section 15.6	Setting Up Notifications	All Product Families	Mandatory	N/A
Section 16.2	Setting Up Global Search	All Product Families	Conditional	Required only if you want to enable Oracle Secure Enterprise Search-based Global Search for all users.

Section	Task	Applies To	Task Requirement	Task Execution Criteria
Section 16.3	Setting Up Privacy Statement	All Product Families	Conditional	Required only to enable the Privacy Statement link under the Help menu and configure it to link to a user-defined page. By default, the link is disabled.
Section 16.4	Configuring Oracle User Productivity Kit In-Application Support	All Product Families	Conditional	Required to allow users o access the Oracle User Productivity Kit (UPK) content while working with Oracle Fusion Applications.
Section 16.5	Reviewing and Configuring Diagnostic Logging Settings and Diagnostic Testing Features	All Product Families	Conditional	Recommended
Section 16.6	Implementing Compliance Rules	All Product Families	Conditional	Recommended
Section 16.7	Configuring Oracle HTTP Server with Custom Certificates	All Product Families	Conditional	Recommended only for environments provisioned without a LBR, in which case the SSL channel terminates at the HTTP Servers. If not performed, end users will have to confirm acceptance of the default certificate each time they access each virtual hosts in Fusion Applications and Oracle Identity Management.
Section 16.8	Setting Up Backup for Oracle Fusion Applications	All Product Families	Conditional	Recommended
Section 16.9	Setting up Oracle Enterprise Manager Cloud Control to Monitor and Manage Oracle Fusion Applications	All Product Families	Conditional	Recommended if you use Enterprise Manager Cloud Control to Monitor and Manage Fusion Applications.
Section 16.10.1	Updating Oracle Identity Management HTTP Server Runtime Parameters	All Product Families	Conditional	
Section 16.10.2	Post-Provisioning Steps for Oracle Access Manager	All Product Families	Conditional	

Section	Task	Applies To	Task Requirement	Task Execution Criteria
Section 16.10.3	Configuring Oracle Identity Federation	All Product Families	Conditional	Required only if you want to configure OIF as an authentication frontend to Fusion Applications.
Section 16.10.4	Configuring Identity Integration with Active Directory	All Product Families	Conditional	Required only if you want to integrate with Active Directory users and groups.
Section 16.10.5	Setting Up Oracle Identity Management Node Manager for SSL	All Product Families	Conditional	
Section 16.11	Installing and Configuring Oracle Business Intelligence Applications	All Product Families	Conditional	Required to enable Oracle Business Intelligence Applications for Fusion Applications.
Section 16.12	Configuring Oracle Transactional Business Intelligence	All Product Families	Conditional	
Section 16.13	Setting Up Report Delivery Servers	All Product Families	Conditional	Required to configure different types of delivery mechanisms for BI Publisher reports (Printer and Fax, E-mail, WebDAV, HTTP, FTP).
Section 16.14	Setting Up Oracle ADF Desktop Integration	All Product Families	Conditional	Required to allow users to download and upload Fusion Applications data via Microsoft Excel workbooks.
Section 16.15	Configuring Oracle Data Integrator Studio	All Product Families	Conditional	Required for administrators to update the ODI repository.
Section 16.16	Setting Up the Oracle Business Intelligence Administration Tool	All Product Families	Conditional	Required to make chnages to the BI repository (e.g create or modify data sources, etc.).
Section 16.17	Performing Optional Language Installations	All Product Families	Conditional	Required only if you install languages in addition to US English.
Section 16.18	Setting Up Segregation of Duties	All Product Families	Conditional	Required only for using Application Access Controls Governor to check for segregation of duties (SOD) violations when a role assignment is requested through Oracle Identity Management. Requires Fusion GRC.

Section	Task	Applies To	Task Requirement	Task Execution Criteria
Section 16.19	Configuring Presence Servers	All Product Families	Conditional	Required only if you want to enable Presence functionality in Fusion Applications. Requires use of Microsoft Office Communication Server (OCS) 2007 or Microsoft Live Communication Server (LCS) as presence servers.
Section 16.20	Configuring Audit Trails for Oracle Fusion Middleware	All Product Families	Conditional	Recommended if you want to enable middleware auditing capabilities.
Section 16.21	Installing Print Servers	All Product Families	Conditional	Required if you want to use print server functionality in the following products: ▪ Oracle Business Intelligence Financial Reporting Studio and Financial Reporting Print Server ▪ Primavera P6 Enterprise Project Portfolio Management ▪ Informatica Identity Resolution
Section 16.22	Configuring Oracle HTTP Server for Privileged Port (UNIX Only with No Load Balancer)	All Product Families	Conditional	Required only for environments where the Web Tier is installed on Linux on privileged port (< 1024).
Section 17.2	Scaling Identity Management	All Product Families	Conditional	Required only for the Enterprise topology with High Availability implementation
Section 17.3	Setting Up Server Migration for Identity Management	All Product Families	Conditional	Required only for the Enterprise topology with High Availability implementation
Section 18.2	Scaling Oracle Fusion Applications	All Product Families	Conditional	Required only for the Enterprise topology with High Availability implementation
Section 18.3	Setting Up Server Migration for Oracle Fusion Applications	All Product Families	Conditional	Required only for the Enterprise topology with High Availability implementation

Section	Task	Applies To	Task Requirement	Task Execution Criteria
Section 19.1	Installing and Configuring the Bounce Handling Daemon	CRM, Marketing Only	Conditional	Recommended if you want to know which email addresses in your marketing campaigns resulted in the message being bounced back and which campaign members have such email addresses.
Section 19.2	Setting Up SMS Marketing	CRM, Marketing Only	Conditional	Required only for SMS-based marketing campaigns. Requires an account with an SMPP driver gateway vendor.
Section 19.3	Setting Up Informatica Identity Resolution for Data Quality	CRM, All Offerings	Conditional	Required to enable the Data Quality feature.
Section 19.4	Setting Up Sales Prediction Engine	CRM, Sales Only	Conditional	Required for using product recommendations based on data mining and rules for Accounts and Contacts.
Section 19.5	Setting Up Implicit Personalization Behavior	CRM, All Offerings	Mandatory	Required to fix the inconsistent implicit personalization behavior between sessions in the following Oracle Fusion CRM applications: ▪ Oracle Fusion CRM Common ▪ Oracle Fusion Territory Management ▪ Oracle Fusion Customer Center ▪ Oracle Fusion Marketing ▪ Oracle Fusion Order Capture Common Components ▪ Oracle Fusion Sales
Section 20.1	Setting Up the Financial Reporting Center	Financials and Accounting Hub	Conditional	Required only for implementing Financial Reporting Center.
Section 20.2	Setting Up Oracle Document Capture and Oracle Forms Recognition	Financials	Conditional	Required only for implementing Payables Integrated Imaging Solution
Section 20.3	Oracle Fusion Advanced Collections Dunning	Financials	Conditional	Required only if you are using Advanced Collections.

Section	Task	Applies To	Task Requirement	Task Execution Criteria
Section 20.4	Enabling Encryption of Sensitive Payment Information	Financials	Conditional	Recommended only for encrypting employee, customer or supplier bank account information stored in Fusion Applications.
Section 20.5	Configuring a Communication Channel to a Payment System	Financials	Conditional	Required in order to transmit or receive payment information to or from a payment system through a firewall.
Section 20.6	Configuring Oracle B2B Inbound Flow to Receive Supplier Invoices in XML	Financials	Conditional	Required only if you want to setup receiving Payables invoices in OAG XML format.
Section 20.7	Setting Up Oracle B2B to Send Receivables Transactions in XML	Financials	Conditional	Required only if you are using XML Invoicing in Receivables.
Section 21.2	Integrating with Other Products	Accounting Hub	Conditional	Required only for integrating external transactional systems with the Fusion Accounting Hub.
Section 22.1	Recommended Memory Requirement for Oracle Fusion Human Capital Management Workforce Reputation Management Product	HCM	Mandatory	
Section 22.2	Setting Up Oracle Fusion Human Capital Management Coexistence	HCM	Conditional	Recommended if you want to integrate the existing Oracle Human Resource applications (PeopleSoft Enterprise or Oracle E-Business Suite) with Oracle Fusion HCM As a result of the integration, you can use Oracle Fusion Workforce Compensation and Talent Management functionality alongside your existing setup.
Section 22.3	Creating an ISAM Vertex Database	HCM	Conditional	Required only for US and Canadian Payroll setup. Separate license with Vertex required for tax updates.

Section	Task	Applies To	Task Requirement	Task Execution Criteria
Section 23.1	Integrating Oracle Fusion Incentive Compensation with Geo Map Server	Incentive Compensation	Conditional	Required only if you want to use a different provider for MapViewer and GeoMapViewer connections which by default points at Oracle-hosted services.
Section 24.1	Configuring Oracle Fusion Project Portfolio Management Integration with Primavera P6 Enterprise Project Portfolio Management	Projects	Conditional	Required only to integrate Fusion Projects with Primavera P6.
Section 25.1	Installing Oracle Enterprise Data Quality for Product Data Oracle DataLens Server	SCM	Conditional	Required to enable integration between Oracle Enterprise Data Quality for Product Data and Oracle Fusion Product Hub.
Section 26.3	Completing Common User Setup Tasks	All Product Families	Mandatory	N/A

Part VII contains the following chapters:

- Chapter 15, "Completing Mandatory Common Post-Installation Tasks"
- Chapter 16, "Completing Conditional Common Post-Installation Tasks"
- Chapter 17, "Completing Conditional Common High Availability Post-Installation Tasks for Oracle Identity Management"
- Chapter 18, "Completing Conditional Common High Availability Post-Installation Tasks for Oracle Fusion Applications"
- Chapter 19, "Completing Oracle Fusion Customer Relationship Management Post-Installation Tasks"
- Chapter 20, "Completing Oracle Fusion Financials Post-Installation Tasks"
- Chapter 21, "Completing Oracle Fusion Applications Accounting Hub Post-Installation Tasks"
- Chapter 22, "Completing Oracle Fusion Human Capital Management Post-Installation Tasks"
- Chapter 23, "Completing Oracle Fusion Incentive Compensation Post-Installation Tasks"
- Chapter 24, "Completing Oracle Fusion Project Portfolio Management Post-Installation Tasks"
- Chapter 25, "Completing Oracle Fusion Supply Chain Management Post-Installation Tasks"
- Chapter 26, "What To Do Next"

15

Completing Mandatory Common Post-Installation Tasks

This chapter describes the mandatory post-installation tasks you should complete before you can start working with Oracle Fusion Applications.

15.1 Introduction to Completing Mandatory Post-Installation Tasks

After you have successfully completed the installation phases on all the hosts in your environment, perform the following required manual steps described in this chapter.

Some components in the Oracle Fusion Applications environment are dependent on one another. Therefore, it is important to start and stop components in the proper order. In the course of normal IT operations, common operations include shutting down computers and starting them back up. Therefore, it is crucial to start and stop Oracle Fusion Applications in a sequential manner. For more information, see "Starting and Stopping the Entire Oracle Fusion Applications Environment" in the *Oracle Fusion Applications Administrator's Guide*.

15.2 Applying Patches to Your New Environment

Refer to Oracle Fusion Applications release notes for mandatory post-installation steps, including the application of all mandatory patches. For general information about applying patches to an applications environment, see *Oracle Fusion Applications Patching Guide*.

15.3 Upgrading LDAP Users for Single Sign-on

Create a file called `upgradeLDAPUsersForSSO.props` with the following contents. This file is only for the IDSTORE user.

Note: You do not need to complete this step if your Oracle Fusion Applications environment is created from the certified Oracle Fusion Applications Oracle VM templates or the environment is not created by following the instructions in this installation guide.

```
IDSTORE_DIRECTORYTYPE: OID
IDSTORE_HOST: idstore.mycompany.com
IDSTORE_PORT: 3060
IDSTORE_ADMIN_USER: cn=IDRWUSER,cn=users,dc=mycompany,dc=com
IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=groups,dc=mycompany,dc=com
IDSTORE_LOGINATTRIBUTE: uid
PASSWORD_EXPIRY_PERIOD: 7300
```

Note: The PASSWORD_EXPIRY_PERIOD is calculated as number of days.

The IDRWUser is the read-write user created for provisioning:

```
IAM_ORACLE_HOME/idmtools/bin/idmConfigTool.sh -upgradeLDAPUsersForSSO
input file=upgradeLDAPUsersForSSO.props log_
file=upgradeLDAPUsersForSSO.out
```

15.4 Adding Privileges to IDStore and Policy Store Entities

Additional privileges must be given to the entities that are created during provisioning for the IDStore and the Policy Store. To add these privileges, following these steps from the IDM domain:

1. Set the environment variables: *MW_HOME*, *JAVA_HOME, IDM_HOME*, and *ORACLE_HOME*. Set *IDM_HOME* to *IDM_ORACLE_HOME*. Set *ORACLE_HOME* to *IAM_ORACLE_HOME*.
2. Create a properties file as follows and replace the values accordingly:

   ```
   IDSTORE_HOST: idstore.mycompany.com
   IDSTORE_PORT: 3060
   IDSTORE_BINDDN: cn=orcladmin
   IDSTORE_USERSEARCHBASE: cn=Users,DC=mycompany,dc=com
   IDSTORE_SEARCHBASE: dc=mycompany,dc=com
   IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
   POLICYSTORE_HOST: policystore.mycompany.com
   POLICYSTORE_PORT:  389
   POLICYSTORE_BINDDN: cn=orcladmin
   POLICYSTORE_CONTAINER: cn=FAPolicies
   POLICYSTORE_READWRITEUSER: cn=PolicyRWUser,cn=Users,dc=us,dc=oracle,dc=com
   OIM_T3_URL : t3://idstore.mycompany.com:14000
   OIM_SYSTEM_ADMIN : xelsysadm
   OVD_HOST: idstore.mycompany.com
   OVD_PORT: 6501
   OVD_BINDDN: cn=orcladmin
   ```

3. Execute the following post-provisioning configuration commands:

   Linux x86-64:

```
idmConfigTool.sh -postProvConfig input_file=idm.props
```

Windows:

```
idmConfigTool.bat -postProvConfig input_file=idm.props
```

15.5 Updating the MDS Schema Database Statistics

After Oracle Fusion Applications is deployed and provisioned, you should ensure optimized query plans for Oracle Metadata Services (MDS) queries are generated so that performance does not decline until the next automatic statistics collection window. For each MDS schema, execute the following statements in SQL*Plus as a privileged database user, for example SYS.

1. Execute the following command to regather the statistics:

```
execute dbms_stats.gather_schema_stats(
ownname =>'schemaOwner',
estimate_percent =>dbms_stats.auto_sample_size,
method_opt =>'for all columns size auto',
cascade => true);
```

> **Note:** Replace *schemaOwner* with the name of the schema, for example FUSION_MDS. Also, place the entire command in a single line at the time of execution.

2. If there is no performance improvement after collecting statistics, then flush the shared pool to clear the execution plan for the database and generate a new query plan, using the following command:

```
alter system flush shared_pool;
alter system flush buffer_cache;
```

> **Note:** Perform this action only when the system is not being actively used as it may affect the performance of production systems.

15.6 Setting Up Notifications

Oracle User Messaging Service is a component of Oracle SOA Suite, which enables you to receive notifications sent from SOA applications.

Applications in the following product families receive approval notifications and complete approvals and rejections of requests through e-mail:

- Oracle Fusion Customer Relationship Management
- Oracle Fusion Financials
- Oracle Fusion Human Capital Management
- Oracle Fusion Supply Chain Management
- Oracle Fusion Procurement
- Oracle Fusion Project Portfolio Management

Note: Before you proceed, ensure that an e-mail server exists. If you intend to use the bulk e-mail feature of Oracle Fusion Customer Relationship Management, you need to set up the e-mail to handle bulk e-mail. To configure an e-mail server, see detailed instructions in the Oracle Fusion Middleware Administrator's and Developer's Guide for Oracle Business Intelligence Publisher.

15.6.1 Configuring E-Mail Notification Using Oracle SOA Suite

You must configure Oracle SOA Suite as follows to enable e-mail notifications:

1. For existing users, associate the users with their e-mail addresses in the domain.
2. For new users, do the following:
    1. Add user profile in the domain.
    2. Create e-mail account in the e-mail server for the added user.
    3. Associate the user profile with the respective e-mail address.
3. Configure e-mail driver properties.

    Note: To enable the workflow participants to receive and forward notifications, configure Oracle User Messaging Service by setting the appropriate driver instances with Oracle Enterprise Manager Fusion Applications Control.

    a. In the navigation pane, expand **farm** - **User Messaging Service** - **usermessagingdriver-email**.

    b. Go to **User Messaging Email Driver** - **Email Driver Properties**. The Email Driver Properties page displays.

    c. In the **Driver-Specific Configuration**, modify the **Outgoing** and **Incoming** properties with the following:

    Modify `OutgoingMailServer`, `OutgoingMailServerPort`, `OutgoingDefaultFromAddr`, `OutgoingUsername`, and `OutgoingPassword`.

    Modify `IncomingMailServer`, `IncomingMailServerPort`, `IncomingMailIDs`, `IncomingUserIDs`, `IncomingUserPasswords`, and `receivefolder`.

    d. Select the **ImapAuthPlainDisable** checkbox.

    e. Click **Apply** to save the changes.

    Note: To configure e-mail driver properties for other **usermessagingdriver-email** services under **farm** - **User Messaging Service**, repeat Steps a to e.

4. Configure notification properties to enable workflow e-mail notifications using Oracle Enterprise Manager Fusion Applications Control:
    a. In the navigation pane, expand **farm** - **SOA**.

    b. Go to **SOA Infrastructure** - **SOA Administration** - **Workflow Notification Properties**. The Workflow Notification Properties page displays.

c. From the **Notification Mode** list, choose **All**.

d. In the **Notification Service** section, specify the notification channel values. These properties are used to notify the users of any changes to the state of a task. Workflow notifications can use three types of addresses:

From Address: For sending notifications.

Actionable Address: For receiving actionable responses. The Actionable Address is the account in which task action-related e-mails are received and processed by human workflow.

Reply To Address: For receiving reply notifications.

e. Click **Apply** to save the changes.

Note: To configure workflow notification properties for other Oracle SOA Suite servers, repeat Steps 3a to 3e.

For more information on user messaging server and configuring human workflow notification properties, refer to section Configuring Oracle User Messaging Service in the Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite.

5. Specify the actionable e-mail account name using Oracle Enterprise Manager Fusion Applications Control:

a. In the navigation pane, expand **farm** - **SOA**.

b. Go to **SOA Infrastructure** - **SOA Administration** - **Workflow Task Service Properties**. The Workflow Task Service Properties page displays.

c. In the **Actionable Email Account** field, specify the incoming actionable e-mail account to use. The default account name is `Default`, which is the account configured in Step 3. If a different account name is specified in the **Actionable Email Account** field, then create and configure that account.

For more information on configuring human workflow notification properties, see the Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite.

Note: Repeat Steps 2 to 4 to configure e-mail notification separately for each product family such as Oracle Fusion CRM, Oracle Fusion HCM, and so on.

---

6. Restart the Oracle WebLogic Server Managed Servers for the domains in the product families:

a. Stop the Managed Servers by using one of the following scripts from the Oracle Fusion Applications Middleware home directory. In these scripts, `managed_server_name` specifies the name of the Managed Server and `admin_url` specifies the listen address and port number of the domain's administration server. The listen address is the host name, IP address, or domain name server (DNS) name. When prompted, enter your user name and password.

Platform	Script

Windows	`FA_MW_HOME\user_projects\domains\domain_name\bin\stopManagedWebLogic.cmd managed_server_name admin_url`
UNIX	`FA_MW_HOME/user_projects/domains/domain_name/bin/stopManagedWebLogic.sh managed_server_name admin_url`

b. Start the Oracle WebLogic Server Managed Servers for the product families using one of the following scripts from the fusionapps Middleware directory. In these scripts, `managed_server_name` specifies the name of the Managed Server and `admin_url` specifies the listen address (host name, IP address, or DNS name) and port number of the domain's administration server. When prompted, enter your user name and password.

Platform	Script
Windows	`FA_MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd managed_server_name admin_url`
UNIX	`FA_MW_HOME/user_projects/domains/domain_name/bin/startManagedWebLogic.sh managed_server_name admin_url`

For more information about performing administrative activities, refer to the *Oracle Fusion Applications Administrator's Guide*.

7. Add the host name and address of the e-mail server to the `/etc/hosts` file on the server hosting the SOA managed servers where the drivers are running.

15.7 What to Do Next

You must review and complete the conditional common post-installation tasks you want to perform before you proceed to the product specific post-installation tasks. Go to Chapter 16 to get started.

16

Completing Conditional Common Post-Installation Tasks

This chapter describes the conditional post-installation tasks you should review and complete as required.

16.1 Introduction to Completing Conditional Common Post-Installation Tasks

After you have successfully completed the mandatory post-installation tasks review and perform the following conditional tasks.

Some components in the Oracle Fusion Applications environment are dependent on one another. Therefore, it is important to start and stop components in the proper order. In the course of normal Information Technology (IT) operations, common operations include shutting down computers and starting them back up. Therefore, it is crucial to start and stop Oracle Fusion Applications in a sequential manner. For more information, see "Starting and Stopping the Entire Oracle Fusion Applications Environment" in *Oracle Fusion Applications Administrator's Guide*.

16.2 Setting Up Global Search

Oracle Fusion Applications Search provides the search framework to manage enterprise-wide searches. Each product family within Oracle Fusion Applications such as Oracle Fusion Customer Relationship Management, Oracle Fusion Human Capital Management, and Oracle Fusion Supply Chain Management has its own set of seeded searchable objects that are packaged into its corresponding search application. For example, the seeded searchable objects for Oracle Fusion Customer Relationship Management such as leads, opportunities, and contacts are packaged in the Oracle Fusion Customer Relationship Management search application. To support the lifecycle management of searchable objects for a particular product family, you must provision your Oracle Fusion Applications environment.

Note: This task is not applicable to Oracle Cloud implementations.

16.2.1 Oracle Fusion Applications Environment

- Provisioning the Oracle Fusion Applications environment is mandatory before you can manage the searchable objects of any product family. See Chapter 13, "Provisioning a New Oracle Fusion Applications Environment".

16.2.2 Oracle Enterprise Crawl and Search Framework

Oracle Fusion Applications Search functionality is fundamentally made possible by the integration of three systems, each playing a role in forming the complete search platform:

- Oracle Fusion Applications Search leverages the Oracle Enterprise Crawl and Search Framework (ECSF) to enable search on transactional business objects. Therefore, validating the environment for Enterprise Crawl and Search Framework involves the recommended checks for establishing Oracle Fusion Applications Search. See Section 16.2.3, "Validating the Oracle Enterprise Crawl and Search Framework Environment".
- Managing search involves making seeded searchable objects available for search, maintaining search categories, and so on.
- To make the Oracle Fusion Applications search components appear on the user interface, you need to enable the relevant profile option.

ECSF is an Oracle Fusion Middleware search framework that enables the exposure of application context information on various business objects to enable full-text transactional search. Benefits of ECSF include:

- Transparent integration of applications with search engines, which minimizes development time and maximizes the user experience with search
- Code reuse, through use of a well designed set of abstract classes, to reduce long design cycles
- Basic platform for developing search, which helps new developers to grasp the conceptual flow of work easily
- Centralized process and control mechanism, which enhances search functionality
- Wide range of optimizations that offer better control to leverage search results

16.2.2.1 Oracle Enterprise Crawl and Search Framework Management Features

ECSF management features include:

- Runtime server, a metadata-driven runtime engine that serves as an integration framework between enterprise data sources and Oracle Secure Enterprise Search (Oracle SES). It enables crawling, indexing, and the security service. It also serves as the semantic engine that provides "smart" search features, such as faceted navigation, actionable results, and related search.
- Oracle Enterprise Manager Fusion Applications Control (Fusion Applications Control), an administration user interface for configuring and administering the ECSF runtime server, managing the searchable object lifecycle, and synchronizing with Oracle SES. Support for a command line administration option is also provided. For more information, see Appendix "ECSF Command Line Administration Utility" in the *Oracle Fusion Applications Developer's Guide*.

16.2.2.2 Key Oracle Enterprise Crawl and Search Framework Features

Key ECSF features that are built on top of Oracle SES and enhance the Oracle Fusion Applications user experience with search include:

- Basic search, which allows query based on keyword and search category
- Advanced search, which allows query based on keyword, search category, and up to 100 attribute filters
- Faceted navigation, which allows the filtering of search results based on attributes of the business objects. Users can navigate a search result set based on a set of predefined facets, or dimensions. This feature returns a list of facets and their associated set of available values with the search result. Users can select a value for each facet, which is then submitted with the search query to narrow down the result set
- Actionable results, which are search results with action links associated with the searchable objects. From the search results users can either go straight to the page displaying the record they selected, or they can invoke a specific task on a search result
- Saved searches, which allows saved search criteria for later use. Users can create new saved search entries, edit and delete existing saved search entries, and retrieve user-specified or public saved search entries
- File attachments, which allow the crawling of attachments that are associated with Oracle Fusion Applications transactional objects or records

- Crawling Oracle WebCenter Portal tags, which supports crawling searchable objects that contain Oracle WebCenter Portal tags
- Crawling tree structures, which supports search functionality on source systems containing data that is organized in a tree structure (for example, Oracle Business Intelligence Catalog)
- Search support for external data sources, which allows querying against search groups that contain external data sources, which are non-ECSF related data sources, such as wiki pages and blogs, that are directly crawled by Oracle SES

16.2.3 Validating the Oracle Enterprise Crawl and Search Framework Environment

Before you begin to manage search with ECSF, make sure that the environment is set up properly for using ECSF.

To validate the ECSF setup, follow the procedures in the following sections.

Task 1 Make Sure That Oracle Fusion Applications Includes Search Functionality

Oracle Fusion Applications Search should be embedded within Oracle Fusion Applications, but it must be enabled in the user interface by setting the profile option `FUSION_APPS_SEARCH_ENABLED` to `Y`.

To make sure that Oracle Fusion Applications includes search functionality:

1. Log in to Oracle Fusion Applications. If you cannot log in to Oracle Fusion Applications, contact your installation team.
2. Verify that the **Enterprise Search** box is available at the top of every Oracle Fusion Applications page.
3. View the **Search Categories** dropdown list. There should be no search categories listed.
4. Log out.

Task 2 Make Sure That Oracle SES Is Installed and Configured Properly

Oracle SES provides the fundamental search capability that includes crawling, indexing, and querying. For more information about Oracle SES, see *Oracle Secure Enterprise Search Administrator's Guide*.

To make sure that Oracle SES is installed and configured properly:

1. Check the administration endpoint by logging in to the Oracle SES Administration GUI with the administration username and password at the following URL.

   `http: host_name:7777/search/admin/index.jsp`

   The default port number is 7777. Make sure that you use the correct port number for your installation. If you cannot access the Oracle SES search engine, contact your installation team.
2. Make sure that the Oracle SES identity plug-in has been registered.
3. Make sure that the federated trusted entities are created. Depending on what product families are installed, you should see one to three proxy users listed. The valid values are:
   - `FUSION_APPS_CRM_ECSF_SEARCH_APPID`
   - `FUSION_APPS_FSCM_ECSF_SEARCH_APPID`

- FUSION_APPS_HCM_ECSF_SEARCH_APPID

Task 3 Make Sure That Fusion Applications Control Is Available

Fusion Applications Control must be available for configuring and administering the ECSF runtime server, managing the searchable object lifecycle, and synchronizing with Oracle SES.

To make sure that Fusion Applications Control is available:

1. Log in to Oracle Enterprise Manager.
2. From the navigation pane, expand the farm and then the **Enterprise Crawl and Search Framework** folder.
3. Select the application engine instance that contains the searchable objects you want to manage to open the Enterprise Crawl and Search Framework Configuration Settings page.

   The search engine types (Oracle SES) should be listed.
4. Click the Oracle SES search engine type name link in the Search Engine Types table to open the Search Engine Instance administration page, and validate the Oracle SES search engine instance parameters.
5. From the table of search engine instances, select a search engine instance record, and then select the **Searchable Objects** tab to view the table of searchable objects, and validate the list of searchable objects for the application. For a list of seeded searchable objects.
6. Select the **Search Categories** tab to view the table of search categories, and validate the list of search categories and objects associated with the search categories for the application. For a list of seeded search categories.
7. From the navigation pane, re-select the application to open the Enterprise Crawl and Search Framework Configuration Settings page, then click the **Search Application Service Component** link to open the Search Application Service Component administration page, and validate that the search applications for the product families are installed.

Task 4 Provide Access to ECSF Pages in Fusion Applications Control

To access the ECSF pages in Fusion Applications Control, users must have Operator privileges in Oracle WebLogic Server. You must add the users to the Operator group and above on Oracle WebLogic Server.

Task 5 Validate the Application Identities

Oracle Fusion Applications include seven search-related application identities that are seeded and are stored in the identity store:

- FUSION_APPS_CRM_SES_CRAWL_APPID
- FUSION_APPS_CRM_ECSF_SEARCH_APPID
- FUSION_APPS_FSCM_SES_CRAWL_APPID
- FUSION_APPS_FSCM_ECSF_SEARCH_APPID
- FUSION_APPS_HCM_SES_CRAWL_APPID
- FUSION_APPS_HCM_ECSF_SEARCH_APPID
- FUSION_APPS_ECSF_SES_ADMIN_APPID

ECSF is powered by Oracle SES. To integrate with Oracle SES, several integration identities known as application identities are used. For each Oracle Fusion Applications application, there are a pair of application identities, for example, FUSION_APPS_HCM_SES_CRAWL_APPID and FUSION_APPS_HCM_ECSF_SEARCH_APPID. The CRAWL application identities are used by Oracle SES to interact with ECSF for crawling and security requests, while the SEARCH application identities are used by Oracle SES to query Oracle SES as proxy users.

FUSION_APPS_ECSF_SES_ADMIN_APPID is the application identity used by ECSF to integrate with Oracle SES for administration tasks, such as deployment, scheduling, and so on.

Application identities are provisioned as users in the Oracle Fusion Applications identity store. They often have high level privileges, and their credentials are generated and stored in the credential store. These users are used mainly for machine to machine (application to application) integration.

The Lightweight Directory Access Protocol (LDAP) credential store stores the passwords for the identities that Oracle Fusion Applications and ECSF uses to retrieve passwords for Oracle SES integration.

View the LDAP credential store to make sure the application identities exist.

16.2.4 Configuring Help Search: Highlights

You can include Help in the list of search categories for the search in the global area of Oracle Fusion Applications. This search is of type Oracle Fusion Applications Search, and administering this search involves tasks in Oracle Enterprise Crawl and Search Framework.

Note: This task is not applicable to Oracle Cloud implementations.

The search in Oracle Fusion Applications Help and the navigators, for example Search by Business Process, are based on other search functionality and do not require configuration.

Oracle Enterprise Crawl and Search Framework administration is described fully in the Oracle Fusion Applications Administrator's Guide. As you read content from that guide, keep in mind that Oracle Fusion Applications Search is not used only for Oracle Fusion Applications Help; therefore, the content is not specific to help.

16.2.5 Searchable Objects

- Deploy and activate the TopicSearchPVO searchable object, associate it with the Help category and deploy the category, and deploy and start index schedules. Each crawl picks up customizations and patches for help, so the frequency depends on how often you add, manage, or patch help.
- Do not modify the TopicSearchPVO searchable object itself.*See:* Modifying the Display Name of Deployed Searchable Objects.

16.2.6 Configuring External Search Categories for Oracle Business Intelligence and Oracle WebCenter Portal: Procedures

To perform global search within Oracle Business Intelligence and Oracle WebCenter Portal, you must create the appropriate external search categories in Oracle Fusion Applications. For general instructions on making external search categories available

for search, see the *Oracle Fusion Applications Administrator's Guide*.

However, before you proceed with the configuration of external search categories for Oracle Business Intelligence and Oracle WebCenter Portal, you must manually create the Business Intelligence data source. Refer to the section "Configuring for Full-Text Catalog Search" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

You can perform the search-related configuration tasks using Oracle Enterprise Crawl and Search Framework. To configure external search categories for Oracle Business Intelligence and Oracle WebCenter Portal, follow these instructions.

1. Log in to Oracle Enterprise Manager Fusion Applications Control.
2. From the navigation pane, open **Farm - Enterprise Crawl and Search Framework** folder.
3. Select the application engine instance SES 11.2.1. It contains the searchable objects that you want to manage to open the Enterprise Crawl and Search Framework Configuration Settings page.
4. From the Search Engine Types table, click Oracle Fusion Application Search engine SES 11.2.1 to open the Search Engine Instance administration page.
5. On the External Search Categories tab, click **Import**.
6. In the Available Categories column, select the checkbox of the external search categories you want to import, and click **Move** to shuttle your selection to the Selected Categories column.
   - To import Oracle Business Intelligence, select bi_search
   - To import Oracle WebCenter Portal, select Collaboration
7. Click **OK** to import the selected external search categories.
8. Associate the Application ID with the imported external categories:
   - To associate with Oracle Business Intelligence, in the Application ID column corresponding to the external search category you imported (bi_search), enter BI.
   - To associate with Oracle WebCenter Portal, in the Application ID column corresponding to the external search category you imported (Collaboration), enter WC.
9. Click **Save External Search Category** to save the selected record.
10. Associate the Application ID with the Search Service component:
    1. From the navigation pane on the left side, select **Enterprise Crawl and Search Framework** folder. The Enterprise Crawl and Search Framework Settings page appears.
    2. From the context menu of **Enterprise Crawl and Search Framework**, select **Home**.
    3. Select the first active service component and note down the search engine instance that is associated with the active service component.
    4. In the `ECSF_QUERY_SERVICE_APP_IDS` field, enter the Application ID in comma separated string format:
    - To configure external search category for Business Intelligence, enter BI.
    - To configure external search category for Oracle WebCenter Portal, enter WC

11. Save the changes.
12. Restart the Search application from the WebLogic Server Console.

16.2.7 Making a Search Application Highly Available

Each installation of Oracle Fusion Applications can provision one or more offerings such as Oracle Fusion Customer Relationship Management (Oracle Fusion CRM), Oracle Fusion Human Capital Management (Oracle Fusion HCM), and so on. Each offering has its own search application such as CRM Search Application, HCM Search Application and so on. However, the application architecture restricts running only one search application at a time and only that search application is registered as the identity plug-in end point of Oracle Secure Enterprise Search (Oracle SES). The identity plug-in end point of Oracle SES is a critical part of Oracle Fusion Search and is used in authenticating all users using the search functionality. Therefore, to mitigate the risk of any down time, it is necessary to identify and make the registered search application highly available by adding more managed WebLogic servers to the cluster.

Depending on the provisioned offerings, the actual search application registered as the identity plug-in endpoint varies. The following instructions help you identify the search application and add more managed WebLogic servers to the existing cluster.

1. Log in to the Oracle SES Administration page.
2. On the Global Settings tab, click **Identity Management Setup**. Review the protocol identified by the HTTP end point for authentication and the current search application indicated by one of the following values for User ID:
   - User ID = `FUSION_APPS_CRM_ECSF_SEARCH_APPID`: indicates CRM Search Application is used
   - User ID = `FUSION_APPS_FSCM_ECSF_SEARCH_APPID`: indicates FSCM Search Application is used
   - User ID = `FUSION_APPS_HCM_ECSF_SEARCH_APPID`: indicates HCM Search Application is used
3. Identify the search application and add more managed servers to the cluster. For detailed instructions, see the Oracle Fusion Applications High Availability Guide.

16.3 Setting Up Privacy Statement

You can enable the Privacy Statement link under the Help menu and configure it to link to a customer-defined page. By default, the link is disabled.

16.4 Configuring Oracle User Productivity Kit In-Application Support

This section describes the procedures for setting up the Oracle User Productivity Kit In-Application Support.

Users may need to access and take advantage of the Oracle User Productivity Kit (UPK) content while working with Oracle Fusion Applications. To make the Oracle UPK content available for users, you need to enable and configure the UPK link under the Help menu of Oracle Fusion Applications, using the Oracle UPK In-Application Support functionality.

To perform this task, you must have the role of a System Administrator and have relevant privileges on the environment where you want to enable and configure the UPK link.

Configuring the Oracle UPK In-Application Support involves the following activities:

1. Registering Oracle UPK as an Enterprise Application.
2. Deploying the Oracle UPK package on a HTTP server.

16.4.1 Registering Oracle UPK as an Enterprise Application

Your system administrator must have security access to use Oracle Fusion Functional Setup Manager to complete the steps that follow.

To complete the configuration:

1. From the Oracle Fusion Applications home page, navigate to Navigator -> Tools -> Setup and Maintenance to access the Setup and Maintenance work area.
2. In the Tasks list, select Topology Registration -> Register Enterprise Applications to access the Register Enterprise Applications work area.
3. In the Register Enterprise Applications work area, do one of the following:
   - To modify an existing configuration, click the **Name** link of the registered application.

     For example: Oracle User Productivity Kit
   - If this is a new configuration, click **Add (+)** to register Oracle UPK as a new application in Oracle Fusion Applications.
4. In the Add Enterprise Application work area, in the Basic Information section, do the following:
   1. In the Enterprise Environment drop-down list, select your environment.

      For example: Oracle
   2. In the Enterprise Application drop-down list, select your enterprise application.

      For example: Oracle User Productivity Kit
   3. In the Name field, enter the name of the enterprise application that you are registering.

      For example: Oracle User Productivity Kit
5. In the Server Details section, do the following:
   1. In the Server Protocol drop-down list, select the appropriate protocol for the server that you plan to use to launch UPK content.

      The UPK Player supports both HTTP and HTTPS.
   2. In the External Server Host field, enter the full DNS name of the server host.

      For example: content.mycompany.com
   3. In the External Server Port field, enter the appropriate port for either HTTP or HTTPS. It could be either the default value 80/443 or customer configured port location.

      Note: The Context Root name is the name of the virtual directory used in the URL that launches your UPK content.

      ---
   4. Click **Save and Close** when you are done.

6. Click **Regenerate Domain Connections**.
7. Log out of Oracle Fusion Applications and log in again.
8. Click the Help menu on the Oracle Fusion Applications Home page to verify if the Oracle User Productivity Kit is now available as a menu item.

16.4.2 Deploying the Oracle UPK Player Package

Deploy your Oracle UPK Player Package to any server that uses the HTTP or HTTPS protocols.

The content root directory must be configured to the location of your Oracle UPK Player on the web server.

For example: `http(s)://<server>:<port>/<directory>`

Test access to the content.

If the Oracle UPK Player launches with all topics, you are ready to configure Oracle Fusion Applications for In-Application Support.

16.5 Reviewing and Configuring Diagnostic Logging Settings and Diagnostic Testing Features

The infrastructure for health checking and troubleshooting Oracle Fusion Applications is provided along with provisioning. However, before beginning any production activity on Oracle Fusion Applications, perform the following configuration tasks.

Note: This task is not applicable to Oracle Cloud implementations.

16.5.1 Configuring Settings for Log Files During Normal Operation

Although critical business logic sections of Oracle Fusion Applications may write more information to log files than less critical areas of the application code, the amount of information that Oracle Fusion Applications log depends primarily on how the environment is configured. Oracle supplies default values for log settings, but you can specify different setting values if you want to adjust the amount of information to be logged. Most Oracle Fusion Applications components use a standard set of log configuration settings.

In busy computing environments, the amount of disk space used by log files can become a concern. Large log files can also affect system performance. Oracle Fusion applications that are written in PL/SQL address this concern using automatic log file rotation.

16.5.1.1 Managing Rotating Log File Space Usage for PL/SQL Applications

For Oracle Fusion Applications modules that are implemented using PL/SQL, when a `diagnostic.log` file reaches a specific size, the `diagnostic.log` file is automatically renamed, and a new `diagnostic.log` file is created. If the `AFLOG_PLSQL_FILENAME` profile option is set so that the logging framework uses a log file name other than `diagnostic.log`, then the file name that the profile option specifies is used, instead of `diagnostic.log`.

Use the following profile options settings to specify the maximum log file size:

- AFLOG_MAX_FILE_SIZE: This setting specifies the size in megabytes beyond which a PL/SQL log file name is automatically renamed and a new log file is started. The default value is 10 megabytes.

  Note: If the AFLOG_BUFFER_MODE profile option is set to a value larger than 0, enabling asynchronous buffering of PL/SQL log entries, then the actual maximum size of any single PL/SQL log file is the value of AFLOG_MAX_FILE_SIZE plus the number of megabytes that are flushed from the buffer. This value is approximate, because the amount of information that can accumulate in the buffer is set using the AFLOG_BUFFER_SIZE setting, which specifies a specific number of log records, rather than a specific number of megabytes.

- AFLOG_NUMBER_OF_LOG_FILES: This setting specifies the maximum number of PL/SQL log files the system keeps at any one time. The default value is 10 files.

PL/SQL log rotation is currently done only on the basis of file size, not on the basis of the passage of a specified amount of time.

When a PL/SQL log file is renamed, the new name depends on whether the AFLOG_PLSQL_FILENAME profile option is set:

- If the profile option is set, then the new log file name is of the format *AFLOG_PLSQL_FILENAME_value-n*.log, where *n* is a positive integer.
- If the profile option is not set, then the new log file name is of the format diagnostic-*n*.log, where *n* is a positive integer.

The value of *n* depends on the names of the log files that are already present in the directory. If the directory contains no previously renamed log files, then the first renamed log file is called diagnostic-1.log or *AFLOG_PLSQL_FILENAME_value-1*.log. If other log files exist, then *n* is set to the next higher integer after the highest integer that is already in use. For example, if the directory contains diagnostic-1.log through diagnostic-8.log at the time when the diagnostic.log file surpasses the size limit set in the AFLOG_MAX_FILE_SIZE profile option, then the diagnostic.log file is renamed to diagnostic-9.log.

When the number of log files reaches the value specified using the AFLOG_NUMBER_OF_LOG_FILES profile option, then older log files are deleted automatically, to prevent the disk space usage of the log file directory from getting too large.

Over time, the value of *n* in diagnostic-*n*.log or *AFLOG_PLSQL_FILENAME_value-n*.log can become large enough to cause usability challenges or exceed the number of characters that the operating system allows in a file name. If you want to have the value of *n* start over at 1, you can move all existing log files except the currently active diagnostic.log file or *AFLOG_PLSQL_FILENAME_value*.log file into another directory. When the active file surpasses the size limit and the log rotation code finds no previously renamed log files in the directory, the active file is renamed using a value of 1 for *n*.

Note: If your Oracle Fusion Applications environment includes multiple database nodes such as Oracle Real Application Clusters (RAC), then each database node corresponds to a server instance that has its own location for log files.

If an incident is created, then the server instance that creates the incident handles all subsequent jobs related to that incident. Identifiers for incidents are unique within a specific instance, but not across instances. For more information about working with incidents, see the "Troubleshooting Oracle Fusion Applications Using Incidents, Logs, QuickTrace, and Diagnostic Tests" chapter in the *Oracle Fusion Applications Administrator's Troubleshooting Guide*.

16.5.1.2 Managing Log File Space Usage for C Applications

Oracle Fusion Applications modules that are implemented in C currently produce log files that continually increase in size.

To manage log file space usage for log files created by Oracle Fusion Applications modules that are written in C:

1. Navigate to the directory that contains the log files:
   - If the `AFLOG_FILENAME` profile option is set, then navigate to the location designated by the profile option value.
   - If the `AFLOG_FILENAME` profile option is not set, then navigate to the location set by Oracle Enterprise Scheduler Service.

     You can use Fusion Applications Control to determine the location of Oracle Enterprise Scheduler log files, as follows:

     a. In the navigation pane, expand the farm part of the navigational tree, then expand **Scheduling Services**, and then select an Oracle Enterprise Scheduler server as your target.

     b. In the context pane, from the **Scheduling Service** dropdown menu, choose **Logs** > **View Log Messages.**

     c. Click **Target Log Files** to view a list of log files associated with the selected server.

        For example, a typical path and file name might be the following, where *`APPLICATIONS_CONFIG/domain/<domain_name>`* is the domain home directory, *`SERVER_HOME`* is the server home directory, and *`serverName`* is the name of the Oracle Enterprise Scheduler server:

        `APPLICATIONS_CONFIG/domain/<domain_name>``/servers/`*`SERVER_HOME`*`/logs/`*`serverName`*`-diagnostic.log`

2. Rename the log file that is currently in use.

   For example, if the current log file is called `Cdiagnostic.log`, you might rename it to `Cdiagnostic_`*`MMDDYYYY`*`.log`, where *`MMDDYYYY`* is the current date.

3. Delete any previously renamed log files that you no longer need.

16.5.2 Understanding Oracle Fusion Applications Diagnostic Tests and the Diagnostic Framework

Diagnostic tests are executables that are designed to exercise particular aspects of Oracle Fusion applications, to determine whether they are operating correctly and to help identify and resolve any problems. The Oracle Fusion Applications Diagnostic Testing Framework (Diagnostic Testing Framework) lets you execute diagnostic tests and collects the results into detailed diagnostic reports. Oracle provides diagnostics tests that are installed along with Oracle Fusion Applications releases and patches.

You can use diagnostic tests along with information from log files and the collections of error condition information that are called incidents.

16.5.2.1 Relationships Between Diagnostic Tests, Incidents, and Log Messages

Oracle developers create diagnostic tests that you can use to help diagnose and resolve Oracle Fusion application problems.

Oracle developers use mechanisms such as application programming interface (API) calls in Oracle Fusion Applications code to record application operations in log files and to provide error messages as appropriate. A diagnostic test may or may not be associated with a particular error message.

If an Oracle Fusion application handles a particular error in a way that triggers the creation of an incident, then any diagnostic tests that are associated with the error message for the incident run automatically. Oracle developers accomplish this by setting the value of each diagnostic test's `APPS_MSG_ID` tag to match the identifier of any error message that should trigger the automatic execution of that test. There is no configuration setting for disabling this automatic execution of diagnostic tests.

The results of any automatically run diagnostic test are automatically associated with the related incident, and the identity of the user who received the error message is recorded.

For more information about using diagnostic tests and log files to help diagnose a problem, see the "Troubleshooting Oracle Fusion Applications Using Incidents, Logs, QuickTrace, and Diagnostic Tests" chapter in the *Oracle Fusion Applications Administrator's Troubleshooting Guide*.

It is important to be familiar with the following additional concept that **Seed data** is information that Oracle provides to you in the form of database records. Diagnostic tests are included in seed data.

16.5.2.2 Standard Diagnostic Testing Administration Tasks and Tools

Under normal circumstances, the following administrative tasks are associated with Oracle Fusion Applications diagnostic tests:

- Configuring security to provide appropriate access to diagnostic tests. You can assign job roles to particular users to grant those users the ability to perform various diagnostic operations.

> **Note:** In the current release, a job role for diagnostic operations grants the user the ability to perform the specified operations for all diagnostic tests that are provided with Oracle Fusion Applications. When choosing whether to grant a diagnostic job role to specific users, be aware that some diagnostic tests may include sensitive information in their results.

- Running diagnostic tests. You can use diagnostic tests for the following purposes:
  - Routinely checking the health of your Oracle Fusion applications
  - Troubleshooting a problem with an Oracle Fusion application
  - Collecting detailed data that may help Oracle Support to resolve a problem for you

Some diagnostic tests require a specific Oracle Fusion application to be running while the test is performed—these diagnostic tests are called **internal** diagnostic tests. Other diagnostic tests can perform their functions even if the Oracle Fusion application to be tested is not running—these tests are called **external** diagnostic tests.

The distinction between internal and external tests is important because it affects both when you can run the tests and which interfaces you can use to run the tests. The Diagnostic Testing Framework provides two interfaces:

- The Oracle Fusion Applications Diagnostic Dashboard application (Diagnostic Dashboard) provides a graphical user interface that lets you perform the following tasks:
  - Execute and monitor both internal and external diagnostic tests for Oracle Fusion applications
  - Purge diagnostic test results
  - Register any special-purpose diagnostic tests that Oracle Support may provide to you
- The `diagctl` command-line interface lets you perform the following tasks:
  - Execute external diagnostic tests (tests that do not require a specific Oracle Fusion application to be running)

    Note: Technical constraints prevent the `diagctl` command-line interface from returning useful results for internal diagnostic tests (tests that require a specific Oracle Fusion application to be running when the test is performed). You must use Diagnostic Dashboard to run any internal diagnostic tests.

    You must also use Diagnostic Dashboard to determine whether a particular test is an internal or an external test.

  - View diagnostic test results
  - Register any special-purpose diagnostic tests that Oracle Support may provide to you

16.5.3 Configuring the Diagnostic Testing Framework for Normal Operation

You can use diagnostic tests to check normal system health and to troubleshoot system problems. You can configure your Oracle Fusion Applications environment to run all Oracle Fusion Applications diagnostic tests using the Diagnostic Dashboard application, and to run external diagnostic tests using the `diagctl` command-line interface.

Note: Technical constraints prevent the `diagctl` command-line interface from returning useful results for internal diagnostic tests (tests that require a specific Oracle Fusion application to be running when the test is performed). You must use Diagnostic Dashboard to run any internal diagnostic tests.

You must also use Diagnostic Dashboard to determine whether a particular test is an internal or an external test.

Both the Diagnostic Dashboard application and the `diagctl` command-line interface are automatically installed as part of the Oracle Fusion Applications installation. However, you must assign appropriate job roles to specific users to give them the ability to display and perform operations using the Diagnostic Dashboard application. Access to the `diagctl` command-line interface is controlled at the level of the server operating system.

For proper operation of the `diagctl` command-line interface, you must also set certain environment variables.

To help you locate diagnostic tests for specific purposes, the diagnostic tests that you receive with Oracle Fusion applications are all assigned to predefined categories.

Note: You cannot change the tag name and tag value assignments that Oracle uses to categorize diagnostic tests, and you cannot remove those tag names or tag values from the database. The following related links in the Task pane of the Diagnostic Dashboard application are intended for use by Oracle personnel only:

- Add New Tag
- Add New Tag Value
- Assign Tags to Tests
- Unassign Tags from Tests
- Remove Tag
- Remove Tag Value

Caution: Do not attempt to modify the diagnostic test seed data provided to you by Oracle. Unauthorized modification of this seed data may prevent diagnostic tests from functioning correctly, lengthening the amount of time required to resolve both current and future problems.

16.5.3.1 Controlling Access to Diagnostic Testing Functionality

Access to diagnostic testing functionality is controlled separately for Diagnostic Dashboard and the `diagctl` command-line interface.

For the `diagctl` command-line interface, access is controlled at the level of the server operating system. If a user can log in to the server where `diagctl` is stored, and if that user has operating system permissions to read and execute `diagctl`, then that user can use `diagctl` to perform all diagnostic operations that the command-line interface supports.

For Diagnostic Dashboard, you can use Oracle Identity Manager to assign specific users to any of the four preconfigured job roles that grant users access to Diagnostic Dashboard. Each of these four job roles provides access to a different amount of the functionality of the dashboard.

> **Note:** Oracle Fusion applications display the **Troubleshooting > Run Diagnostic Tests** command in the **Help** menu only for users who are associated with the preconfigured job roles that grant access to Diagnostic Dashboard operations.

- The `Diagnostic Viewer` job role can view and analyze diagnostic test results for Oracle Fusion applications.
- The `Diagnostic Regular User` job role can execute diagnostic test runs and view diagnostic test results for Oracle Fusion applications, and cancel diagnostic test runs that were started by the current user.
- The `Diagnostic Advanced User` job role can schedule and execute diagnostic test runs, view diagnostic test results, attach test results to application incidents for Oracle Fusion applications, and cancel diagnostic test runs that were started by the current user. In general, this job role is recommended for running Oracle Fusion Applications diagnostic tests, because its added capabilities allow users to work with administrators more flexibly during troubleshooting.
- The `Diagnostic Administrator` job role can use all of the diagnostic testing functionality provided for Oracle Fusion applications, including purging test results from the database and canceling test runs started by other users.

> **Note:** In the current release, any job role for diagnostic operations grants the user the ability to perform the role's specified operations for all diagnostic tests that are provided with Oracle Fusion applications. When choosing whether to grant any diagnostic job role to specific users, be aware that some diagnostic tests may include sensitive information in their results.

To grant specific users permission to use Diagnostic Dashboard:

1. Decide which users need the capabilities of each of the four preconfigured job roles for diagnostic operations.
2. Use Oracle Identity Manager to assign the appropriate job role to each user.

16.5.3.2 Navigating to the Diagnostic Dashboard Application

The Diagnostic Dashboard application for Oracle Fusion Applications provides a graphical user interface that lets you execute and monitor diagnostic tests, display and purge test results, and register any special-purpose diagnostic tests that Oracle Support may provide to you. Each product family within Oracle Fusion Applications has its own instance of Diagnostic Dashboard. Provided that you are assigned to an appropriate job role, you can navigate to Diagnostic Dashboard from any Oracle Fusion application or from Oracle Enterprise Manager Cloud Control (Cloud Control).

16.5.3.2.1 Navigating to the Diagnostic Dashboard Application from an Oracle Fusion Application If you want to use Diagnostic Dashboard to execute or monitor diagnostic tests or display or purge test results while you are using an Oracle Fusion application, you can navigate to Diagnostic Dashboard directly from the application.

To display the Diagnostic Dashboard application from an Oracle Fusion application:

1. Log in to the relevant Oracle Fusion application as a user who has access to the specific Diagnostic Dashboard operations that you need.
2. From the **Help** menu in the application, choose **Troubleshooting > Run Diagnostic Tests** to display Diagnostic Dashboard.

> **Note:** Oracle Fusion applications display the **Troubleshooting > Run Diagnostic Tests** command in the **Help** menu only for users who are assigned to the preconfigured jobs roles that grant access to Diagnostic Dashboard operations.

16.5.3.2.2 Navigating to the Diagnostic Dashboard Application from Cloud Control If you want to use the Diagnostic Dashboard application to execute or monitor diagnostic tests or display or purge test results while you are using Cloud Control, such as while you are using Support Workbench to gather additional information about an existing incident, you can navigate to Diagnostic Dashboard directly from Cloud Control.

To display to Diagnostic Dashboard from Cloud Control:

1. In Oracle Enterprise Manager, select the product family or cluster application for which you want to run diagnostic tests or view diagnostic test results.
2. From the dynamic dropdown menu, choose **Diagnostics > Fusion Applications Diagnostic Dashboard**.

   A login screen for Diagnostic Dashboard appears in a new window.
3. Log in using an account for the Oracle Fusion Applications product family that you intend to test.

   The account that you use must also be assigned to a job role that provides access to Diagnostic Dashboard.

16.5.3.2.3 Configuring Required Variables for the diagctl Command Line Interface To operate properly, the `diagctl` command-line interface requires you to set certain environment variables.

> **Note:** You must set the required environment variables for each session that plans to use the `diagctl` command-line interface. For your convenience, you may want to add the commands that define these variables to the `.profile` or `.bashrc` files of all users who will run `diagctl`.

To set environment variables for a user of the `diagctl` command-line interface:

1. Log in to the operating system of the Administration Server of the Common domain.
2. Use a command such as the following to set the `DIAGJPSCONFIGFILE` environment variable to the location of the `jps-config-jse.xml` file, making these substitutions:

Replace *APPLICATIONS_CONFIG* with the location of the top-level directory of Oracle Fusion Applications configuration files.

Replace *primordial_host_name* with the host name of the Administration Server of the Common domain).

```
UNIX: export DIAGJPSCONFIGFILE=APPLICATIONS_CONFIG/domains/
primordial_host_name/CommonDomain/config/fmwconfig/jps-config-jse.xml

Windows: set DIAGJPSCONFIGFILE=APPLICATIONS_CONFIG\domains\
primordial_host_name\CommonDomain\config\fmwconfig\jps-config-jse.xml
```

Note: Command syntax for UNIX environments may vary depending on which shell you are using. Whenever you define an environment variable, use the command syntax for your chosen shell.

3. Use a command such as the following to set the JAVA_HOME environment variable to the location of the directory that contains Java files, where *APPLICATIONS_BASE* is the top-level directory for the Oracle Fusion Applications binaries.

```
UNIX: export JAVA_HOME=APPLICATIONS_BASE/fusionapps/jdk6

Windows: set JAVA_HOME=APPLICATIONS_BASE\fusionapps\jdk6
```

4. Use a command such as the following to set the MW_HOME environment variable to the location of the directory that contains Oracle Fusion Middleware files.

```
UNIX: export MW_HOME=APPLICATIONS_BASE/fusionapps

Windows: set MW_HOME=APPLICATIONS_BASE/fusionapps
```

After you complete this step, you can use the diagctl command-line interface to run diagnostic tests.

16.5.4 Health Checking and Diagnostic Tasks

Only after ensuring the completeness of the following configuration, you can perform health checking and troubleshooting for Oracle Fusion applications using log files, incidents, diagnostic tests and so on. Refer to the *Oracle Fusion Applications Administrator's Guide*.

16.5.5 Configuration Tasks

The configuration tasks are described in the *Oracle Fusion Applications Administrator's Guide* unless otherwise specified.

- Enable viewing of logs generated by C and PL/SQL. For more information, see Configuring Access to Logs for Fusion Applications Control
- Configure log file rotation. For more information, see Managing Log File Size and Disk Space Usage
- Review default logging profile options and adjust values for your specific requirements. For more information, see Using Profile Options to Configure Standard Log Settings
- Review and adjust your QuickTrace settings. For more information, see Default System Settings for Incident Creation and QuickTrace

- Configure user access to diagnostic testing functionality. For more information, see Controlling Access to Diagnostic Testing Functionality
- Configure a job role for future user access to troubleshooting options. For more information, see Assisting Users in Gathering Data Using Troubleshooting Options
- To benefit from the health checking, patching recommendations, and configuration services offered by My Oracle Support, install and configure Oracle Configuration Manager. For more information, see Install Configuration Manager on My Oracle Support.
- To use the latest troubleshooting features, including a purpose built Oracle Fusion Applications module, provided by Remote Diagnostic Agent (RDA), install and configure RDA. For more information, see RDA Documentation on My Oracle Support.

16.6 Implementing Compliance Rules

Oracle has established an array of configuration details that optimize the performance and handling of Oracle Fusion Applications, and now delivers seeded compliance rules with Cloud Control 12c. "Compliance" means having a system adhere to, or comply with, such performance standards. This section explains how compliance Rules are defined, and how they are organized (into Standards and Frameworks). It explains how to associate the Standards to your Oracle Fusion Applications instance, how to create, edit, or delete configurations if desired, and how subsequently to monitor and respond to the results in Cloud Control.

16.6.1 Understanding Rules, Standards, and Frameworks

Compliance is implemented as a hierarchy, wherein configuration details -- such as cache sizes, connection time-outs, and more-- are codified into individual Rules. The Rules are collected into logical groups called Standards, which are further organized into a Framework.

Out of the box, you can associate the predefined compliance Standards to your own installation. Each of these components-- Rules, Standards, and Frameworks-- can also be created, edited, or deleted by a Oracle Fusion Applications administrator who has the appropriate privileges. You can freely mix-and-match custom Rules or Standards with predefined ones.

16.6.1.1 What are Real-Time Monitoring Facets?

It is also possible to create "real-time monitoring facets" if you want to create security warnings associated with particular files on your system. Facets, which can be associated with multiple Rules, define particular entities that should be monitored on an ongoing basis. Only critical files should be chosen, to avoid excess CPU load and data generation.

16.6.2 Prerequisites and Related Documentation

It is necessary to have the Oracle Fusion Applications plug-in for Oracle Enterprise Manager Cloud Control 12c, version 12.1.0.5 or above, installed and configured.

There are two additional guides that contain how-to steps on using the Compliance interface. This guide gives specific cross-references to them when needed. These guides are:

- Part VIII of the *Oracle Enterprise Lifecycle Management Guide*

- All of the *Oracle® Enterprise Manager Cloud Control Oracle Database Compliance Standards*

16.6.3 Implementing Compliance

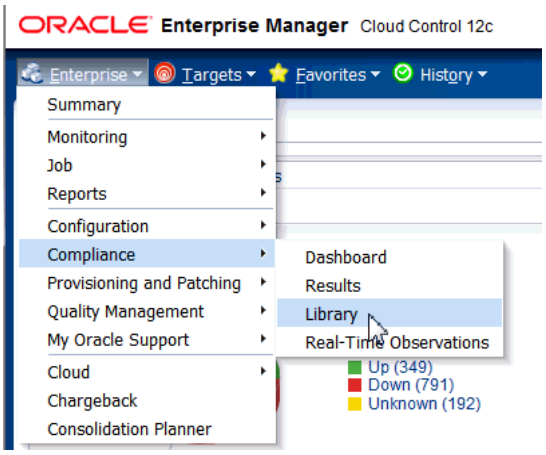
This section explains how to access and implement the Compliance components for Oracle Fusion Applications.

16.6.3.1 Understanding the Rules, Standards, and Framework in the Compliance Library

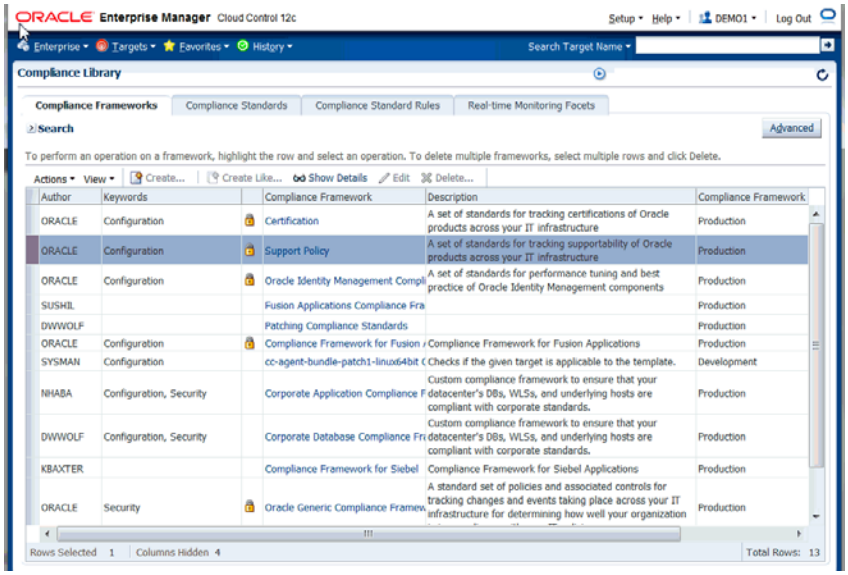
The Compliance components are created, edited, and stored in the Compliance Library.

16.6.3.1.1 Accessing the Compliance Library

1. Log in to the Cloud Control Console.
2. Select **Enterprise** and **Compliance** and **Library**.



The Compliance Library homepage is displayed.



3. Select the relevant tab for the Compliance component you want to use.

16.6.3.1.2 Viewing the System Defined Rules for Oracle Fusion Applications To find the Rules delivered for Oracle Fusion Applications:

1. Access the Compliance Library.
2. Select the **Compliance Standard Rules** tab.
3. Set the **System-Defined** dropdown to **YES**.
4. Expand the **Search** item at the top left of the page, and select **Applicable To: Fusion Instance** in the Search drop-down.

   The defined Rules for Oracle Fusion Applications are listed in the table.
5. To adjust the columns that you see, click **View**, and **Columns**. You can select/deselect items to include in the overview. Note: selecting **Manage Columns** has the same effect.
6. Follow the same steps to search for the Oracle Fusion Applications-specific Standards or Frameworks.

The 42 defined Rules are organized in four separate Standards. This section describes the primary details of the Rules delivered in:

- Table 16–1, " Java Platform Security Compliance Standard"
- Table 16–2, " Oracle HTTP Server Configuration Standard"
- Table 16–3, " WebLogic Server Configuration Standard"
- Table 16–4, " Java Virtual Machine Configuration Standard"
- Table 16–5, " Oracle Business Intelligence Configuration Standard"

Note: All the compliance Rules for Oracle Fusion Applications currently share the following attributes:

Type: *Repository Rule*

Compliance Rule State: *Production*

Severity: *Minor warning*

Description: *Fusion Applications Configuration Rule for <Rule name>.*

Rationale: *<Rule name>*

Table 16–1 Java Platform Security Compliance Standard

Compliance Standard Rule Name	Recommended Value
JPS_jps.authz	ACC
JPS_jps.combiner.lazyeval	TRUE
JPS_jps.combiner.optimize	TRUE
Java Platform Security permission cache size	1000
Java Platform Security permission cache strategy	PERMISSION_FIFO
Java Platform Security Enable Policy Lazy Load Property	TRUE
JPS_jps.policystore.hybrid.mode	FALSE
Java Platform Security rolemember cache size	1000

Table 16–1 (Cont.) Java Platform Security Compliance Standard

Compliance Standard Rule Name	Recommended Value
Java Platform Security rolemember cache strategy	FIFO
Java Platform Security rolemember cache type	'STATIC
Java Platform Security Refresh Purge Time Out	1296000000

Table 16–2 Oracle HTTP Server Configuration Standard

Compliance Standard Rule Name	Recommended Value
Oracle HTTP Server keep alive timeout	61
Oracle HTTP Server maximum clients	1000
Oracle HTTP Server maximum keep alive requests	0
Oracle HTTP Server server limit	20
Fusion Applications Configuration rule for Oracle HTTP Server StartServers	10
Oracle HTTP Server threads per child	50
Oracle HTTP Server WLIOTimeoutSecs	900
Oracle HTTP Server Conn Retry Seconds	1
Oracle HTTP Server Custom Log	Enabled
Oracle HTTP Server File caching	OFF
Oracle HTTP Server Max Spare Threads	800
Oracle HTTP Server Min Spare Threads	200
Oracle HTTP Server Thread Limit	250
Oracle HTTP Server Browser caching	Enabled
OHS Set Env If No Case	'Request_URI \.swf$ no-gzip don't-vary'
Oracle HTTP Server Lock File	http_lock
Oracle HTTP Server StartServers	10

Table 16–3 WebLogic Server Configuration Standard

Compliance Standard Rule Name	Recommended Value
WebLogic Domain Log Severity	Error
WebLogic Log File Severity	Warning
WebLogic Memory Buffer Severity	Error
WebLogic stdout Severity	Error
WebLogic Keep Alive Enabled	TRUE
WebLogic Domain Cache Size	102400
WebLogic Domain Capacity Increment	1
WebLogic Domain Cache TTL	600

Table 16–3 (Cont.) WebLogic Server Configuration Standard

Compliance Standard Rule Name	Recommended Value
WebLogic Domain Conn. Creation Retry Frequency Seconds	60
WebLogic Domain Elf Fields	'date time time-taken bytes cs-method cs-uri sc-status sc(X-ORACLE-DMS-ECID) cs(ECID-Context) cs(Proxy-Remote-User) cs(Proxy-Client-IP)'
WebLogic Domain File Name	'logs/access.log.%yyyyMMdd%'
WebLogic Domain Highest Num Waiters	2147483647
WebLogic Domain Ignore In Use Connections Enabled	TRUE
WebLogic Domain Max Group Hierarchies In Cache	15000
WebLogic Domain Log File Format	Extended
WebLogic Domain Login Delay Seconds	0
WebLogic Domain Pinned To Thread	FALSE
WebLogic Domain Statement Cache Size	5
WebLogic Domain Statement Timeout	-1
WebLogic Domain Test Table Name	SQL SELECT 1 FROM DUAL
WebLogic Domain Test Frequency Seconds	300
WebLogic Domain Test Connections On Reserve	TRUE
WebLogic Domain Enable Group Membership Lookup Hierarchy Caching	TRUE
WebLogic Domain Second To Trust An Idle Conn.	0
WebLogic Domain Initial Capacity	0'
WebLogic Domain Min Capacity	0'
WebLogic Domain Max Capacity	100
WebLogic Domain Inactive Conn. Timeout Seconds	0
WebLogic Domain Init SQL	SQL SELECT 1 FROM DUAL'
WebLogic Domain State Check Interval	1000

Table 16–4 Java Virtual Machine Configuration Standard

Compliance Standard Rule Name	Recommended Value
JVM_HTTPClient.socket.connectionTimeout	300000
JVM_HTTPClient.socket.readTimeout	300000
JVM_HeapDumpOnOutOfMemoryError	+HeapDumpOnOutOfMemoryError
JVM_VOMaxFetchSize	N/A

Table 16–4 (Cont.) Java Virtual Machine Configuration Standard

Compliance Standard Rule Name	Recommended Value
JVM_Xgc	genpar
JVM_Xmanagement	1
JVM_Xverbose	gc
JVM_jbo.ampool.minavailablesize	1
JVM_jbo.ampool.timetolive	-1
JVM_jbo.doconnectionpooling	TRUE
JVM_jbo.load.components.lazily	TRUE
JVM_jbo.max.cursors	5
JVM_jbo.recyclethreshold	75
JVM_jbo.txn.disconnect_level	1
JVM_jps.auth.debug	FALSE
JVM_jrockit	jrockit
JVM_weblogic.ProductionModeEnabled	TRUE
JVM_weblogic.SocketReaders	3
JVM_ weblogic.http.client.weblogic.http.client.defaultConnectTimeout	300000
JVM_weblogic.http.client.defaultReadTimeout	300000
JVM_ weblogic.security.providers.authentication.LDAPDelegatePoolSize	20

Table 16–5 Oracle Business Intelligence Configuration Standard

Compliance Standard Rule Name	Recommended Value
BI Presentation Service Client Session Expire Minutes	210
BI Server DB Gateway Thread Range	40-200
BI Server DB Gateway Thread Stack Size	0
BI Server Enable	YES
BI Server Init Block Cache Entries	20
BI Server Max Cache Entries	1000
BI Server Max cache Entry Size	20 MB
BI Server Max Drilldown Query Cache Entries	1024
BI Server Max Expanded Subquery Predicates	8192

Table 16–5 (Cont.) Oracle Business Intelligence Configuration Standard

Compliance Standard Rule Name	Recommended Value
BI Server Max Query Plan Cache Entries	1024
BI Server Max Request Per Session Limit	5000
BI Server Max Session Limit	2000
BI Presentation Service New Sync Logon Wait Seconds	60
BI Server Read Only Mode	NO
BI Server Thread Range	40-1000
BI Server Thread Stack Size	0
BI Presentation Service Path Job Log	'saw.mktgsqlsubsystem.joblog'
BI Presentation Service Path Saw	saw
BI Server FMW Sec.Max No. Of Connections	2000
BI Presentation Service Max Queue	N/A
BI Presentation Service Max Queue	N/A

16.6.3.2 Applying Standards to Targets in Your Fusion Instance

To associate the compliance Rules on your own Oracle Fusion Applications instance, it is necessary to apply the relevant Standards to the relevant targets.

To associate predefined Standards to targets:

1. Navigate to **Enterprise** -> **Compliance** -> **Library** and then select the **Compliance Standards** tab.
2. Expand the **Search** item at the top of the page and select **Applicable To: Fusion Instance.** Click **Search**.

   The predefined Standards are listed.
3. Select a Standard and click **Associate Targets.**
4. On the **Target Association** page, click **+Add**. A search page is displayed.
5. Select the relevant target name(s) from the list and click **Select**.

   The host(s) appear in the Target Association page.
6. Select the host(s) and click **Enable**.
7. Click **OK**.
8. On the Save Association window that appears, click **YES**.

After a Compliance Standard is associated to a specific target, the results can be seen almost immediately in the Compliance Results page.

16.6.3.2.1 Optional: Creating, Editing, or Deleting Compliance Details Rules, Standards, and Frameworks can all be created, edited, or deleted as desired. To do so requires having the correct user permissions. Thereafter, it is a simple matter to click the appropriate button (such as **Create**) and fill out the subsequent page.

For information on Compliance user permissions, see: "Privileges and Roles Needed to Use the Compliance Features", in the "Managing Compliance" chapter of the *Oracle® Enterprise Manager Lifecycle Management Administrator's Guide*.

For information on how to create, edit, or delete, see:

- "Operations on Compliance Frameworks,"
- "Operations on Compliance Standards," and
- "Operations on Compliance Standards Rules," in the *Oracle® Enterprise Manager Lifecycle Management Administrator's Guide*

16.6.3.2.2 Optional: Creating Real-Time Monitoring Facets Real-time monitoring facets allow an administrator to receive warnings that are generated on-the-fly, should certain sensitive files be accessed or changed. This is especially useful as a security alert in case of any potential unauthorized activity to important parts of the system.

There are no real-time monitoring facets delivered with Cloud Control 12c, version 12.1.0.5, for Oracle Fusion Applications. To create your own and apply them to your system, see "Real Time Monitoring Facets" in the **"Managing Compliance"** chapter of *Oracle® Enterprise Manager Lifecycle Management Administrator's Guide*.

16.7 Configuring Oracle HTTP Server with Custom Certificates

If you have implemented Simple topology, SSL will terminate at OHS. Provisioning configures OHS with a default dummy certificate. As the dummy certificate is not trusted by browsers, you will get certificate warning messages when you access any external URL.

To avoid this, you need to configure OHS to use certificate(s) signed by a trusted certificate authority (CA). It can be an external certificate authority such as Verisign, or an internal certificate authority whose root certificate is trusted by the browser.

You can generate a certificate signing request and obtain signed certificate(s) and import these certificate(s) into wallet(s). There are two options for choosing certificate(s) and the OHS configuration will be different based on the option you choose.

Option 1:

Obtain a wildcard or Subject Alternative Name (SAN) certificate. A single wildcard certificate can protect all sub-domains at the same level (for example, *.mycompany.com can be used for both fin.mycompany.com and prj.mycompany.com). A SAN certificate can protect various domains mentioned in the Subject Alternative Name field.

You can import a single certificate (SAN or wildcard) into the wallet. Wallet location is specified using SSLWallet directive in `${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/FusionSSL.conf` and by default points to the directory containing the default wallet.

To specify the wallet containing the signed certificate, comment the existing SSLWallet directive and add a new line which points to the directory containing the wallet you have created, for example,

```
SSLWallet "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_
NAME}/keystores/myWallet
```

Option 2

Obtain a separate server certificate for all external URLs. You can procure up to 10 certificates, one for each external URL. This number will vary depending on the offerings you choose to provision.

1. Create a separate wallet for each certificate and import the certificates into them, since a wallet can only hold a single server certificate.
2. Copy `FusionSSL.conf` into separate files, one for each certificate (for example, `FusionSSL_fin.conf`, `FusionSSL_hcm.conf`, and so on).
3. Edit the individual `FusionSSL_<product>.conf` and edit SSLWallet directive to point to the directory containing the wallet you have created, for example,

   ```
   FusionSSL_hcm.conf -> SSLWallet "${ORACLE_INSTANCE}/config/${COMPONENT_
   TYPE}/${COMPONENT_NAME}/keystores/hcm
   ```

4. Specify the modified SSL configuration files in external Virtual Hosts defined in the `FusionVirtualHost_<product>.conf` files present in the `${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}` directory.

   By default, all VirtualHost entries for external URLs point to a single `FusionSSL.conf` file. You can edit this line in each file to point to the respective `FusionSSL_<product>.conf` file.

   For example, change the fragment as follows:

   #External virtual host for hcm

   ```
   <VirtualHost hcm.mycompany.com:10620>

    ServerName https://hcm.mycompany.com:10620

    include "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_
   NAME}/FusionSSL.conf"
   ```

   to

   #External virtual host for hcm

   ```
   <VirtualHost hcm.mycompany.com:10620>

    ServerName https://hcm.mycompany.com:10620

   #    include "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_
   NAME}/FusionSSL.conf"

   include "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_
   NAME}/FusionSSL_hcm.conf"
   ```

After making all the necessary changes, restart OHS.

For more information about generating wallets, see the *Oracle Fusion Middleware Administrator's Guide*.

16.8 Setting Up Backup for Oracle Fusion Applications

If you have Enterprise Manager Cloud Control and want to use it for backing up and restoring Oracle Fusion Applications, you must set it up before performing your initial backup. Follow the instructions detailed in "Prerequisites for Using Cloud Control to

Back Up or Restore Your Environment" in the *Oracle Fusion Applications Administrator's Guide*.

If you do not want to use Enterprise Manager Cloud Control, you may also perform backup and restore using operating system commands or third party tools to back up the Oracle Fusion Applications and Oracle Identity Management file systems, as well as database tools to back up the databases.

Ensure you perform a full backup either immediately or when you have completed the remaining post-installation tasks. See "Performing a Backup" in the *Oracle Fusion Applications Administrator's Guide* for instructions on how to perform a backup using Enterprise Manager Cloud Control or command line.

16.9 Setting up Oracle Enterprise Manager Cloud Control to Monitor and Manage Oracle Fusion Applications

Oracle Enterprise Manager Cloud Control (Cloud Control) is a system management software that delivers centralized monitoring, administration, and life cycle management functionality for the complete Oracle Fusion Applications IT infrastructure from one single console. For example, you can monitor all the Oracle WebLogic Server domains for all the product families from one console.

See the following documentation to install Cloud Control:

- *Oracle Enterprise Manager Cloud Control Basic Installation Guide*
- *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*

16.10 Completing Conditional Oracle Identity Management Post-Installation Tasks

Review and complete the conditional Oracle Identity Management Post-Installation tasks described in this section.

16.10.1 Updating Oracle Identity Management HTTP Server Runtime Parameters

By default, the Oracle HTTP Server contains parameter values that are suitable for most applications. These values, however, must be adjusted in IDM Deployments, on both WEBHOST1 and WEBHOST2.

Proceed as follows:

1. Edit the file `httpd.conf`, which is located in:

   `WEB_ORACLE_INSTANCE``/config/OHS/`*`component_name`*

2. Find the entry that looks like this:

   ```
   <IfModule mpm_worker_module>
   ```

3. Update the values in this section as follows:

   ```
   <IfModule mpm_worker_module>
     ServerLimit 20
     MaxClients 1000
     MinSpareThreads 200
     MaxSpareThreads 800
     ThreadsPerChild 50
     MaxRequestsPerChild 10000
   ```

```
  AcceptMutex fcntl
</IfModule>
```

4. Leave all remaining values unchanged.
5. Save the file.

16.10.2 Post-Provisioning Steps for Oracle Access Manager

Perform the tasks in the following sections:

- Section 16.10.2.1, "Updating Existing WebGate Agents"
- Section 16.10.2.2, "Update WebGate Configuration"

The Oracle Identity Management Console URLs are provided in Chapter 10.9.2, "About Oracle Identity Management Console URLs"

16.10.2.1 Updating Existing WebGate Agents

Update the OAM Security Model of all WebGate profiles, with the exception of Webgate_IDM and Webgate_IDM_11g, which should already be set

To do this, perform the following steps:

1. Log in to the Oracle Access Manager Console as the Oracle Oracle Access Manager administration user.
2. Click the **System Configuration** tab.
3. Expand **Access Manager Settings - SSO Agents**.
4. Click **OAM Agents** and select **Open** from the **Actions** menu.
5. In the Search window, click **Search**.
6. Click an Agent, for example: **IAMSuiteAgent**.
7. Set the Security value to the security model in the **OAM Configuration** screen of the Oracle Identity Management Provisioning Wizard, as described in Chapter 10.2, "Creating an Oracle Identity Management Provisioning Profile".

   Click **Apply**.
8. Restart the managed servers WLS_OAM1 and WLS_OAM2 as described in Section 10.9.1, "Starting and Stopping Components".

16.10.2.2 Update WebGate Configuration

To update the maximum number of WebGate connections, proceed as follows.

1. In the Oracle Access Manager Console, select the **System Configuration** tab.
2. Select **Access Manager -> SSO Agents -> OAM Agent** from the directory tree. Double-click or select the Open Folder icon.
3. On the displayed search page, click **Search** to perform an empty search.
4. Click the Agent **Webgate_IDM**.
5. Select **Open** from the Actions menu.
6. Set **Maximum Number of Connections** to `20` for all of the OAM Servers listed in the primary servers list. (This is the total maximum number of connections for the primary servers, which is 10 wls_oam1 connections plus 10 wls_oam2 connections.)

7. Set **AAA Timeout Threshold** to `5`.
8. In the **User Defined Parameters** box, set `client_request_retry_attempts` to `11`.
9. If the following Logout URLs are not listed, add them:
   - `/oamsso/logout.html`
   - `/console/jsp/common/logout.jsp`
   - `/em/targetauth/emaslogout.jsp`
10. Click **Apply**.
11. Repeat Steps 4 to 7 for each WebGate.

16.10.2.3 Creating Oracle Access Manager Policies for WebGate 11*g*

In order to allow WebGate 11*g* to display the credential collector, you must add `/oam` to the list of public policies.

Do the following:

1. Log in to the OAM console at: `http://ADMIN.mycompany.com/oamconsole`
2. Select the **Policy Configuration** tab.
3. Expand **Application Domains - IAM Suite**
4. Click **Resources**.
5. Click **Open**.
6. Click **New resource**.
7. Provide the following values:
   - **Type**: `HTTP`
   - **Description**: `OAM Credential Collector`
   - **Host Identifier**: `IAMSuiteAgent`
   - **Resource URL**: `/oam`
   - **Protection Level**: `Unprotected`
   - **Authentication Policy**: `Public Policy`
8. Leave all other fields at their default values.
9. Click **Apply**.

16.10.3 Configuring Oracle Identity Federation

This section is not applicable for the Single Host topology or when all Oracle Identity Management products are installed on the same host.

The Oracle Identity Management provisioning tools create, but do not start, Oracle Identity Federation. This section explains how to enable Oracle Identity Federation after provisioning has completed.

Oracle Identity Federation is an optional component. If you are not planning to use Oracle Identity Federation, skip this section. This section describes how to extend the Oracle Identity Management domain to include Oracle Identity Federation in an enterprise deployment.

This section contains the following topics:

- Starting Oracle Identity Federation Managed Servers
- Updating OIF Web Configuration
- Validating Oracle Identity Federation
- Configuring the Enterprise Manager Agents
- Enabling Oracle Identity Federation Integration with LDAP Servers
- Updating the Oracle Identity Federation Authentication Scheme in Oracle Access Manager
- Setting Oracle Identity Federation Authentication Mode and Enabling Password Policy Profile
- Enabling and Disabling Oracle Identity Federation

16.10.3.1 Starting Oracle Identity Federation Managed Servers

Do the following to start the managed servers wls_oif1 and wls_oif2:

1. Run `stopall.sh` as described in Chapter 10.9.1, "Starting and Stopping Components".
2. Edit the `oif_startup.conf` file to automatically start Oracle Identity Federation. This file is located in the directory: *`IDM_CONFIG`*`/scripts`.

```
#
# OIF is enabled OOTB for Shared IDM
#
# OIF_ENABLED indicates whether or not OIF should be started/stopped
# as part of the startoif.sh/stopoif.sh scripts. Valid values are true or false
# If false, the OIF will not be started or stopped
OIF_ENABLED=true
# OPMN_EMAGENT_MANAGED_BY_OIF_SCRIPT indicates whether or not OPMN and
# the EMAgent components for the OIM domain should be started, when OIF is
enabled.
# Valid values are true or false. If false, OPMN and the EMAgent components
will not
# be started or stopped when OIF is enabled.
# If OIF is disabled, OPMN and the EMAgent components will not be started or
stopped
OPMN_EMAGENT_MANAGED_BY_OIF_SCRIPT=true
```

   Save the file.

3. Run `startall.sh` as described in Chapter 10.9.1, "Starting and Stopping Components".

16.10.3.2 Updating OIF Web Configuration

Edit the `idminternal_vh.conf` file, which is located in *`WEB_ORACLE_INSTANCE`*`/config/OHS/`*`component`*`/modultconf`.

Add the following lines inside the VirtualHost block:

```
################################################
## Entries Required by Oracle Identity Federation
################################################

   #OIF
   <Location /fed>
      SetHandler weblogic-handler
      WLProxySSL ON
```

```
    WLProxySSLPassThrough ON
    WebLogicCluster IDMHOST1.mycompany.com:7499,IDMHOST2.mycompany.com:7499
</Location>
```

Save the file and restart the Oracle HTTP Server as described in Chapter 10.9.1, "Starting and Stopping Components".

Repeat this for each Oracle HTTP Server instance.

16.10.3.3 Validating Oracle Identity Federation

Validate the configuration of Oracle Identity Federation on IDMHOST1 and IDMHOST2 by accessing the Service Provider (SP) metadata on each host.

On IDMHOST1, access the SP metadata by going to:

`http://IDMHOST1.mycompany.com:7499/fed/sp/metadata`

On IDMHOST2, access the SP metadata by going to:

`http://IDMHOST2.mycompany.com:7499/fed/sp/metadata`

If the configuration is correct, you can access the following URL from a web browser:

`https://SSO.mycompany.com/fed/sp/metadata`

You should see metadata.

16.10.3.4 Configuring the Enterprise Manager Agents

All the Oracle Fusion Middleware components deployed in this enterprise deployment are managed by using Oracle Enterprise Manager Fusion Middleware Control. To manage Oracle Identity Federation with this tool, you must configure the EM agents with the correct monitoring credentials. Update the credentials for the EM agents associated with IDMHOST1 and IDMHOST2. Follow these steps to complete this task:

1. Use a web browser to access Oracle Enterprise Manager Fusion Middleware Control at `http://`*`ADMINVHN`*`.mycompany.com:7001/em`. Log in as the WebLogic user.
2. From the Domain Home Page, navigate to the Agent-Monitored Targets page using the menu under **Farm -> Agent-Monitored Targets**.
   a. Click the **Configure** link for the Target Type Identity Federation Server to go to the Configure Target Page.
   b. On the Configure Target Page, click **Change Agent** and choose the correct agent for the host.

      Note: If you are unsure about which agent to update, execute the command:

      `OIF_ORACLE_INSTANCE``/EMAGENT/EMAGENT/bin/emctl status agent`

   c. Update the **WebLogic monitoring user name** and the **WebLogic monitoring password**. Enter `weblogic_idm` as the WebLogic monitoring user name and the password for the weblogic user as the WebLogic monitoring password.
   d. Click **OK** to save your changes.

16.10.3.5 Enabling Oracle Identity Federation Integration with LDAP Servers

This section is not applicable for the Single Host topology or when all Oracle Identity Management products are installed on the same host.

By default, Oracle Identity Federation is not configured to be integrated with LDAP Servers deployed in a high availability configuration. To integrate Oracle Identity Federation with highly available LDAP Servers to serve as user data store, federation data store, or authentication engine, you must configure Oracle Identity Federation based on the LDAP server's function.

Proceed as follows to integrate Oracle Identity Federation with an LDAP Server deployed in a high availability configuration

1. On IDMHOST1, set environment variables as follows:

   Set `DOMAIN_HOME` to *`IDM_CONFIG/domains/IDMDomain`*

   Note: If you are using the Local Domain Configuration option, set `DOMAIN_HOME` to *IDM_CONFIG/domains/IDMDomain*.

   Set `IDM_ORACLE_HOME` to *`IDM_ORACLE_HOME`*

2. Set Oracle Identity Federation-specific environment variables by executing the `setOIFEnv.sh` script. This script is located under the *IDM_BASE*`/products/dir/idm/fed/scripts` directory.

   For example:

   ```
   cd IDM_BASE/products/dir/idm/fed/scripts
   . setOIFEnv.sh
   ```

3. On IDMHOST1, run the `WLST` script located under the *IDM_BASE*`/products/dir/oracle_common/bin` directory.

   ```
   cd IDM_BASE/products/dir/oracle_common/common/bin
   ./wlst.sh
   ```

4. Connect to one of the Oracle Identity Federation Managed Servers:

   ```
   connect()
   ```

   Enter the username and password to connect to the Oracle Identity Federation Managed Servers. This is the same as the WebLogic Administration user name and password.

   Enter the URL to connect to the Oracle Identity Federation Managed Server:

   ```
   t3://IDMHOST1.mycompany.com:7499
   ```

5. Then enter the following properties, as needed:

   - To integrate the user data store with a highly available LDAP Server, set the `userldaphaenabled` boolean property from the `datastore` group to `true`:

     ```
     setConfigProperty('datastore','userldaphaenabled', 'true', 'boolean')
     Update was successful for: userldaphaenabled
     ```

   - Validate the user data store is integrated with a highly available LDAP store by running:

     ```
     getConfigProperty('datastore', 'userldaphaenabled')
     Value(s) for property: true
     ```

     The userldaphaenabled property must return `true`.

- To integrate the LDAP authentication engine with a highly available LDAP Server, set the `ldaphaenabled` boolean property from the `authnengines` group to `true`:

```
setConfigProperty('authnengines','ldaphaenabled', 'true', 'boolean')
Update was successful for: ldaphaenabled
```

- Validate the LDAP authentication engine is integrated with a highly available LDAP store by running:

```
getConfigProperty('authnengines','ldaphaenabled')
Value(s) for property: true
```

The `ldaphaenabled` property for the `authnengines` group must return `true`.

Note: On IDMHOST1, delete the following directories:

- *IDM_CONFIG/domains/IDMDomain*`/config/fmwconfig/servers/wls_oif1/applications`
- *IDM_CONFIG/domains/IDMDomain*`/config/fmwconfig/servers/wls_oif2/applications`

16.10.3.6 Updating the Oracle Identity Federation Authentication Scheme in Oracle Access Manager

Oracle Access Manager ships with an Oracle Identity Federation Authentication Scheme. This scheme needs to be updated before it can be used. To update the scheme, log in to the OAM console as the OAM administration user. The URL is: `http://ADMIN.mycompany.com/oamconsole`

Then perform the following steps:

1. Click the **Policy Configuration** tab.
2. Expand **Authentication Schemes** under the Shared Components tree.
3. Select **OIFScheme** from under the Authentication Schemes and then select **Open** from the menu.
4. On the Authentication Schemes page, provide the following information
   - **Challenge URL**: `https://SSO.mycompany.com:443/fed/user/spoam11g`
   - **Context Type**: Select **external** from the list.

   Accept the defaults for all other values
5. Click **Apply** to update the `OIFScheme`.

16.10.3.7 Setting Oracle Identity Federation Authentication Mode and Enabling Password Policy Profile

Proceed as follows:

1. On IDMHOST1, run the `WLST` script located under the *IDM_BASE*`/products/dir/oracle_common/bin` directory.

```
cd IDM_BASE/products/dir/oracle_common/common/bin
./wlst.sh
```

2. Connect to one of the Oracle Identity Federation Managed Servers:

```
connect()
```

Enter the username and password to connect to the Oracle Identity Federation Managed Servers. This is the same as the WebLogic Administration user name and password.

Enter the URL to connect to the Oracle Identity Federation Managed Server:

```
t3://IDMHOST1.mycompany.com:7001
```

3. To set Oracle Identity Federation authentication mode, execute the following WLST command:

```
domainRuntime()
```

4. To configure the Oracle Access Manager for Oracle Identity Federation SSO flows, execute the following WLST commands:

```
configOAMOIFSaaS(fedMode="Dedicated")

enablePasswordPolicyProfile()
```

16.10.3.8 Enabling and Disabling Oracle Identity Federation

In Service Provider (SP) mode, Oracle Access Manager delegates user authentication to Oracle Identity Federation, which uses the Federation Oracle Single Sign-On protocol with a remote Identity Provider. Once the Federation Oracle Single Sign-On flow is performed, Oracle Identity Federation will create a local session and then propagates the authentication state to Oracle Access Manager, which maintains the session information.

This section provides the steps to integrate Oracle Identity Federation with Oracle Identity Manager in authentication mode and SP mode.

> **Note:** Federation Trust must be established prior to enabling Oracle Identity Federation.

This section contains the following topics:

- Section 16.10.3.8.1, "Enabling Oracle Identity Federation"
- Section 16.10.3.8.2, "Disabling Oracle Identity Federation"

16.10.3.8.1 Enabling Oracle Identity Federation

This section describes how to switch the authentication of the Oracle Access Manager security domain from local authentication to Federation SSO.

Perform the following operations to switch from local authentication to Federation SSO for Browser Based Schemes:

1. In a browser, go to the OAM Console, at:

   ```
   http://ADMINVHN.mycompany.com:7001/oamconsole
   ```

   Log in as the Oracle Access Manager user.

2. Navigate to **Policy Configuration -> Shared Components -> Authentication Schemes -> FAAuthScheme**.

3. Set the **Challenge Method** to **FORM**.

4. Set the **Authentication Module** to `SaaSModule`.

5. Set the **Challenge URL** to `/pages/oamLogin.jsp`.
6. Set the **Context Type** to **customWar**.
7. Set the **Context Value** to `/fusion_apps`.
8. Set the Challenge Parameters field with the following entries:
   - `federationEnabled=true`
   - `ssoChooserEnabled=false`[1]
   - `fedSSOEnabled=true`
   - `initial_command=NONE`
   - `TAPPartnerId=OIFDAPPartner`
   - `TAPChallengeURL=https://SSO.mycompany.com:443/fed/user/spoam11g`
9. Click **Apply**.

16.10.3.8.2 Disabling Oracle Identity Federation This section describes how to switch the authentication of the OAM security domain from Federation SSO to local authentication.

Perform the following operations to switch from local authentication to Federation SSO for Browser Based Schemes:

1. In a browser, go to the OAM Console, at:

   `http://ADMINVHN.mycompany.com:7001/oamconsole`

   Log in as the Oracle Access Manager user.
2. Navigate to **Policy Configuration -> Shared Components -> Authentication Schemes -> FAAuthScheme**.
3. Set the **Challenge Method** to **FORM**.
4. Set the **Authentication Module** to `SaaSModule`.
5. Set the **Challenge URL** to `/pages/oamLogin.jsp`.
6. Set the **Context Type** to **customWar**.
7. Set the **Context Value** to `/fusion_apps`.
8. Set the Challenge Parameters field with the following entries:
   - `federationEnabled=false`
   - `ssoChooserEnabled=false`
   - `fedSSOEnabled=false`
   - `initial_command=NONE`
   - `TAPPartnerId=OIFDAPPartner`
   - `TAPChallengeURL=https://SSO.mycompany.com:443/fed/user/spoam11g`
9. Click **Apply**.

[1] If dual authentication mode is required, set `ssoChooserEnabled=true` instead of `ssoChooserEnabled=false`. Dual authentication mode is required when some users in the Oracle Fusion Applications LDAP directory do not exist in the Identity Provider's directory. Those users cannot be authenticated with Federation SSO and must be challenged locally.

16.10.4 Configuring Identity Integration with Active Directory

This section describes how to add support for Active Directory to your enterprise deployment.

This section contains the following topics:

- Section 16.10.4.1, "Creating Adapters in Oracle Virtual Directory"
- Section 16.10.4.2, "Preparing Active Directory"
- Section 16.10.4.3, "Modifying Oracle Identity Manager to Support Active Directory"
- Section 16.10.4.4, "Updating the Username Generation Policy for Active Directory"

16.10.4.1 Creating Adapters in Oracle Virtual Directory

Oracle Virtual Directory communicates with other directories through adapters.

The procedure is slightly different, depending on the directory you are connecting to. The following sections show how to create and validate adapters for supported directories:

- Section 16.10.4.1.1, "Removing Existing Adapters"
- Section 16.10.4.1.2, "Creating an Oracle Virtual Directory Adapter for Active Directory"
- Section 16.10.4.1.3, "Validating the Oracle Virtual Directory Adapters"

16.10.4.1.1 Removing Existing Adapters The provisioning process created Oracle Virtual Directory adapters to Oracle Internet Directory. When you switch the identity store to Active Directory, you must remove these adapters.

1. Log in to Oracle Directory Services Manager (ODSM) at:
   `http://admin.mycompany.com/odsm`
2. If you have not already done so, create connections to each of your Oracle Virtual Directory instances.
3. Select one of the Oracle Virtual Directory instances and connect to it.
4. Click the **Adapter** tab.
5. Click the adapter **User ID**.
6. Click **Delete Selected Adapter**.
7. Repeat for the adapter **CHANGELOG_OID**.
8. Repeat Steps 1- 7 for each Oracle Virtual Directory instance.

16.10.4.1.2 Creating an Oracle Virtual Directory Adapter for Active Directory You can use `idmConfigTool` to create the Oracle Virtual Directory User and Changelog adapters for Oracle Internet Directory and Active Directory. Oracle Identity Manager requires adapters. It is highly recommended, though not mandatory, that you use Oracle Virtual Directory to connect to Oracle Internet Directory.

1. Set the environment variable `ORACLE_HOME` to *`IDM_BASE/products/app/iam`*.
2. Create a properties file for the Active Directory adapter called `ovd1.props`, with the following content:

```
ovd.host:LDAPHOST1.mycompany.com
ovd.port:8899
```

```
ovd.binddn:cn=orcladmin
ovd.password:ovdpassword
ovd.oamenabled:true
ovd.ssl:true
ldap1.type:AD
ldap1.host:ADIDSTORE.mycompany.com
ldap1.port:636
ldap1.binddn:cn=adminuser
ldap1.password:adpassword
ldap1.ssl:true
ldap1.base:dc=mycompany,dc=com
ldap1.ovd.base:dc=mycompany,dc=com
usecase.type: single
```

The following list describes the parameters used in the properties file.

- `ovd.host` is the host name of a server running Oracle Virtual Directory.
- `ovd.port` is the https port used to access Oracle Virtual Directory (*`OVD_ADMIN_PORT`*).
- `ovd.binddn` is the user DN you use to connect to Oracle Virtual Directory.
- `ovd.password` is the password for the DN you use to connect to Oracle Virtual Directory.
- `ovd.oamenabled` is always `true` in Oracle Fusion Applications deployments.
- `ovd.ssl` is set to `true`, as you are using an https port.
- `ldap1.type` is set to OID for the Oracle Internet Directory back end directory or set to AD for the Active Directory back end directory.
- `ldap1.host` is the host on which back end directory is located. Use the load balancer name.
- `ldap1.port` is the port used to communicate with the back end directory (*`OID_LDAP_PORT`*).
- `ldap1.binddn` is the bind DN of the `oimLDAP` user.
- `ldap1.password` is the password of the `oimLDAP` user
- `ldap1.ssl` is set to `true` if you are using the back end's SSL connection, and otherwise set to `false`. This should always be set to `true` when an adapter is being created for AD.
- `ldap1.base` is the base location in the directory tree.
- `ldap1.ovd.base` is the mapped location in Oracle Virtual Directory.
- `usecase.type` is set to `Single` when using a single directory type.

3. Configure the adapter by using the `idmConfigTool` command, which is located at:

   `IDM_BASE/products/app/iam``/idmtools/bin`

   Note: When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:

   `IDM_BASE/products/app/iam``/idmtools/bin`

The syntax of the command is:

```
idmConfigTool.sh -configOVD input_file=configfile [log_file=logfile]
```

For example:

```
idmConfigTool.sh -configOVD input_file=ovd1.props
```

The command requires no input. The output looks like this:

```
The tool has completed its operation. Details have been logged to logfile
```

Perform the following tasks on IDMHOST1:

Run this command for each Oracle Virtual Directory instance in your topology, with the appropriate value for `ovd.host` in the property file.

16.10.4.1.3 Validating the Oracle Virtual Directory Adapters Perform the following tasks by using ODSM:

1. Access ODSM through the load balancer at: `http://ADMIN.mycompany.com/odsm`
2. Connect to Oracle Virtual Directory.
3. Go the **Data Browser** tab.
4. Expand **Client View** so that you can see each of your user adapter root DNs listed.
5. Expand the user adapter root DN, if there are objects already in the back end LDAP server, you should see those objects here. ODSM does not support changelog query, so you cannot expand the `cn=changelog` subtree.
6. Perform the following tasks by using the command-line:
   a. Validate the user adapters by typing:

      ```
      ldapsearch -h directory_host -p ldap_port -D "cn=orcladmin" -q  -b <user_
      search_base> -s sub "objectclass=inetorgperson" dn
      ```

      For example:

      ```
      ldapsearch -h LDAPHOST1.mycompany.com -p 6501 -D "cn=orcladmin" -q -b
      "cn=Users,dc=mycompany,dc=com" -s sub "objectclass=inetorgperson" dn
      ```

      Supply the password when prompted.

      You should see the user entries that already exist in the back end LDAP server.

   b. Validate changelog adapters by typing:

      ```
      ldapsearch -h directory_host -p ldap_port -D "cn=orcladmin" -q  -b
      "cn=changelog" -s one "changenumber>=0"
      ```

      For example:

      ```
      ldapsearch -h LDAPHOST1 -p 6501 -D "cn=orcladmin" -q -b "cn=changelog" -s
      one "changenumber>=0"
      ```

      The command returns logs of data, such as creation of all the users. It returns without error if the changelog adapters are valid.

   c. Validate lastchangenumber query by typing:

      ```
      ldapsearch -h directory_host -p ldap_port -D "cn=orcladmin" -q -b
      "cn=changelog" -s base 'objectclass=*' lastchangenumber
      ```

For example:

```
ldapsearch -h LDAPHOST1 -p 6501 -D "cn=orcladmin" -q -b "cn=changelog" -s
base 'objectclass=*' lastchangenumber
```

The command returns the latest change number generated in the back end LDAP server.

16.10.4.2 Preparing Active Directory

Prepare Active Directory as described in the following sections:

- Section 16.10.4.2.1, "Configuring Active Directory for Use with Oracle Access Manager and Oracle Identity Manager"
- Section 16.10.4.2.2, "Creating Users and Groups"
- Section 16.10.4.2.5, "Creating Access Control Lists in Non-Oracle Internet Directory Directories"

16.10.4.2.1 Configuring Active Directory for Use with Oracle Access Manager and Oracle Identity Manager This section describes how to configure Active Directory. Extend the schema in Active Directory as follows.

IMPORTANT: The order in which you perform the steps is critical!

1. Locate the following files:

   IDM_BASE`/products/dir/idm/oam/server/oim-intg/ldif/ad/schema/ADUserSchema.ldif`

   IDM_BASE`/products/dir/idm/oam/server/oim-intg/ldif/ad/schema/AD_oam_pwd_schema_add.ldif`

2. In both these files, replace the `domain-dn` with the appropriate `domain-dn` value

3. Use `ldapadd` from the command line to load the two LDIF files, as follows.

   ```
   ldapadd -h activedirectoryhostname -p activedirectoryportnumber -D AD_
   administrator -q -c -f file
   ```

   where *AD_administrator* is a user which has schema extension privileges to the directory

   For example:

   ```
   ldapadd -h "ACTIVEDIRECTORYHOST.mycompany.com" -p 389 -D adminuser -q -c -f
   ADUserSchema.ldif
   ldapadd -h "ACTIVEDIRECTORYHOST.mycompany.com" -p 389 -D adminuser -q -c -f AD_
   oam_pwd_schema_add.ldif
   ```

   Note: After the `-D` you can specify either a DN or *user@domain.com*.

4. Then go to:

   IDM_BASE`/products/app/oracle_common/modules/oracle.ovd_11.1.1/oimtemplates`

   Run the following command to extend Active Directory schema:

```
sh extendadschema.sh -h AD_host -p AD_port -D 'administrator@mydomain.com' -AD
"dc=mydomain,dc=com" -OAM true
```

16.10.4.2.2 Creating Users and Groups Create users and groups as described in the following sections.

16.10.4.2.3 Creating Users and Groups by Using the idmConfigTool Configure the Identity Store by using the command `idmConfigTool`, which is located at:

IDM_BASE/products/app/iam/idmtools/bin

> **Note:** When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory in which the `idmConfigTool` is run. To ensure that the same file is appended to every time you run the tool, always run the `idmConfigTool` from the directory:
>
> *IDM_BASE/products/app/iam*/idmtools/bin

The syntax of the command on Linux is:

```
idmConfigTool.sh -prepareIDStore mode=all input_file=configfile
```

For example:

```
idmConfigTool.sh -prepareIDStore mode=all input_file=idstore.props
```

When the command runs, it prompts you to enter the password of the account you are connecting to and passwords for the accounts that are being created.

> **Note:** The password must conform to the following rules:
>
> - Six characters or more
> - One or more numeric character
> - Two or more alphabetic characters
> - Start with alphabetic character
> - One or more lowercase character

> **Note:** This invocation of `idmConfigTool` creates the group `orclFAOAMUserWritePrivilegeGroup`.

16.10.4.2.4 Creating the Configuration File Create a property file, `idstore.props`, to use when preparing the Identity Store. The file will have the following structure:

```
# Common
IDSTORE_HOST: LDAPHOST1.mycompany.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
IDSTORE_SEARCHBASE: dc=mycompany,dc=com
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users, dc=mycompany,dc=com
```

```
POLICYSTORE_SHARES_IDSTORE: true
# OAM
IDSTORE_OAMADMINUSER:oamadmin
IDSTORE_OAMSOFTWAREUSER:oamLDAP
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN:OAMAdministrators
# OAM and OIM
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=mycompany,dc=com
# OIM
IDSTORE_OIMADMINGROUP: OIMAdministrators
IDSTORE_OIMADMINUSER: oimLDAP
# Required due to bug
IDSTORE_OAAMADMINUSER : oaamadmin
# Fusion Applications
IDSTORE_READONLYUSER: IDROUser
IDSTORE_READWRITEUSER: IDRWUser
IDSTORE_SUPERUSER: weblogic_fa
# Weblogic
IDSTORE_WLSADMINUSER : weblogic_idm
```

Where:

- `IDSTORE_BINDDN` is an administrative user in the Identity Store Directory
- `IDSTORE_GROUPSEARCHBASE` is the location in the directory where Groups are Stored.
- `IDSTORE_HOST` and `IDSTORE_PORT` are, respectively, the host and port of your Identity Store directory. Specify the back end directory here, rather than Oracle Virtual Directory, Active Directory: `LDAPHOST1` and `389`.
- `IDSTORE_LOGINATTRIBUTE` is the LDAP attribute which contains the users Login name.
- `IDSTORE_OAMADMINUSER` is the name of the user you want to create as your Oracle Access Manager Administrator.
- `IDSTORE_OAMSOFTWAREUSER` is a user that gets created in LDAP that is used when Oracle Access Manager is running to connect to the LDAP server.
- `IDSTORE_OIMADMINGROUP` Is the name of the group you want to create to hold your Oracle Identity Manager administrative users.
- `IDSTORE_OIMADMINUSER` is the user that Oracle Identity Manager uses to connect to the Identity store.
- `IDSTORE_READONLYUSER` is the name of a user you want to create which has Read Only permissions on your Identity Store.
- `IDSTORE_READWRITEUSER` is the name of a user you want to create which has Read/Write permissions on your Identity Store.
- `IDSTORE_SUPERUSER` is the name of the administration user you want to use to log in to the WebLogic Administration Console in the Oracle Fusion Applications domain.
- `IDSTORE_SEARCHBASE` is the location in the directory where Users and Groups are stored.
- `IDSTORE_SYSTEMIDBASE` is the location of a container in the directory where users can be placed when you do not want them in the main user container. This happens rarely but one example is the Oracle Identity Manager reconciliation user which is also used for the bind DN user in Oracle Virtual Directory adapters.
- `IDSTORE_USERSEARCHBASE` is the location in the directory where Users are Stored.

- OAM11G_IDSTORE_ROLE_SECURITY_ADMIN is the name of the group which is used to allow access to the OAM console.
- POLICYSTORE_SHARES_IDSTORE is set to true for IDM 11*g*.
- IDSTORE_OAAMADMINUSER is required because of a bug in idmConfigTool.

16.10.4.2.5 Creating Access Control Lists in Non-Oracle Internet Directory Directories In the preceding sections, you seeded the Identity Store with users and artifacts for the Oracle components. If your Identity Store is hosted in a non-Oracle Internet Directory directory, such as Microsoft Active Directory, you must set up the access control lists (ACLs) to provide appropriate privileges to the entities you created. This section lists the artifacts created and the privileges required for the artifacts.

- Users and groups. ACLs to the users and groups container are provided in Oracle Internet Directory. Set them manually for other directories. The Oracle Identity Manager/Oracle Access Manager integration and Oracle Fusion Applications require the following artifacts to be created in the Identity store.
  - Group with read privileges to the users container (orclFAUserReadPrivilegeGroup). Configure the local directory ACLs so that this group has privileges to read all the attributes of the users in the Identity Store.
  - Group with read/write privileges to the users container (orclFAUserWritePrivilegeGroup)
  - Group with read privileges to the groups container (orclFAGroupReadPrivilegeGroup)
  - Group with read privileges to the groups container (orclFAGroupWritePrivilegeGroup)
  - Group with write privileges to a partial set of attributes (orclFAUserWritePrefsPrivilegeGroup)
- The user specified by the IDSTORE_READONLYUSER parameter. When you run the preconfigIDstore command, this user is assigned to the groups orclFAUserReadPrivilegeGroup, orclFAWritePrefsPrivilegeGroup, and orclFAGroupReadPrivilegeGroup. The user also needs compare privileges to the userpassword attribute of the user entry.
- The user specified by the IDSTORE_READWRITEUSER parameter. It is assigned to the groups orclFAUserWritePrivilegeGroup and orclFAGroupWritePrivilegeGroup.
- System IDs. The System ID container is created for storing all the system identifiers. If there is another container in which the users are to be created, that is specified as part of the admin.
- Oracle Access Manager Admin User. This user is added to the OAM Administrator group, which provides permission for the administration of the Oracle Access Manager Console. No LDAP schema level privileges are required, since this is just an application user.
- Oracle Access Manager Software User. This user is added to the groups where the user gets read privileges to the container. This is also provided with schema admin privileges.
- Oracle Identity Manager user oimLDAP under System ID container. Password policies are set accordingly in the container. The passwords for the users in the System ID container must be set up so that they do not expire.

- Oracle Identity Manager administration group. The Oracle Identity Manager user is added as its member. The Oracle Identity Manager admin group is given complete read/write privileges to all the user and group entities in the directory.
- WebLogic Administrator. This is the administrator of the IDM domain for Oracle Virtual Directory
- WebLogic Administrator Group. The WebLogic administrator is added as a member. This is the administrator group of the IDM domain for Oracle Virtual Directory.
- Reserve container. Permissions are provided to the Oracle Identity Manager admin group to perform read/write operations.

16.10.4.3 Modifying Oracle Identity Manager to Support Active Directory

When first installed, Oracle Identity Manager has a set of default system properties for its operation.

If your Identity Store is in Active Directory, you must change the System property `XL.DefaultUserNamePolicyImpl` to `oracle.iam.identity.usermgmt.impl.plugins.FirstNameLastNamePolicyForAD` or `oracle.iam.identity.usermgmt.impl.plugins.LastNameFirstNamePolicyForAD`.

To learn how to do this, see the Administering System Properties chapter of *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

16.10.4.4 Updating the Username Generation Policy for Active Directory

If your back-end directory is Active Directory, you must update Oracle Identity Manager so that it only allows user names with a maximum of 20 characters. This is a limitation of Active Directory. Update the username generation policy from `DefaultComboPolicy` to `FirstnameLastnamepolicyforAD` as follows.

1. Log in to the OIM Console at the URL listed in Section 10.9.2, "About Oracle Identity Management Console URLs."
2. Click **Advanced** on the top of the right pane.
3. Click **Search System properties.**
4. On the navigation bar in the left pane, search on **Username Generation**.
5. Click **Default Policy for Username Generation**.
6. In the **Value** field, update the entry from `oracle.iam.identity.usermgmt.impl.plugins.DefaultComboPolicy` to `oracle.iam.identity.usermgmt.impl.plugins.FirstNameLastNamePolicyForAD`.
7. Click **Save**.

16.10.5 Setting Up Oracle Identity Management Node Manager for SSL

Follow the instructions detailed in this section **ONLY** for EDG topology and only if you have selected the **Configure Second application instances** option on the Node Topology Configuration Page.

Failing Over the Administration Server on Windows

After performing Oracle Identity Management Provisioning, you might need to fail over the Administration Server from one node to a different node. The procedure on Windows is as follows:

1. Stop the WebLogic Administration Server.
2. Migrate the IP address to the second node.
3. Run the following command as root on the first node:

   ```
   netsh interface ip delete address interface netmask
   ```

   In the following example, the IP address is disabled on the interface Local Area Connection:

   ```
   netsh interface ip delete address "Local Area connection"
   100.200.140.206
   ```

4. Run the following command on the second node:

   ```
   netsh interface ip add address interface IP_Address netmask
   ```

   In the following example, the IP address is enabled on the interface Local Area Connection:

   ```
   netsh interface ip add address "Local Area connection" 100.200.140.206
   255.255.255.0
   ```

This section contains the following topics:

- Overview of the Node Manager
- Configuring Node Manager to Use SSL
- Update Domain to Access Node Manager Using SSL
- Update Start and Stop Scripts to Use SSL
- Enabling Host Name Verification Certificates for Node Manager
- Update boot.properties Files
- Starting Node Manager

16.10.5.1 Overview of the Node Manager

Node Manager enables you to start and stop the Administration Server and the Managed Servers.

Process

The topologies and hosts are shown in Table 16–6.

Table 16–6 Hosts in Each Topology

Topology	Hosts
OAM11g/OIM11g	IDMHOST1
	IDMHOST2
OIF11g	IDMHOST1
	IDMHOST2

Note that the procedures in this chapter must be performed multiple times for each VIP-and-IP pair using the information provided in the component-specific chapters.

Recommendations

Oracle provides two main recommendations for Node Manager configuration in enterprise deployment topologies:

- Oracle recommends placing the Node Manager log file in a location different from the default one (which is inside the Middleware Home where Node Manager resides).
- Oracle also recommends using host name verification for the communication between Node Manager and the servers in the domain. This requires the use of certificates for the different addresses used in the domain. This chapter explains the steps for configuring certificates in the hosts for host name verification. See Section 16.10.5.5, "Enabling Host Name Verification Certificates for Node Manager" for further details.

> **Note:** The passwords used in this guide are used only as examples. Use secure passwords in a production environment. For example, use passwords that consist of random sequences of both uppercase and lowercase characters as well as numbers.

16.10.5.2 Configuring Node Manager to Use SSL

By default, provisioning does not configure Node Manager in SSL mode. You must configure each node manager in the topology to use SSL.

For each node manager that has its configuration in *IDM_CONFIG*`/nodemanager/hostname`, perform the following steps:

1. Edit the file `nodemanager.properties`.
2. Change the line `SecureListener=false` to `SecureListener=true`.
3. Save the file.
4. Restart Node Manager by killing the `nodemanager` process, and restart by running the following command:

   ```
   startNodeManagerWrapper.sh
   ```

Repeat these steps for each node manager.

16.10.5.3 Update Domain to Access Node Manager Using SSL

1. Log in to the WebLogic Administration console as the user `weblogic_idm`. Console URLs are provided in Chapter 10.9.2, "About Oracle Identity Management Console URLs".
2. Select **IDMDomain > Environment > Machines** from the Domain Structure menu.
3. Click on **Lock and Edit**.
4. Click on one of the machines, for example **idmhost1.mycompany.com**.
5. Click on the **Node Manager** tab.
6. Change **Type** from **Plain** to **SSL**.
7. Click **Save**.
8. Repeat Steps 4-7 for each machine.
9. Click **Activate Changes**.

16.10.5.4 Update Start and Stop Scripts to Use SSL

You must update the following files, which are generated by the provisioning tool. Each of these files is located in the directory *IDM_CONFIG*`/scripts/basescripts`:

- `stop_nodemanager_template.py`
- `stop_adminserver_template.py`
- `start_adminserver_template.py`

Do the following for each of the files:

1. Locate the line in the file that starts with `nmConnect`.
2. Change the last parameter from `plain` to `SSL`.

   For example, in `start_adminserver_template.py`, change the line:

   ```
   nmConnect('admin', nmpwd, 'localhost', '5556', 'IDMDomain' ,
   '/u01/oracle/config/domains/IDMDomain' , 'Plain')
   ```

   to

   ```
   nmConnect('admin', nmpwd, 'localhost', '5556', 'IDMDomain' ,
   '/u01/oracle/config/domains/IDMDomain' , 'SSL')
   ```

3. Save the file.

16.10.5.5 Enabling Host Name Verification Certificates for Node Manager

This section describes how to set up host name verification certificates for communication between Node Manager and the Administration Server. It consists of the following steps:

- Section 16.10.5.5.1, "Generating Self-Signed Certificates Using the utils.CertGen Utility"
- Section 16.10.5.5.2, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility"
- Section 16.10.5.5.3, "Creating a Trust Keystore Using the Keytool Utility"
- Section 16.10.5.5.4, "Configuring Node Manager to Use the Custom Keystores"
- Section 16.10.5.5.5, "Configuring Managed Oracle WebLogic Servers to Use the Custom Keystores"
- Section 16.10.5.5.6, "Changing the Host Name Verification Setting for the Managed Servers"

16.10.5.5.1 Generating Self-Signed Certificates Using the utils.CertGen Utility

The certificates added in this chapter (as an example) address a configuration where Node Manager listens on a physical host name (*HOST*.mycompany.com) and a WebLogic Managed Server listens on a virtual host name (*VIP*.mycompany.com). Whenever a server is using a virtual host name, it is implied that the server can be migrated from one node to another. Consequently, the directory where keystores and trust keystores are maintained ideally must reside on a shared storage that is accessible from the failover. If additional host names are used in the same or different nodes, the steps in this example must be extended to:

1. Add the required host names to the certificate stores (if they are different from *HOST*.mycompany.com and *VIP*.mycompany.com).
2. Change the identity and trust store location information for Node Manager (if the additional host names are used by Node Manager) or for the servers (if the additional host names are used by Managed Servers).

Follow these steps to create self-signed certificates on *HOST*. These certificates should be created using the network name or alias. For information on using trust CA

certificates instead, see "Configuring Identity and Trust" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*. The following examples configure certificates for *HOST*.mycompany.com and *VIP*.mycompany.com; that is, it is assumed that both a physical host name (*HOST*) and a virtual host name (*VIP*) are used in *HOST*. It is also assumed that *HOST*.mycompany.com is the address used by Node Manager and *VIP*.mycompany.com is the address used by a Managed Server or the Administration Server. This is the common situation for nodes hosting an Administration Server and a Fusion Middleware component, or for nodes where two Managed Servers coexist with one server listening on the physical host name and one server using a virtual host name (which is the case for servers that use migration servers).

1. Set up your environment by running the *IDM_BASE*`/products/app/wl_server10.3/server/bin/setWLSEnv.sh` script. In the Bourne shell, run the following commands:

   ```
   cd IDM_BASE/products/app/wl_server10.3/server/bin
   . ./setWLSEnv.sh
   ```

   Verify that the *CLASSPATH* environment variable is set:

   ```
   echo $CLASSPATH
   ```

2. Create a user-defined directory for the certificates. For example, create a directory called 'keystores' under the *IDM_CONFIG/domains/IDMDomain* directory. Note that certificates can be shared across WebLogic domains.

   ```
   cd IDM_CONFIG/domains/IDMDomain
   mkdir keystores
   ```

   Note: The directory where keystores and trust keystores are maintained must be on shared storage that is accessible from all nodes so that when the servers fail over (manually or with server migration), the appropriate certificates can be accessed from the failover node. Oracle recommends using central or shared stores for the certificates used for different purposes (like SSL set up for HTTP invocations, for example).

3. Change directory to the directory that you just created:

   ```
   cd keystores
   ```

4. Using the utils.CerGen tool, create certificates for each Physical and Virtual Host in the topology. For example:

   ```
   java utils.CertGen Key_Passphrase IDMHOST1.mycompany.com_cert
   IDMHOST1.mycompany.com_key domestic IDMHOST1.mycompany.com
   ```

   Other examples include: `IDMHOST2`, `ADMINVHN`, `SOAHOST1VHN`, `SOAHOST2VHN`, `OIMHOST1VHN`, and `OIMHOST2VHN`.

16.10.5.5.2 Creating an Identity Keystore Using the utils.ImportPrivateKey Utility

Follow these steps to create an identity keystore on IDMHOST1:

1. Create a new identity keystore called `appIdentityKeyStore` using the `utils.ImportPrivateKey` utility. Create this keystore under the same directory as the certificates (that is, *IDM_CONFIG/domains/IDMDomain/keystores*).

> **Note:** The Identity Store is created (if none exists) when you import a certificate and the corresponding key into the Identity Store using the `utils.ImportPrivateKey` utility.

2. The default password for the standard Java keystore is `changeit`. Oracle recommends always changing the default password. Use the `keytool` utility to do this. The syntax is:

   ```
   keytool -storepasswd -new New_Password -keystore Trust_Keystore -storepass
   Original_Password
   ```

   For example:

   ```
   keytool -storepasswd -new Key_Passphrase -keystore appTrustKeyStoreIDMHOST1.jks
   -storepass changeit
   ```

3. The CA certificate CertGenCA.der is used to sign all certificates generated by the utils.CertGen tool. It is located in the *WL_HOME*`/server/lib` directory. This CA certificate must be imported into the `appTrustKeyStore` using the `keytool` utility. The syntax is:

   ```
   keytool -import -v -noprompt -trustcacerts -alias Alias_Name
   -file CA_File_Location -keystore Keystore_Location -storepass Keystore_Password
   ```

   For example:

   ```
   keytool -import -v -noprompt -trustcacerts -alias clientCACert -file WL_
   HOME/server/lib/CertGenCA.der -keystore appTrustKeyStoreIDMHOST1.jks -storepass
   Key_Passphrase
   ```

16.10.5.5.3 Creating a Trust Keystore Using the Keytool Utility Follow these steps to create the trust keystore on each host, for example IDMHOST1 and IDMHOST2:

1. Copy the standard Java keystore to create the new trust keystore since it already contains most of the root CA certificates needed. Oracle does not recommend modifying the standard Java trust keystore directly. Copy the standard Java keystore CA certificates located under the *IDM_BASE*`/products/app/wl_server10.3/server/lib` directory to the same directory as the certificates. For example:

   ```
   cp IDM_BASE/products/app/wl_server10.3/server/lib/cacerts IDM_
   CONFIG/domains/IDMDomain/keystores/appTrustKeyStoreIDMHOST1.jks
   ```

2. The default password for the standard Java keystore is `changeit`. Oracle recommends always changing the default password. Use the `keytool` utility to do this. The syntax is:

   ```
   keytool -storepasswd -new New_Password -keystore Trust_Keystore -storepass
   Original_Password
   ```

   For example:

   ```
   keytool -storepasswd -new Key_Passphrase -keystore appTrustKeyStoreIDMHOST1.jks
   -storepass changeit
   ```

3. The CA certificate CertGenCA.der is used to sign all certificates generated by the utils.CertGen tool. It is located in the *IDM_BASE*`/products/app/wl_`

server10.3/server/lib directory. This CA certificate must be imported into the appTrustKeyStore using the keytool utility. The syntax is:

```
keytool -import -v -noprompt -trustcacerts -alias Alias_Name
-file CA_File_Location -keystore Keystore_Location -storepass Keystore_Password
```

For example:

```
keytool -import -v -noprompt -trustcacerts -alias clientCACert -file IDM_
BASE/products/app/wl_server10.3/server/lib/CertGenCA.der -keystore
appTrustKeyStoreIDMHOST1.jks -storepass Key_Passphrase
```

16.10.5.5.4 Configuring Node Manager to Use the Custom Keystores

To configure Node Manager to use the custom keystores, add the following lines to the end of the nodemanager.properties file located in the *IDM_CONFIG*/nodemanager/*hostname* directory, where *hostname* is the name of the host where nodemanager runs:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=Identity_Keystore
CustomIdentityKeyStorePassPhrase=Identity_Keystore_Password
CustomIdentityAlias=Identity_Keystore_Alias
CustomIdentityPrivateKeyPassPhrase=Private_Key_Used_When_Creating_Certificate
```

For example:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=IDM_
CONFIG/domains/IDMDomain/keystores/appIdentityKeyStore.jks
CustomIdentityKeyStorePassPhrase=Key_Passphrase
CustomIdentityAlias=appIdentityIDMHOST1
CustomIdentityPrivateKeyPassPhrase=Key_Passphrase
```

The passphrase entries in the nodemanager.properties file get encrypted when you start Node Manager as described in Chapter 10.9.1, "Starting and Stopping Components" For security reasons, minimize the time the entries in the nodemanager.properties file are left unencrypted. After you edit the file, start Node Manager as soon as possible so that the entries get encrypted.

16.10.5.5.5 Configuring Managed Oracle WebLogic Servers to Use the Custom Keystores

Follow these steps to configure the identity and trust keystores for *WLS_SERVER*:

1. Log in to Oracle WebLogic Server Administration Console at: http://ADMIN.mycompany.com/console
2. Click **Lock and Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Click the name of the server for which you want to configure the identity and trust keystores (*WLS_SERVER*). The settings page for the selected server is displayed.
6. Select **Configuration**, then **Keystores**.
7. In the Keystores field, select the **Custom Identity and Custom Trust** method for storing and managing private keys/digital certificate pairs and trusted CA certificates.
8. In the Identity section, define attributes for the identity keystore:
   - **Custom Identity Keystore:** The fully qualified path to the identity keystore:

IDM_CONFIG/domains/*IDMDomain*/keystores/appIdentityKeyStore.jks

- **Custom Identity Keystore Type:** Leave blank; it defaults to JKS.
- **Custom Identity Keystore Passphrase:** The password (*Keystore_Password*) you provided in Section 16.10.5.5.3, "Creating a Trust Keystore Using the Keytool Utility." This attribute is optional or required depending on the type of keystore. All keystores require the passphrase to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore, so whether you define this property depends on the requirements of the keystore.

9. In the Trust section, define properties for the trust keystore:
   - **Custom Trust Keystore:** The fully qualified path to the trust keystore:

     IDM_CONFIG/domains/*IDMDomain*/keystores/appTrustKeyStoreIDMHOST1.jks

   - **Custom Trust Keystore Type:** Leave blank; it defaults to JKS.
   - **Custom Trust Keystore Passphrase:** The password you provided as *New_Password* in Section 16.10.5.5.3, "Creating a Trust Keystore Using the Keytool Utility." This attribute is optional or required depending on the type of keystore. All keystores require the passphrase to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore, so whether you define this property depends on the requirements of the keystore.
10. Click **Save**.
11. Click **Activate Changes** in the Administration Console's Change Center to make the changes take effect.
12. Select **Configuration**, then **SSL**.
13. Click **Lock and Edit**.
14. In the **Private Key Alias** field, enter the alias you used for the host name the Managed Server listens on, for example:
    - For `wls_ods1`, use `appIdentityIDMHOST1`.
    - For `wls_ods2` use `appIdentityIDMHOST2`.
    - For `ADMINSERVER` use `appIdentityADMINVHN`.

    In the **Private Key Passphrase** and the **Confirm Private Key Passphrase** fields, enter the password for the keystore that you created in Section 16.10.5.5.2, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility."
15. Click **Save**.
16. Click **Activate Changes** in the Administration Console's Change Center to make the changes take effect.
17. Restart the server for which the changes have been applied, as described in Chapter 10.9.1, "Starting and Stopping Components".

16.10.5.5.6 Changing the Host Name Verification Setting for the Managed Servers

Once the previous steps have been performed, set host name verification for the affected Managed Servers to `Bea Hostname Verifier`. To do this, perform the following steps:

1. Log in to Oracle WebLogic Server Administration Console. (Console URLs are provided in Chapter 10.9.2, "About Oracle Identity Management Console URLs").

2. Select **Lock and Edit** from the change center.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Select the Managed Server in the Names column of the table. The settings page for the server is displayed.
6. Open the SSL tab.
7. Expand the **Advanced** section of the page.
8. Set host name verification to `Bea Hostname Verifier`.
9. Click **Save**.
10. Click **Activate Changes**.

16.10.5.6 Update boot.properties Files

Each managed server has a `boot.properties` file which is created as part of the process described in previous sections. In order to start managed servers using the provisioning start script, you must update each of these files and comment out following line:

```
TrustKeyStore=DemoTrust
```

When you have finished updating the file, the line should look like this:

```
#TrustKeyStore=DemoTrust
```

The files you must update are:

IDM_CONFIG/domains/IDMDomain/servers/AdminServer/security/boot.properties

and each Managed Server `boot.properties` file. These have path names of the form:

IDM_CONFIG/domains/IDMDomain/servers/*servername*/security/boot.properties

and

IDM_CONFIG/domains/IDMDomain/servers/AdminServer/data/nodemanager/boot.properties

16.10.5.7 Starting Node Manager

Run the following commands to start Node Manager.

```
cd IDM_CONFIG/nodemanager/hostname
./startNodeManagerWrapper.sh
```

Note: Verify that Node Manager is using the appropriate stores and alias from the Node Manager output. You should see the following when Node Manager starts.:

```
<Loading identity key store:
  FileName=IDM_
CONFIG/domains/IDMDomain/keystores/appIdentityKeyStore.jks,
Type=jks, PassPhraseUsed=true>
```

Host name verification works if you apply a test configuration change to the servers and it succeeds without Node Manager reporting any SSL errors.

16.11 Installing and Configuring Oracle Business Intelligence Applications

Oracle Business Intelligence Applications consists of pre-built metadata, dashboards, analyses, and ETL tools that provide insight into your organization's historical data. The Oracle Business Intelligence Applications software binaries are installed during Oracle Fusion Applications installation and provisioning in the Oracle Home for Business Intelligence. You must set up the Oracle Business Intelligence Applications components before using them. For details, refer to the *Oracle Business Intelligence Applications Installation Guide*.

16.12 Configuring Oracle Transactional Business Intelligence

After you install Oracle Fusion Transactional Business Intelligence, configure it to obtain real-time analysis of your organization's day-to-day operational data. For information on setting up accounting segment, modeling Essbase cubes, and setting up Descriptive Flexfields see the Oracle Fusion Transactional Business Intelligence Administrator's Guide.

16.13 Setting Up Report Delivery Servers

Oracle Business Intelligence Publisher is the report generation and delivery engine for Oracle Fusion Applications. Oracle BI Publisher receives report requests from Oracle Fusion Applications in the following ways:

- Through Oracle Enterprise Scheduler
- Through the Reports and Analytics pane
- From an application page

Requests submitted through Oracle Enterprise Scheduler are processed by the Oracle BI Publisher scheduler. Requests submitted through the Reports and Analytics pane can be either real-time online requests or scheduled requests. Requests submitted through an application may invoke Oracle Enterprise Scheduler or may return report request results directly back to the application page.

After installing Oracle Fusion Applications, Oracle BI Publisher is configured to accept requests from Oracle Fusion Applications. However, before you can deliver report documents to their destinations you must define the delivery servers in Oracle BI Publisher. Use the Oracle BI Publisher Administration page to define your delivery servers.

After setup, you can then further configure the number of report processor and delivery threads to best handle your processing and delivery requirements. In addition, you can configure report properties for the system or at the report level to tune performance of your reports. To diagnose report processing issues, BI Publisher provides a set of scheduler diagnostics.

16.13.1 Navigating to the Oracle BI Publisher Administration Page

Use the Oracle BI Publisher Administration page to:

- Configure delivery servers
- Manage report and delivery processors
- View scheduler diagnostics
- Set system properties and report runtime configuration properties

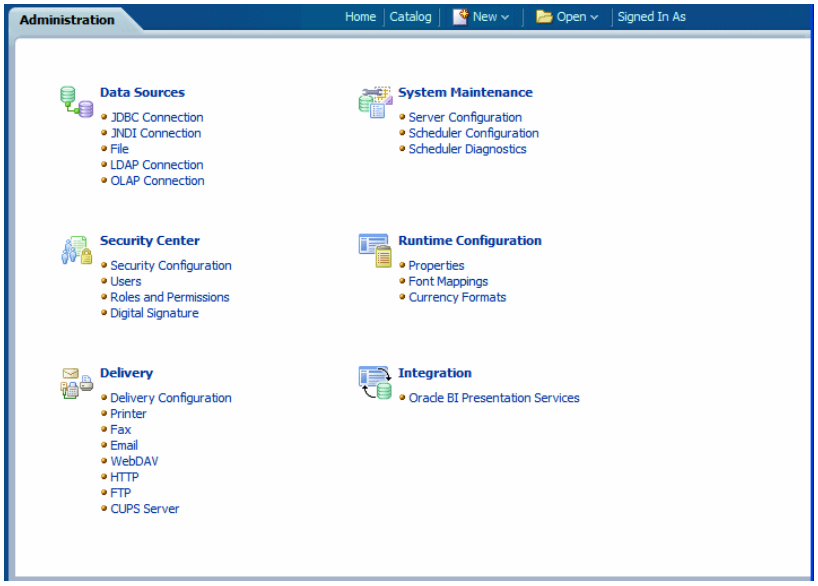
> **Note:** You must be assigned the `BIAdministrator` role to access the BI Publisher Administration page.

To navigate to the Oracle BI Publisher Administration page:

- From the Oracle Fusion Applications **Navigator**, under **Tools**, click **Reports and Analytics**. In the **Reports and Analytics** pane, click **Catalog** to display the Oracle Business Intelligence presentation catalog page. From here, click **Administration** and then click **Manage BI Publisher**.
- Alternatively, log in to Oracle Business Intelligence directly (example: `http://example.com:port/analytics`). Click **Administration** and then click **Manage BI Publisher**.

Figure 16–1 shows the BI Publisher Administration page:

Figure 16–1 BI Publisher Administration Page

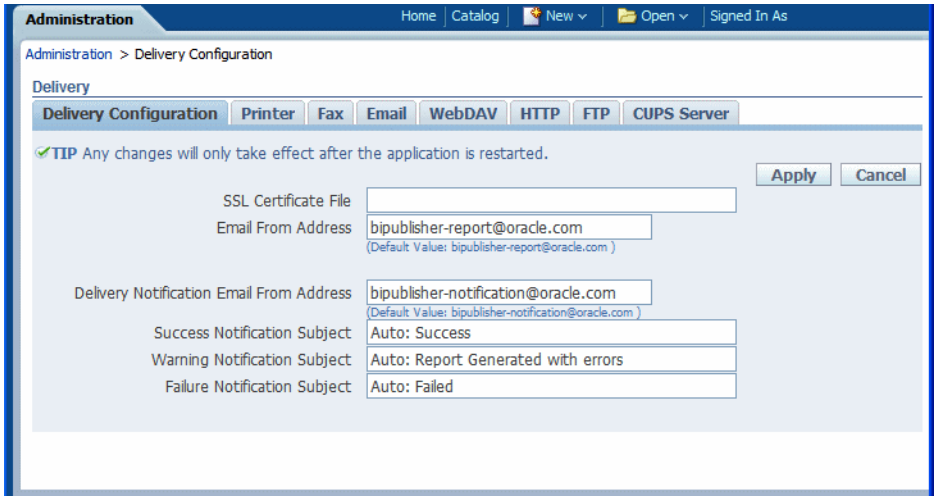


16.13.2 Configuring Report Delivery Servers

To configure delivery servers:

1. From the BI Publisher Administration page, click **Delivery Configuration**.
2. Enter values in the **Delivery Configuration Options** tab to set general properties for email deliveries and notifications. Figure 16–2 shows the Delivery Configuration Options tab:

Figure 16–2 Delivery Configuration Options Tab



For more information about this tab see "Configuring Delivery Options" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Business Intelligence Publisher*.

3. To configure a delivery server, click the appropriate tab.

The following table lists the report delivery channels supported by Oracle BI Publisher. See the corresponding section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Business Intelligence Publisher* for configuration information.

Delivery Type	Section
Printer and Fax	Adding a Printer or Fax Server
E-mail	Adding an E-mail Server
WebDAV	Adding a WebDAV Server
HTTP	Adding an HTTP Server
FTP	Adding an FTP Server

Note that printing is supported through Internet Printing Protocol (IPP). If Oracle BI Publisher is operating in a UNIX environment, you must set up the Common UNIX Printing Service (CUPS) and then define your CUPS server to Oracle BI Publisher. For a Windows environment, you must set up Windows Print Server for IPP. For information on setting up CUPS and Windows IPP, see "Setting Up Print Servers" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Business Intelligence Publisher*.

16.14 Setting Up Oracle ADF Desktop Integration

Oracle Application Development Framework (Oracle ADF) Desktop Integration is part of Oracle ADF and enables desktop integration with Microsoft Excel workbooks. Users can manage large volumes of data from web applications using Excel, for example to create journals, load currency rates, or create expense entries. To enable the integration of Oracle ADF with Microsoft Excel workbook, you need to make the Oracle ADF Desktop Integration add-in available on each client where Microsoft Excel is installed.

Note: This task is not applicable to Oracle Cloud implementations.

As Oracle ADF Desktop Integration is an add-in to Microsoft Office products, ensure that all the system requirements are fulfilled.

Note:

- Ensure that the version installed on the client is same as that installed on the server. For information on verifying whether your Oracle Fusion web application supports desktop integration or not, see the Oracle Fusion Middleware Desktop Integration Developer's Guide for Oracle Application Development Framework.
- The Oracle ADF Desktop Integration Client must be installed as the user and not as the administrator. However, Microsoft prerequisites for Oracle ADF Desktop Integration Client require administrator privileges. Therefore, you must provide administrator privileges to the user before you install the Oracle ADF Desktop Integration Client. Alternatively, you can install prerequisites as the administrator and Oracle ADF Desktop Integration Client as the regular user. For more information on prerequisites, see the Oracle Fusion Middleware Desktop Integration Developer's Guide for Oracle Application Development Framework.

To install the client version of the add-in, you must first deploy it at one of the following locations:

- Web server
- Shared network location

After these tasks are performed, you must inform users about the link they can use to download and install the client.

16.14.1 Deploying Oracle ADF Desktop Integration Client on a Web Server

You can deploy the Oracle ADF Desktop Integration Client on a web server that is accessible to the end users from their respective computers running on Microsoft Windows. Ensure that the web server is always up and running. Otherwise, the integration fails when end users access the desktop integrated workbook.

1. Create a folder in *APPLICATIONS_BASE*`/fusionapps/applications/desktop_installer`.

2. From the /u01/*APPLICATIONS_BASE*/fusionapps/oracle_common/modules/oracle.adf.desktopintegration_11.1.1 location, copy the adfdi-excel-runtime-client-installer.zip file and place it on the local computer.
3. Extract the contents of the zip file to a folder and ensure that setup.exe is present among the contents.
4. Using Windows Command Prompt, navigate to the folder path where you extracted the .zip file.
5. Modify the URL property of the setup.exe file to assign the final URL or full path to the installer, as shown here: setup.exe/url="https://<web server url>:<port number>/homePage/desktop_installer/<name of folder created in Step 1>/adfdi-excel-runtime-client-installer".

   Note: Replace the variables indicated within <> with actual values.

6. While remaining in the same folder location in Windows Command Prompt, verify the URL assigned to the setup.exe, as shown here:

   ```
   setup.exe/url
   ```

   A dialog box appears displaying the full path.
7. In Windows Explorer, .zip the same folder that contains the modified setup.exe and copy it to folder created in *APPLICATIONS_BASE*/fusionapps/applications/desktop_installer.
8. Extract the contents of the .zip file.
9. Bounce the Home Page of the managed server in Common Domain so that users can access the setup.exe directly using the following URL:https://<web server url>:<port number>/homePage/desktop_installer/<name of folder created in Step 1>/adfdi-excel-runtime-client-installer/setup.exe.
10. Uninstall any existing version of Oracle ADF Desktop Integration client from the end user computers.
11. Access the URL to install the Oracle ADF Desktop Integration client on the end user computers.

    Tip: After you place the Oracle ADF Desktop Integration Client on the web server, it is recommended that you use the Manage Menu Customizations task in the Setup and Maintenance work area of Oracle Fusion Applications to establish a link to the web server and install the client on the end user computer.

    a. Log in to Oracle Fusion Applications.
    b. From the menu bar, select **Administration** - **Setup and Maintenance**.
    c. Navigate to the task Manage Menu Customizations. The Manage Menu Customizations page appears.
    d. Select the Tools folder and on the menu select **Actions** - **Insert Item Child**. The Create Item Node dialog box appears.
    e. Enter a name in the Label field. For example, Download Oracle ADF Desktop Integration Runtime client.

f. In the Destination field, enter the URL of the `setup.exe` as shown here:

```
#{EndPointProvider.externalEndpointByModuleShortName['HomePage']}/d
esktop_installer/<new folder created under desktop_
installer>/adfdi-excel-runtime-client-installer/setup.exe
```

g. Click **Save**. The custom navigator link for Oracle ADF Desktop Installer appears under **Navigator - Tools** menu of Oracle Fusion Applications.

Users can use this link to download or directly run the `setup.exe` to install the Oracle ADF Desktop Integration Client on their computers.

For more information on customizing the navigator menu by using the Manage Menu Customizations task, see the *Oracle Fusion Applications Extensibility Guide*.

Note: Whenever a new version of the Oracle ADF Desktop Integration Client is available for upgrade, you need to consider the following to keep the client up-to-date:

- Repeat Steps b to g to overwrite the existing installer content in the `adfdi-excel-runtime-client-installer` folder.
- Whenever a new version of the Oracle ADF Desktop Integration Client is available at the web server location, it automatically checks for any updates to Microsoft Excel and prompts the end users to download and upgrade. To make this happen without any disruption, you need to ensure that the associated web server hosting the Oracle ADF Desktop Integration Client is always up and running.
- If there is a change in the web server location or the web server URL or the port number, end users will need to uninstall the ADF Desktop Integration Client and reinstall it as the links responsible for communicating automatic upgrades would have been broken.
- At Step g, users may encounter "The Publisher is not verified" warning message when running the downloaded `setup.exe` directly in Internet Explorer. The warning is prompted because the digital signature on the `setup.exe` file has been invalidated when you modify the URL property. This invalid signature warning does not prevent users from installing the client successfully. To avoid this warning, you need to sign the `setup.exe` file again with a valid certificate after modifying the URL property.

16.14.2 Deploying Oracle ADF Desktop Integration Client on a Shared Network Location

You can deploy the Oracle ADF Desktop Integration Client on a shared network location that is accessible to the end users from their respective computers running on Microsoft Windows.

1. Identify a shared network location where you plan to host the Oracle ADF Desktop Integration Client.
2. From the /u01/APPLICATIONS_BASE/fusionapps/oracle_common/modules/oracle.adf.desktopintegration_11.1.1 location, copy the adfdi-excel-runtime-client-installer.zip file and place it in a folder at the shared location.

3. Extract the contents of the zip file to the same folder.
4. Uninstall any existing version of Oracle ADF Desktop Integration client from the end user computers.
5. From the end user computer, access the shared folder and run the setup.exe to install the Oracle ADF Desktop Integration client on that computer.

IMPORTANT:

Whenever a new version of the Oracle ADF Desktop Integration Client is available for upgrade, you need to consider the following to keep the client up-to-date:

- Overwrite the existing installer content in the shared folder on the network.
- Whenever a new version of the Oracle ADF Desktop Integration Client is available at the shared location on the network, Microsoft Excel automatically checks for any updates and prompts the end users to upgrade. To make this happen without any disruption, you need to ensure that the network connectivity is always up.
- If there is a change in the shared location, end users will need to uninstall the Oracle ADF Desktop Integration Client and reinstall it from its new location as the links responsible for communicating automatic upgrades would have been broken.

16.15 Configuring Oracle Data Integrator Studio

Configuring Oracle Data Integrator Studio for external authentication is necessary to prevent any unauthorized access. The access credentials are stored in a configuration file. To make the external configuration work, the jps configuration file (jps-config.xml) must be configured and placed in the prescribed directory where the application is installed.

Prerequisites

- Select the Developer Installation options on the Select Installation Type page:
  - **ODI Studio (with local agent)**
  - **ODI SDK**
- Skip Repository Configuration on the Repository Configuration page

> **Note:** You must install Oracle Data Integrator Studio in a separate Oracle home other than Oracle Fusion Middleware Oracle homes and Oracle Fusion Applications Oracle home.

For more information about installing Oracle Data Integrator, see the *Oracle Fusion Middleware Installation Guide for Oracle Data Integrator*.

16.16 Setting Up the Oracle Business Intelligence Administration Tool

Oracle Business Intelligence Administration Tool is a part of the Oracle Business Intelligence Client Tools and is packaged along with the Oracle Business Intelligence Applications. It enables you to manage the metadata repository and is required for certain steps in the Oracle Business Intelligence Applications setup process. For more information about setting up the Oracle Business Intelligence Administration Tool, see "Installing and Uninstalling Oracle Business Intelligence Client Tools" in the *Oracle Business Intelligence Applications Installation Guide*

16.17 Performing Optional Language Installations

This section describes how to install a language other than US English, using Language Pack Installer. For more information about language packs, see "Installing and Upgrading Languages" in the *Oracle Fusion Applications Administrator's Guide*.

This section includes the following topics:

- Pre-Installation Steps - Before Down Time
- Pre-Installation Steps - During Down Time
- Install a Language
- Complete the Post-Installation Tasks

16.17.1 Pre-Installation Steps - Before Down Time

This section describes the preparation steps for installing a language pack, all of which can be performed before your scheduled down time.

16.17.1.1 Before You Begin

Before you begin the language pack installation, ensure you have access to the *Oracle Fusion Applications NLS Release Notes* from the current release.

You should also have a clear understanding of the following host and directories:

- **Primordial host**: The location of the Common domain (specifically the Administration Server of the Common domain). Only one primordial host exists in each environment.
- ***APPLICATIONS_CONFIG***: The top-level directory for the Oracle Fusion Applications configuration files.
- ***APPLICATIONS_BASE***: The top-level directory for the Oracle Fusion Applications binaries.
- ***FA_ORACLE_HOME***: Directory named `applications`, located under the `fusionapps` Oracle Fusion Applications Middleware home.

For more information, see Section 2.3.7.2, "Oracle Fusion Applications Oracle Home Directory."

16.17.1.2 Confirming the Oracle Fusion Applications Installation is Complete

Ensure that you performed all tasks described in Chapter 15, "Completing Mandatory Common Post-Installation Tasks."

16.17.1.3 Maintaining Versions of Customized BI Publisher Reports

If you are installing a language pack immediately after the Oracle Fusion Applications installation, you can skip this step.

If you are installing a language pack at a later stage, ensure that you have your own versions of any customized BI Publisher reports. If a language pack includes an update to a catalog object that was delivered with an Oracle Fusion application, the patch will overwrite any customizations applied to the original report. For more information, see "Before You Begin Customizing Reports" in the *Oracle Fusion Applications Extensibility Guide*.

16.17.1.4 Run Health Checker for Pre-Down Time Checks

You must run Health Checker directly from *APPLICATIONS_BASE* and from the primordial host. You can run these checks any number of times prior to your down time. For information about the checks that Health Checker runs, see "Language Pack Readiness Health Checks" in the *Oracle Fusion Applications Upgrade Guide*.

Perform the following steps to run Health Checker:

1. Set the APPLICATIONS_BASE and REPOSITORY_LOCATION environment variables. Set the APPLICATIONS_BASE environment variable to point to the directory that contains Oracle Fusion Applications. For example, if Oracle Fusion Applications is installed in /server01/APPLICATIONS_BASE/fusionapps, then set the APPLICATIONS_BASE environment variable to /server01/APPLICATIONS_BASE. Set the REPOSITORY_LOCATION environment variable to point to the root directory where the Language Pack repository is staged. You created this directory in Section 5.5.2.1, "Download Language Pack Software."

   For example:

   ```
   UNIX:
   setenv APPLICATIONS_BASE /server01/APPTOP/
   setenv REPOSITORY_LOCATION /server01/REL8Repo/

   Windows:
   SET APPLICATIONS_BASE=\server01\APPTOP\
   SET REPOSITORY_LOCATION=\server01\REL8Repo\
   ```

2. Run Health Checker. Note that this is one command.

   ```
   UNIX:
   $APPLICATIONS_BASE/fusionapps/applications/lcm/hc/bin/hcplug.sh -manifest
   $APPLICATIONS_
   BASE/fusionapps/applications/lcm/hc/config/LanguagePackReadinessHealthChecks.xm
   l [-DlogLevel=log_level]

   Windows:
   %APPLICATIONS_BASE%\fusionapps\applications\lcm\hc\bin\hcplug.cmd -manifest
   %APPLICATIONS_
   BASE%\fusionapps\applications\lcm\hc\config\LanguagePackReadinessHealthChecks.x
   ml [-DlogLevel=log_level]
   ```

Review the Health Checker log file or the HTML summary report to see if any errors occurred that require corrective action. The log file and the HTML summary are located in *APPLICATIONS_CONFIG*/lcm/logs/*release_version*/healthchecker.

After you resolve the issue that caused the error, start Health Checker again to run the failed tasks. You must rerun Health Checker until there are no more failed tasks.

16.17.2 Pre-Installation Steps - During Down Time

This section describes the mandatory preparation steps for installing a language pack, all of which must be performed during your system down time. Language Pack Installer does not require any servers to be shut down. However, no users should be online, so it is still considered to be down time.

16.17.2.1 Run Health Checker for General System Health Checks

You must run Health Checker directly from *APPLICATIONS_BASE* and from the primordial host. For information about the checks that Health Checker runs, see "General System Health Checks" in the *Oracle Fusion Applications Upgrade Guide*.

Perform the following steps to run Health Checker:

1. Set the APPLICATIONS_BASE and REPOSITORY_LOCATION environment variables. Set the APPLICATIONS_BASE environment variable to point to the directory that contains Oracle Fusion Applications. For example, if Oracle Fusion Applications is installed in /server01/APPLICATIONS_BASE/fusionapps, then set the environment variable APPLICATIONS_BASE to /server01/APPLICATIONS_BASE. Set the REPOSITORY_LOCATION environment variable to point to the root directory where the Language Pack repository is staged.

   For example:

```
UNIX:
setenv APPLICATIONS_BASE /server01/APPTOP/
setenv REPOSITORY_LOCATION /server01/REL8Repo/

Windows:
SET APPLICATIONS_BASE=\server01\APPTOP\
SET REPOSITORY_LOCATION=\server01\REL8Repo\
```

   Note: Set this environment variable on all hosts that share the same *APPLICATIONS_BASE* before executing all tools and utilities mentioned in this guide.

2. Run Health Checker. Note that this is one command.

```
UNIX:
$APPLICATIONS_BASE/fusionapps/applications/lcm/hc/bin/hcplug.sh -manifest
$APPLICATIONS_
BASE/fusionapps/applications/lcm/hc/config/GeneralSystemHealthChecks.xml
[-DlogLevel=log_level]

Windows:
%APPLICATIONS_BASE%\fusionapps\applications\lcm\hc\bin\hcplug.cmd -manifest
%APPLICATIONS_
BASE%\fusionapps\applications\lcm\hc\config\GeneralSystemHealthChecks.xml
[-DlogLevel=log_level]
```

Review the Health Checker log file or the HTML summary report to see if any errors occurred that require corrective action. The log file and the HTML summary are located in *APPLICATIONS_CONFIG*/lcm/logs/*release_version*/healthchecker.

After you resolve the issue that caused the error, start Health Checker again to run the failed tasks. You must rerun Health Checker until there are no more failed tasks.

16.17.2.2 Back Up Oracle Fusion Applications

Back up your entire Oracle Fusion Applications environment by following the steps in "Backing Up and Recovering Oracle Fusion Applications" in the *Oracle Fusion Applications Administrator's Guide*. You should also back up your central inventory.

For additional back up steps that are specific to Windows, refer to Section 16.17.2.2.1, "Back Up Steps for Windows Platforms".

16.17.2.2.1 Back Up Steps for Windows Platforms

Back up the Oracle Fusion Applications environment, including *APPLICATIONS_BASE*, inventory, registry entries, Oracle Identity Management, the database and the System environment PATH variable of the Oracle Fusion Applications host machine.

1. *APPLICATIONS_BASE* contains many files whose path is more than 256 characters. The Microsoft Windows Copy function is limited to copying only those files with a path of less than 256 characters. Therefore, many files fail to copy.

   Use Robust File Copy (Robocopy), which is available as part of the Windows Resource Kit, to copy *APPLICATIONS_BASE*. Use the following command:

   ```
   robocopy <source> <destination> /MIR > <file>
   ```

   Sample output from the `robocopy` command:

	Total	Copied	Skipped	Mismatch	FAILED	Extras
Dirs:	112640	112640	0	0	0	
Files:	787114	787114	0	0	0	
Bytes:	63.822 g	63.822 g	0	0	0	
Times:	2:22:20	2:19:00			0:00:00	0:03:19

2. Back up the inventory location referenced in the registry `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\inst_loc`.
3. Use `Regedit.exe` to back up the following registries related to Oracle Fusion Applications.
   - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
     - Web Tier service
     - BI Service
     - Node Manager service
   - HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE
   - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Oblix
4. Ensure that the System PATH has the following values:

   ```
   C:\<APPLICATIONS_BASE>\dbclient\bin
   C:\<APPLICATIONS_BASE>\webtier_mwhome\webtier\bin
   C:\<APPLICATIONS_BASE>\webtier_mwhome\webtier\\bin
   C:\<APPLICATIONS_BASE>\webtier_mwhome\webtier\opmn\lib
   C:\<APPLICATIONS_BASE>\webtier_mwhome\webtier\perl\bin
   C:\<APPLICATIONS_BASE>\fusionapps\bi\products\Essbase\EssbaseServer\bin
   C:\<APPLICATIONS_BASE>\fusionapps\bi\bin
   C:\<APPLICATIONS_BASE>\fusionapps\bi\opmn\bin
   C:\<APPLICATIONS_BASE>\fusionapps\bi\opmn\lib
   C:\<APPLICATIONS_BASE>\fusionapps\bi\perl\bin
   ```

   Add any of the previous values that are missing to the system PATH. Missing values cause failures in launching the OPMN services and BI Presentation Catalog deployment configuration assistants in Language Pack Installer.
5. Save the system PATH variable.

16.17.2.3 Apply Mandatory Prerequisite Patches

Apply any patches listed in the Post-Installation section of *Oracle Fusion Applications release notes* that you may have downloaded in Section 5.5.2.1, "Download Language Pack Software."

16.17.3 Install a Language

Language Pack Installer does not require any servers to be shut down. However, no users should be online, so it is still considered to be down time. Oracle recommends that language packs be installed from a machine that is co-located in the same subnetwork as the database server to maximize performance. You must run Language Pack Installer on the primordial host.

Ensure that the steps in Section 16.17.1, "Pre-Installation Steps - Before Down Time" and Section 16.17.2, "Pre-Installation Steps - During Down Time" are successfully completed before you start Language Pack Installer.

Language Pack Installer supports GUI mode and silent mode. In GUI mode, you navigate through screens that display the progress of the installation, including log file locations and status messages. In silent mode, Language Pack Installer reports the progress of the installation as console output.

- Run Language Pack Installer in GUI Mode
- Run Language Pack Installer in Silent Mode

> **Note:** If Language Pack Installer encounter errors, refer to "Troubleshoot Language Pack Installer Sessions" in the *Oracle Fusion Applications Administrator's Guide* before clicking any buttons in the Language Pack Installer user interface.

16.17.3.1 Run Language Pack Installer in GUI Mode

Perform the following steps to run Language Pack Installer in GUI mode from the command line, using specific options to further define the necessary actions. You must run Language Pack Installer from the primordial host.

1. Set the *JAVA_HOME* environment variable as follows:

   ```
   UNIX: setenv JAVA_HOME APPLICATIONS_BASE/fusionapps/jdk6

   Windows: set JAVA_HOME=APPLICATIONS_BASE\fusionapps\jdk6
   ```

2. Confirm registration of the network location of *FA_ORACLE_HOME*.

   If the Oracle Fusion Applications Oracle home directory (*FA_ORACLE_HOME*), which is *APPLICATIONS_BASE*/fusionapps/applications, is registered in the central inventory with a /net path, then provide the oraInst.loc location including /net when starting Language Pack Installer. An example follows:

   ```
   UNIX only:
   $REPOSITORY_LOCATION/installers/fusionapps/Disk1/runInstaller -jreLoc
   APPLICATIONS_BASE/fusionapps/jdk6/
   -invPtrLoc /net/APPLICATIONS_BASE/fusionapps/applications/oraInst.loc
   ```

   If not triggered with a /net path, Language Pack Installer copies the -invPtrLoc file to *FA_ORACLE_HOME*. This results in a copy of the file to itself, which then becomes an empty or zero byte file. As a result, the copy phase will fail when oracle_common patches are applied. For more information, see "Inventory Pointer File is Empty" in the *Oracle Fusion Applications Upgrade Guide*.

3. Run the following command to start Language Pack Installer in GUI mode.

   ```
   UNIX: $REPOSITORY_LOCATION/installers/fusionapps/Disk1/runInstaller -addLangs
   -jreLoc APPLICATIONS_BASE/fusionapps/jdk6
   [-invPtrLoc FA_ORACLE_HOME/oraInst.loc]
   ```

```
-noCheckForUpdates OR -updatesDir installer_patch_directory
[-DpatchStageLocation=directory_location_of_patch_stage
[-Dworkers=number_of_workers][-DlogLevel=level]
[-DserverStartTimeout=timeout_period_for_server_in_seconds]
[-DpatchDownloadLocation=patch_directory][-debug]
[-DupdateJAZNPolicyStore=true]

Windows: %REPOSITORY_LOCATION%\installers\fusionapps\Disk1\setup.exe -addLangs
-jreLoc APPLICATIONS_BASE\fusionapps\jdk6
-noCheckForUpdates OR -updatesDir installer_patch_directory
[-DpatchStageLocation=directory_location_of_patch_stage
[-Dworkers=number_of_workers][-DlogLevel=level]
[-DserverStartTimeout=timeout_period_for_server_in_seconds]
[-DpatchDownloadLocation=patch_directory][-debug]
[-DupdateJAZNPolicyStore=true]
```

The following table shows valid options that can be used when running Language Pack Installer.

Table 16–7 Language Pack Installer Command Line Options

Option Name	Description	Mandatory
`-addLangs`	Runs Language Pack Installer to install one language.	Yes.
`-jreLoc`	Path where the Java Runtime Environment is installed. This option does not support relative paths, so you must specify the absolute path.	Yes.
`-noCheckForUpdates`	Skips the application of the installer update patch, if there is no installer update patch available for this release.	No, this option cannot be used if the `-updatesDir` option is used. Either `-noCheckForUpdates` or `-updatesDir` must be used.
`-updatesDir`	The location of the installer update patch. When a valid installer patch is found, the installer automatically restarts itself after applying the patch.	No, this option cannot be used if the `-noCheckForUpdates` option is used. Either `-noCheckForUpdates` or `-updatesDir` must be used.
`-DpatchStageLocation`	Location of patch stage. This is the directory where Middleware patches from a downloaded location, as well as the repository, are consolidated before applying.	No, the default directory is *APPLICATIONS_BASE*`/../patch_stage`. For example, if *APPLICATIONS_BASE* is `/u01/APPLICATIONS_BASE`, the patch stage directory is `/u01/patch_stage`.
`-invPtrLoc` (UNIX platforms only)	The location of an overriding inventory pointer file. If the Oracle Fusion Applications Oracle home directory (*FA_ORACLE_HOME*), is registered in inventory with a `/net` path, then provide the location of `oraInst.loc` including `/net` in the path.	Recommended, use to override the default location of the inventory pointer file, located in `/etc/oraInst.loc`.

Table 16–7 (Cont.) Language Pack Installer Command Line Options

Option Name	Description	Mandatory
`-Dworkers`	The number of workers to use for uploading database content. If you provide a value for the number of workers that is outside the calculated range, you are prompted to provide a value that is within the optimal range. If you do not use this option, a calculated optimal value is used.	No, overrides the default number of workers calculated by Language Pack Installer.
`-DserverStartTimeout`	Configures the timeout value for server in seconds.	No, overrides the default value for server timeout.
`-DpatchDownloadLocation`	The directory path where you downloaded mandatory prerequisite patches to be applied by Language Pack Installer. See Section 5.5.2.1, "Download Language Pack Software".	No, the default is `11.1.8.0.0_post_repo_patches`.
`-DlogLevel`	Records messages in the log file at the level you specify. Enter a value to override the default log level of `INFO`.	No, the default value is `INFO`.
`-DupdateJAZNPolicyStore=true`	Updates the policy store with translated attributes so field descriptions, display names, and other attributes display their translated values.	No, use only when you do not want to use base English in the policy store.
`-debug`	Retrieve debug information from Language Pack Installer.	No.

Example 16–1 Language Pack Installation with no policy store translation

```
UNIX: $REPOSITORY_LOCATION/installers/fusionapps/Disk1/runInstaller -addLangs
-jreLoc APPLICATIONS_BASE/fusionapps/jdk6
-invPtrLoc FA_ORACLE_HOME/oraInst.loc
-noCheckForUpdates OR -updatesDir installer_patch_directory

Windows: %REPOSITORY_LOCATION%\installers\fusionapps\Disk1\setup.exe -addLangs
-jreLoc APPLICATIONS_BASE\fusionapps\jdk6

-noCheckForUpdates OR -updatesDir installer_patch_directory
```

Example 16–2 Language Pack Installation with policy store translation

```
UNIX: $REPOSITORY_LOCATION/installers/fusionapps/Disk1/runInstaller -addLangs
-jreLoc APPLICATIONS_BASE/fusionapps/jdk6
-invPtrLoc FA_ORACLE_HOME/oraInst.loc -DupdateJAZNPolicyStore=true
-noCheckForUpdates OR -updatesDir installer_patch_directory

Windows: %REPOSITORY_LOCATION%\installers\fusionapps\Disk1\setup.exe -addLangs
-jreLoc APPLICATIONS_BASE\fusionapps\jdk6 -DupdateJAZNPolicyStore=true
-noCheckForUpdates OR -updatesDir installer_patch_directory
```

Example 16–3 Language Pack installation when FA_ORACLE_HOME is registered with a /net path

```
UNIX: $REPOSITORY_LOCATION/installers/fusionapps/Disk1/runInstaller -addLangs
-jreLoc APPLICATIONS_BASE/fusionapps/jdk6
-invPtrLoc /net/APPLICATIONS_BASE/fusionapps/applications/oraInst.loc
-noCheckForUpdates OR -updatesDir installer_patch_directory
```

The following table illustrates the tasks that Language Pack Installer runs. For information about log files and troubleshooting Language Pack Installer errors, see "Troubleshoot Language Pack Installer Sessions" in the *Oracle Fusion Applications Administrator's Guide*.

Table 16–8 Language Pack Installer Screen Sequence

Screen	Description and Action Required
Welcome	Appears when you start Language Pack Installer. This screen does not appear if you restart Language Pack Installer after a failure. The standard Welcome screen is read-only. It contains a navigation pane on the left-hand side that summarizes the tasks the installer will take. Each item in the pane represents an installer screen, which contains prompts for the necessary information. Click **Next** to continue.
Install Software Updates	Appears when you start Language Pack Installer. This screen does not appear if you supplied the `-noCheckForUpdates` option, or after the installer restarts itself automatically after applying an installer patch. The screen displays two options: ■ Skip applying the installer update ■ Search Local Directory for Updates Select **Search Local Directory for Updates**. Specify the correct Installer update patch location or click **Browse** to locate the file. Then click **Search for Updates** to display the patch number and the type of patch. Click **Next** to continue.
Installation Location	Specify the location of the existing Oracle Fusion Applications home (*`FA_ORACLE_HOME`*) where you want to install the language. Click **Next** to continue.
Installation Summary	Summarizes the selections you made during this installation session. It includes the Oracle home, required and available disk space, and the language to be installed. Review the information displayed to ensure that the installation details are what you intend. To make changes before installing, click **Back** to return to previous screens in the interview. Click **Install** to start installing this language.
Installation Progress	Displays a progress indicator that shows the percentage of the installation phase that is complete and indicates the location of the installation log file. The installation phase consists of copying files from the language pack to the appropriate Oracle homes. When the installation progress indicator shows 100 percent, click **Next** to continue.

Table 16–8 (Cont.) Language Pack Installer Screen Sequence

Screen	Description and Action Required
Policy Store Analysis (Note that this screen displays only when the `-DupdateJAZNPolicyStore` option is set to `true` when you start Language Pack Installer.)	Analysis is available for the following policy store stripes: hcm, crm, fscm, soa, ucm, bpm, and obi. Select the stripes to be analyzed and then click **Run Analysis** to identify any conflicts or deletions. Only the stripes that are included in the language pack are enabled for analysis and the analysis could run for several minutes. After the analysis runs, review the results of the analysis to determine which deployment method you want Language Pack Installer to use for policy store changes to each stripe. Oracle recommends that you select **Apply safe changes only**. This is the safest method unless you have read and totally understood the consequences of the other three options. If you decide to resolve the conflicts or deletions before the actual JAZN upload from Language Pack Installer, you should run the Policy Store Analysis step again to get the most accurate analysis report. The choices for deployment method are: ■ Apply safe changes only (choose this method if there are no conflicts). ■ Apply all changes and overwrite customizations (not available for soa, ucm, and bpm stripes). ■ Append additive changes. ■ Manually resolve conflicts and upload changes using Authorization Policy Manager. If you choose **Apply safe changes only** or **Append additive changes**, then you must review the results of the analysis to manually upload any changes not applied by Language Pack Installer with the choice you selected, after the installation is complete. If you choose **Apply all changes and overwrite customizations**, then you may need to reapply the customizations that are overwritten after the installation is complete. If you choose one of these options, click **Next** after you make your selection. If you choose **Manually resolve conflicts and upload changes using Authorization Policy Manager** (APM), you must pause the installation while you bring up the APM application and upload the changes. For more information, see "Upgrading Oracle Fusion Applications Policies" in the *Oracle Fusion Applications Administrator's Guide*. Note the location of the following files: ■ Baseline file: *FA_ORACLE_HOME*/admin/JAZN/*stripe*/baseline ■ Patch file for fscm, crm, and hcm stripes: *FA_ORACLE_HOME*/*stripe*/deploy/system-jazn-data.xml ■ Patch file for obi, soa, ucm, and bpm stripes: *FA_ORACLE_HOME*/com/acr/security/jazn/bip_jazn-data.xml When you complete this task in APM, shut down the APM application, return to Language Pack Installer, and click **Next**.
Configuration Progress	Displays a progress indicator that shows the percentage of the configuration phase that is complete. It displays each configuration assistant in the message pane as it is performed. Configuration assistants that could be included in the configuration phase are described in "Language Pack Installer Configuration Assistants" in the *Oracle Fusion Applications Administrator's Guide*. No additional user action is required in the Configuration Progress screen unless a failure occurs. For more information, see "General Troubleshooting During the Configuration Phase in GUI Mode" in the *Oracle Fusion Applications Administrator's Guide*.

Table 16–8 (Cont.) Language Pack Installer Screen Sequence

Screen	Description and Action Required
Installation Complete	Summarizes the installation just completed. If you want to save this configuration to a response file, click **Save**. To complete a successful installation, click **Finish**. The **Finish** button is activated only if all mandatory configuration assistants completed successfully. If you want to rerun this session after you resolve failed configuration assistants, click **Cancel.**

4. Proceed to Section 16.17.4, "Complete the Post-Installation Tasks.".

16.17.3.2 Run Language Pack Installer in Silent Mode

Perform the following steps to start Language Pack Installer in silent mode from the command line, using specific options to further define the necessary actions. You must run Language Pack Installer from the primordial host.

1. Create a response file named `silent.rsp` to be used in silent mode. This file can be located in any directory that is accessible while launching Language Pack Installer. An example follows:

```
ORACLE_HOME=/u01/APPLICATIONS_BASE/fusionapps/applications
CRM_SELECTED_JAZN_MIGRATION_TYPE=PATCH_POLICY
FSCM_SELECTED_JAZN_MIGRATION_TYPE=PATCH_POLICY
HCM_SELECTED_JAZN_MIGRATION_TYPE=PATCH_POLICY
OBI_SELECTED_JAZN_MIGRATION_TYPE=PATCH_POLICY
UCM_SELECTED_JAZN_MIGRATION_TYPE=PATCH_POLICY
BPM_SELECTED_JAZN_MIGRATION_TYPE=PATCH_POLICY
SOA_SELECTED_JAZN_MIGRATION_TYPE=PATCH_POLICY
```

Note: The *stripe*_SELECTED_JAZN_MIGRATION_TYPE properties allow you to choose which deployment method Language Pack Installer will use for policy store changes to each stripe. The following choices are available:

- PATCH_POLICY: Apply safe changes only. This is the recommended method. Choose this method if there are no conflicts.
- MIGRATE_POLICY_OVERRIDE: Apply all changes and overwrite customizations.
- MIGRATE_POLICY_NO_OVERRIDE: Append additive changes.
- MIGRATE_POLICY_APM: Manually resolve conflicts and upload changes using Authorization Policy Manager (APM)

If you choose PATCH_POLICY or MIGRATE_POLICY_NO_OVERRIDE, then you must review the results of the analysis to manually upload any changes not applied by Language Pack Installer, based on the choice you selected, after the installation is complete. If you choose MIGRATE_POLICY_OVERRIDE, then you may need to reapply the customizations that are overwritten after the installation is complete.

If you choose MIGRATE_POLICY_APM, you must pause the installation while you bring up the APM application and upload the changes. For more information, see the "Upgrading Oracle Fusion Applications Policies" chapter in the *Oracle Fusion Applications Administrator's Guide*. Note the location of the following files:

- Baseline file: *FA_ORACLE_HOME*/admin/JAZN/*stripe*/baseline
- Patch file for fscm, crm, and hcm stripes: *FA_ORACLE_HOME*/*stripe*/deploy/system-jazn-data.xml
- Patch file for the obi, ucm, bpm, and soa stripes: *FA_ORACLE_HOME*/com/acr/security/jazn/bip_jazn-data.xml

2. Set the *JAVA_HOME* environment variable as follows:

```
UNIX: setenv JAVA_HOME APPLICATIONS_BASE/fusionapps/jdk6

Windows: set JAVA_HOME=APPLICATIONS_BASE\fusionapps\jdk6
```

3. Confirm the registration of the network location of *FA_ORACLE_HOME*.

   If the Oracle Fusion Applications Oracle home directory (*FA_ORACLE_HOME*), which is *APPLICATIONS_BASE*/fusionapps/applications, is registered in the central inventory with a /net path, then provide the oraInst.loc location including /net when starting Language Pack Installer. An example follows:

```
$REPOSITORY_LOCATION/installers/fusionapps/Disk1/runInstaller -addLangs -jreLoc
APPLICATIONS_BASE/fusionapps/jdk6/
-invPtrLoc /net/APPLICATIONS_BASE/fusionapps/applications/oraInst.loc -silent
-response location_of_response_file
```

   If not triggered with /net path, Language Pack Installer copies the -invPtrLoc file to *FA_ORACLE_HOME*. In the example, this results in a copy of the file to itself, which then becomes an empty or zero byte file. As a result, the copy phase will fail when oracle_common patches are applied. For more information, see "Inventory Pointer File is Empty" in the *Oracle Fusion Applications Upgrade Guide*.

4. Run the following command to start Language Pack Installer in silent mode:

> **Note:** If Language Pack Installer encounters errors in silent mode during the first installer, it terminates the session. You must resolve the issue that caused the failure and then restart Language Pack Installer, using the same command you used previously. Language Pack Installer then restarts from the first failed task. For more information, see "General Troubleshooting During the Configuration Phase in Silent Mode" in the *Oracle Fusion Applications Administrator's Guide*.

```
UNIX: $REPOSITORY_LOCATION/installers/fusionapps/Disk1/runInstaller -addLangs
-jreLoc
APPLICATIONS_BASE/fusionapps/jdk6 [-invPtrLoc FA_ORACLE_HOME/oraInst.loc]
-silent
-response location_of_silent.rsp_file
-noCheckForUpdates OR -updatesDir installer_patch_directory
[-DpatchStageLocation=directory_location_of_patch_stage
[-Dworkers=number_of_workers][-DlogLevel=level]
[-DserverStartTimeout=timeout_period_for_server_in_seconds]
[-DpatchDownloadLocation=patch_directory][-debug]

Windows:
%REPOSITORY_LOCATION%\installers\fusionapps\Disk1\setup.exe -addLangs -jreLoc
APPLICATIONS_BASE\fusionapps\jdk6 [-Dworkers=number_of_
workers][-DlogLevel=level] -silent
-response location_of_silent.rsp_file
-noCheckForUpdates OR -updatesDir installer_patch_directory
[-DpatchStageLocation=directory_location_of_patch_stage
[-DpatchDownloadLocation=patch_directory]
[-DserverStartTimeout=timeout_period_for_server_in_seconds]
[-debug]
```

The following table shows valid options that can be used when running Language Pack Installer in silent mode.

Table 16–9 Language Pack Installer Command Options in Silent Mode

Option Name	Description	Mandatory
`-addLangs`	Runs Language Pack Installer to install one language.	Yes.
`-jreLoc`	Path where the Java Runtime Environment is installed. This option does not support relative paths, so you must specify the absolute path.	Yes.
`-invPtrLoc` (UNIX platforms only)	The location of an overriding inventory pointer file. If the Oracle Fusion Applications Oracle home directory (*`FA_ORACLE_HOME`*) is registered in inventory with a `/net` path, then provide the location of `oraInst.loc` including `/net` in the path.	Recommended, use to override the default location of the inventory pointer file, located in `/etc/oraInst.loc`.
`-silent`	Run Language Pack Installer in silent mode.	Yes.
`-response`	The location of the response file, `silent.rsp`.	Yes.

Table 16–9 (Cont.) Language Pack Installer Command Options in Silent Mode

Option Name	Description	Mandatory
`-noCheckForUpdates`	Skips the application of the installer update patch, if there is no installer update patch available for this release.	No, this option cannot be used if the `-updatesDir` option is used. Either `-noCheckForUpdates` or `-updatesDir` must be used.
`-updatesDir`	The location of the installer update patch. When a valid installer patch is found, the installer automatically restarts itself after applying the patch.	No, this option cannot be used if the `-noCheckForUpdates` option is used. Either `-noCheckForUpdates` or `-updatesDir` must be used.
`-DpatchStageLocation`	Location of patch stage. This is the directory where Middleware patches from a downloaded location, as well as the repository, are consolidated before applying.	No, the default directory is *APPLICATIONS_BASE*`/../patch_stage`.. For example, if *APPLICATIONS_BASE* is `/u01/APPLICATIONS_BASE`, the patch stage directory is `/u01/patch_stage`.
`-DupdateJAZNPolicyStore=true`	Updates the policy store with translated attributes so field descriptions, display names, and other attributes display their translated values.	No, use only when you do not want to use base English in the policy store.
`-Dworkers`	The number of workers to use for uploading database content. If you provide a value for the number of workers that is outside the calculated range, you are prompted to provide a value that is within the optimal range. If you do not use this option, a calculated optimal value is used.	No, overrides the default number of workers calculated by Language Pack Installer.
`-DserverStartTimeout`	Configures the timeout value for server in seconds.	No, overrides the default value for server timeout.
`-DpatchDownloadLocation`	The directory path where you downloaded mandatory prerequisite patches to be applied by Language Pack Installer. See Section 5.5.2.1, "Download Language Pack Software".	No, the default is `11.1.8.0.0_post_repo_patches`.
`-DlogLevel`	Records messages in the log file at the level you specify. Enter a value to override the default log level of `INFO`.	No, default value is `INFO`.
`-debug`	Retrieve debug information from Language Pack Installer.	No.

5. Proceed to Section 16.17.4, "Complete the Post-Installation Tasks.".

16.17.4 Complete the Post-Installation Tasks

Perform the following required manual steps after Language Pack Installer completes successfully:

- Confirm Database Artifact Deployments Were Successful
- Review Log Files for Errors or Exceptions
- Run Health Checker for Post Installation Checks

- Bounce All Servers and Verify the Status of Deployed Applications
- Perform Steps in NLS Release Notes

16.17.4.1 Confirm Database Artifact Deployments Were Successful

Confirm that all database artifact deployments were successful by reviewing the Diagnostics report and log files. For more information, see "Diagnostics Report" in the *Oracle Fusion Applications Patching Guide*.

16.17.4.2 Review Log Files for Errors or Exceptions

Confirm there are no unresolved errors or exceptions in the log files. For information about resolving errors, see "Troubleshoot Language Pack Installer Sessions" in the *Oracle Fusion Applications Administrator's Guide*.

16.17.4.3 Run Health Checker for Post Installation Checks

Run Health Checker to perform post installation checks directly from *APPLICATIONS_BASE* and from the primordial host by performing the following steps. For information about the checks that Health Checker runs, see "Post-Upgrade Tasks Performed by Health Checker" in the *Oracle Fusion Applications Upgrade Guide*.

1. Set the `APPLICATIONS_BASE` and `REPOSITORY_LOCATION` environment variables. For more information, see Step 1 in Section 16.17.1.4, "Run Health Checker for Pre-Down Time Checks."
2. Run Health Checker.

```
UNIX:
$APPLICATIONS_BASE/fusionapps/applications/lcm/hc/bin/hcplug.sh -manifest
$APPLICATIONS_
BASE/fusionapps/applications/lcm/hc/config/PostLanguagePackHealthChecks.xml
[-DlogLevel=log_level]

Windows:
%APPLICATIONS_BASE%\fusionapps\applications\lcm\hc\bin\hcplug.cmd -manifest
%APPLICATIONS_
BASE%\fusionapps\applications\lcm\hc\config\PostLanguagePackHealthChecks.xml
[-DlogLevel=log_level]
```

Review the Health Checker log file or the HTML summary report to see if any errors occurred that require corrective action. The log file and the HTML summary are located in *APPLICATIONS_CONFIG*`/lcm/logs/`*release_version*`/healthchecker`.

After you resolve the issue that caused the error, start Health Checker again to run the failed tasks. You must rerun Health Checker until there are no more failed tasks. If the JAZN Conflicts check fails, refer to "Resolve JAZN Conflicts Found by Health Checker" in the *Oracle Fusion Applications Administrator's Guide*.

16.17.4.4 Bounce All Servers and Verify the Status of Deployed Applications

1. Bounce all servers using the `fastarstop` script "bounce" option. For more information, see "fastartstop Syntax" and "Starting Examples with fastartstop" in the *Oracle Fusion Applications Administrator's Guide*.

> **Note:** If you are installing more than one language in an environment, you need to bounce servers only once at the end of installing all languages in that environment, to minimize time spent bouncing servers.

2. Verify that all deployed applications are up and running. You can check this from Fusion Applications Control, or by reviewing the server side log files. For more information, see "Accessing Fusion Applications Control" in the *Oracle Fusion Applications Administrator's Guide* or "Log Directories for Language Pack Installer Activities" in the *Oracle Fusion Applications Administrator's Guide*.

16.17.4.5 Perform Steps in NLS Release Notes

Perform any steps listed in the Post-Installation Tasks section of *Oracle Fusion Applications NLS release notes*.

16.18 Setting Up Segregation of Duties

When a role assignment is requested through Oracle Identity Management, it needs to check with the Application Access Controls Governor to see if there are any segregation of duties (SOD) violations. If Application Access Controls Governor reports any SOD violations, depending on the violation or access issues, Oracle Identity Manager needs to send the request for an approval to specific roles, automatically approve the request, or reject the request.

16.18.1 Setting Up SOD

To set up SOD, complete the following procedures.

1. Ensure that the following configuration requirements are met:
   - Set up an Application Access Controls Governor server
   - Set up the Oracle Fusion connector
   - Define a data source
   - Update the Application Access Controls Governor server details in Identity Manager

   For more information on setting up these as part of the Oracle Application Access Controls Governor, see the *Oracle Governance, Risk and Compliance Installation Guide*.

   > **IMPORTANT:** Perform all the setup tasks only from the Identity Manager domain.

2. To manually switch from Oracle Identity Management to Lightweight Directory Access Protocol (LDAP) as the source of user roles for Service-Oriented Architecture (SOA) server deployed with Identity Manager, perform the following configuration steps.

   This step is applicable only to the environments set up with Oracle Identity Management and Oracle Access Management integration, and LDAP synchronization of users and roles enabled in Oracle Identity Manager.

   1. Log in to the Enterprise Manager Console as a Weblogic_Administrator user.

2. Access the Weblogic Domain in which Identity Manager is configured.
3. Open the **Security** - **Realms** page.
4. On the Providers tab of the **Security** - **Realms** page, open **OIDAuthenticator**.
5. In the provider specific parameters for `OIDAuthenticator`, update the Oracle Virtual Directory port with the Oracle Internet Directory port by changing the value of the port from Oracle Virtual Directory port to Oracle Internet Directory port.
6. On the Providers tab of the security realm settings page, create a new authentication provider with the name OIMSignatureAuthenticationProvider and the type OIMSignatureAuthenticationProvider.
7. Configure `OIMSignatureAuthenticationProvider` with the following parameters:

   `DBDriver: oracle.jdbc.OracleDrive`

   `DBUrl: jdbc:oracle:thin:@<db_hostname>:<db_port>:<db_sid>.`

   `For example, jdbc:oracle:thin:@localhost:5521:iam4.`

   `PKIKeystore Provider: sun.security.rsa.SunRsaSign`

   `Symmetric Key Keystore Provider: com.sun.crypto.provider.SunJCE`

   `DBUser: the Identity Manager database schema user name`

   `DBPassword: the Identity Manager database schema user password`

   Note: These parameters as same as in `OIMAuthenticationProvider`.

8. Delete the existing `OIMSignatureAuthenticator`.
9. Reorder authentication providers into the following sequence:

   OAMIDAsserter

   OIMSignatureAuthenticationProvider

   OIMAuthenticationProvider

   OIDAuthenticator

   DefaultAuthenticator

   DefaultIdentityAsserter

   IDMDomainAgent

10. Disable the **Weblogic** user profile in Identity Manager.

Note: You need to disable this user profile to avoid the authentication errors at Identity Manager Authenticator level, as Identity Manager Authenticator is now placed ahead of the Default Authenticator in authentication provider ordering. However, you cannot disable the user profile from Identity Manager Administration page. Instead, run the following SQL scripts on the OIM database.

```
update usr set usr_status='Disabled' where usr_
login='WEBLOGIC';

update usr set usr_disabled=1 where usr_login='WEBLOGIC';
```

11. Create the **Weblogic** user profile in LDAP and add it to the **Administrators** role. If the **Administrators** role does not exist in LDAP, create it first and then add the **Weblogic** user profile to it.

    You can create a user in LDAP by creating an LDAP Data Interchange Format (LDIF) file and using the **ldapadd** command.

12. In the jps-config.xml file, locate the element group `<jpsContext name="default">`.

13. Under `<jpsContext name="default">`, locate the identity store element `<serviceInstanceRef ref="idstore.oim"/>`, replace its value with `idstore.ldap` and save the file.

14. Restart all servers in the domain, including the Administration Server.

3. Administer role memberships using the Delegated Administration tasks in Oracle Identity Manager. To apply SOD checks on these administrative actions, configure the following Identity Manager system properties.

   - Set `XL.RM_REQUEST_ENABLED` to `TRUE`
   - Set `XL.RM_ROLE_ASSIGN_TEMPLATE` to `ASSIGN ROLES WITH CALLBACK POLICY`

   For more information about managing system properties of Identity Manager and its request-based role grants, see the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*.

16.18.2 Turning Off SOD Checks

To turn off the SOD checks, do the following.

1. Log in as an Administrator to the Enterprise Manager application for Oracle Identity Manager server.
2. Navigate to the system MBean browser for the Identity Manager server.
3. Locate `OAACGConfig MBean` option.
4. Set the property `SODEnabled` to `False` and save.
5. Log in to the Identity Manager's advanced console and set the system property `XL.RM_REQUEST_ENABLED` to `False`.
6. Restart the Identity Manager server.

Note: To turn on the SOD checks, set the properties `SODEnabled` and `XL.RM_REQUEST_ENABLED` to `True`.

16.18.3 Modifying the Segregation of Duties Routing Policies for Approving Role Provisioning: Procedures

When an access control necessitates an approval, the predefined routing rules determine the approver for a role provisioning request. These rules are defined in the `OAACGRoleAssignSODCheck` composite because of Approval Management Extensions (AMX) functionality such as Supervisory List.

The following rules are used to route the request to the suitable role.

- If the requested role assignment is of Chief Financial Officer, SOD remediation task is assigned to the IT Security Manager role.
- If SOD violation occurs because of a policy where the SOD control perspective is **Business Process** - **Information Technology Management** and the control priority is 1, SOD remediation task is assigned to the Application Administrator role.
- If SOD violation occurs for any other reason (Catch All rule), SOD remediation task is assigned to the Controller role.

If you need to modify these routing rules, you can do it in two ways:

- Using Oracle SOA Composer
- Using JDeveloper

16.18.4 Modifying Rules Using Oracle SOA Composer

Use the Oracle SOA Composer associated with the SOA server used by Oracle Identity Management, and change the `RemediationRules` ruleset associated with `OAACGRoleAssignSODCheck` composite. For instance, you may want to shift the task assignment in the Catch All rule from the Controller role to a different role.

1. Log in to the Oracle SOA Composer.
2. Click **Open** - **Open Task**.
3. Select **OAACGRoleAssignSODCheck** and click **Open**.
4. On the ApprovalTaskRules.rules tab, click **Edit**.
5. Expand Catch All and in the **THEN** statement, replace `GL_CONTROLLER_JOB` with the new role.
6. Save the changes.

For more information about using Oracle SOA Composer to add rules, see the *Oracle Fusion Middleware User's Guide for Oracle Business Rules*.

16.18.5 Modifying Rules Using JDeveloper

You can directly make the modifications to the configuration file available within `OAACGRoleAssignSODCheck.zip`.

> **Note:** To perform this task, you must have the administrative privileges or the role of an Administrator.

1. Go to *IDM_BASE/products/app/oim*`/server/workflows/composites/` and extract the contents of OAACGRoleAssignSODCheck.zip to a directory.
2. Open the application in JDeveloper. You can see the routing rules in the ruleset `RemeditationRules` of the `ApprovalTaskRules.rules` file, where the following

SOD related information is available for configuring the rules as part of the task payload element `oaacgResponse`.

- hasIssues: Acceptable values are:
  - TRUE: Authorization issues exist but can be remedied
  - FALSE: No authorization issues
  - REJECT: Authorization issues exist but cannot be remedied; request has to be rejected
- dimensions: List of dimensions and tags that are defined on the controls related to the authorization issues
- requestedRoles: List of roles that are requested as part of this request
- existingRoles: List of existing role memberships for the user
- authIssues: List of Oracle Governance, Risk and Compliance Controls Incident IDs and the following additional details. This information is subsequently required to notify the approval decision.
  - ctrlPriority: Priority of the Oracle Applications Access Control Governor control that resulted in the authorization issue
  - ctrlName: Name of the SOD policy
  - userName: User profile to which the authorization issue belongs
  - roleName: Role associated with the authorization issue
  - sodStatus: Approval status of the request indicating whether the request is approved by Governance, Risk and Compliance Controls, or approved with conditions, or rejected
  - issuePath: Information about the entity on which the SOD policy is defined

After the rule modifications, update the following values in the `OAACGRoleAssignSODCheck_cfgplan.xml` configuration plan file.

Value	Description
`@oimT3URL`	The OIM server t3 URL
`@oimServerHost`	The OIM server host name
`@oimServerPort`	The OIM server port number

Thereafter, deploy the modified composite with this updated configuration plan file.

16.18.6 Troubleshooting Segregation of Duties for Role Provisioning: Procedures

The following scenarios may require troubleshooting measures to ensure successful completion of segregation of duties (SOD) checks and approval of role provisioning requests.

16.18.7 Failure of Role Assignment Request

The role assignment request fails and the request gets the Request Failed status. To troubleshoot this, do the following:

1. Log in to the Oracle Identity Management domain in Enterprise Manager.
2. On the home page, under (Service Oriented Architecture), click **OAACGRoleAssignSODCheck** composite.
3. Under Recent Instances, click the latest instance and look for any error message or description of failure of request.
4. Check if the Application Access Controls Governor server information provided in Oracle Identity Manager is correct.
5. On the left pane, click IDM domain and from the context menu select System Mbean Browser.
6. Under Application Defined Mbeans, navigate to `oracle.iam` and select the OIM server and Application OIM.
7. Expand **XML Config - Config - XMLConfig.OAACGConfig** and select OAACGCOnfig.
8. Ensure that the attribute values used in Host, Port, DataSourceName, Service URL, and UserName are correct. To modify any incorrect information, on the Operations tab, click `updateOAACGConfigInformation` method, and provide the following parameters.

Parameter	Description
host	Application Access Controls Governor host name or IP address
port	Application Access Control Governor port
username	Admin username
password	Admin password
serviceURL	Application Access Control Governor service URL Note Ensure that there is a forward slash at the end of the URL. The URL must be in the format /grcc/services/GrccService/.
DatasourceName	Data source name of the Oracle Fusion connector that is configured in Application Access Control Governor

9. After saving the modifications, restart the Oracle Identity Management server.

16.18.8 Task Details Missing

If you do not find the task details of the assigned task, perform the following checks to troubleshoot.

1. Ensure that the taskflow is deployed on the SOA server.
   a. Log in to the Weblogic console.
   b. On the left side, under the menu, click Deployments.
   c. Ensure that TaskDetails application is deployed to SOA server and its state is Active.

2. Ensure that the predefined Admin user in Oracle Identity Management (OIM) is available in the Oracle Credential Store Framework (CSF), do the following:
   a. Log in to Oracle Identity Management domain in Enterprise Manager.
   b. On the left pane, click Identity Management domain and from the context menu, select **Security** - **Credentials**.
   c. Expand OIM and check for the key entry `sysadmin`.
   d. Select the entry and click Edit to view the details.
   e. Ensure that the user name is set to `xelsysadm`.

   Note: If these steps do not help, refer to the generic troubleshooting tips associated with Oracle Identity Manager.

For generic information about troubleshooting OIM, see the *Oracle Fusion Applications Administrator's Guide*.

16.18.9 Configuring Oracle Data Integrator Studio for External Authentication: Explained

Configuring Oracle Data Integrator Studio for external authentication is necessary to prevent any unauthorized access. The access credentials are stored in a configuration file. To make the external configuration work, the jps configuration file (jps-config.xml) must be configured and placed in the prescribed directory where the application is installed.

16.18.10 Prerequisites

To configure Oracle Data Integrator Studio, ensure that the following selections were made in the Oracle Data Integrator installation wizard:

- Developer Installation options on the Select Installation Type page:
  - **ODI Studio (with local agent)**
  - **ODI SDK**
- Skip Repository Configuration on the Repository Configuration page

  Note: You must install Oracle Data Integrator Studio in a separate Oracle home other than Oracle Fusion Middleware Oracle homes and Oracle Fusion Applications Oracle home.

For more information on installing Oracle Data Integrator, see the *Oracle Fusion Middleware Installation Guide for Oracle Data Integrator*.

16.18.11 Configuration for ESS

In the `<APPLICATIONS_BASE/fusionapps/odi>/oracledi/client/odi/bin` directory, access the file `odi.conf` and update the parameter `AddVMOption -Doracle.odi.studio.ess=true`. This enables ESS configuration properties to be visible in Topology.

16.19 Configuring Presence Servers

If you have an on-premise installation of Oracle Fusion Applications, you can optionally use Microsoft Office Communication Server (OCS) 2007 or Microsoft Live Communication Server (LCS) as the presence server. The setup involves creating external application connections, and instant messaging and presence connections, to OCS or LCS for each Oracle Fusion application.

Note: You also need to set up prerequisites for OCS or LCS.

This table lists the Java EE applications that you can configure with OCS or LCS.

Product Family or Product	Java EE Application Name
Oracle Fusion Application Customer Relationship Management	■ ContractManagementApp ■ CrmCommonApp ■ CrmPerformanceApp ■ CustomerApp ■ MarketingApp ■ OrderCaptureApp ■ SalesApp
Oracle Fusion Applications Human Capital Management	■ HcmBenefitsApp ■ HcmCompensationApp ■ HcmCoreApp ■ HcmCoreSetupApp ■ HcmPayrollApp ■ HcmTalentApp
Oracle Fusion Applications Projects	ProjectFinancialsApp
Oracle Fusion Application Toolkit	HomePageApp

For each application, you execute the following commands against the appropriate domain:

- `createExtAppConnection`
- `addExtAppField`
- `createIMPConnection`

IMPORTANT: Replace placeholder values enclosed within brackets (< >) with real values, for the appName, url, poolName, userDomain, and server fields.

- For the appName field, enter the Java EE application name, for example HcmBenefitsApp.
- The userDomain field is required only for the OCS connection and refers to the user domain associated with the OCS installation.
- For the server field, enter the managed server name on which the Java EE application is deployed. This field is optional if there is only one managed server for the application.

16.19.1 createExtAppConnection

Execute this command:

```
createExtAppConnection(appName='<JavaEEApp>', name='IMP_EXT_APP',
displayName='Presence Server Login Credentials')
```

The appName field is environment specific and requires you to enter a value.

16.19.2 addExtAppField

Execute this command:

```
addExtAppField(appName='<JavaEEApp>', name='IMP_EXT_APP',
fieldName='Account', fieldValue='', displayToUser=1)
```

The appName field is environment specific and requires you to enter a value.

16.19.3 createIMPConnection

If Oracle Fusion Applications is deployed in a high availability configuration, there may be multiple managed servers targeted for each Java EE application. You must run the createIMPConnection command for each application on each server, and specify the server in the server field.

If you are using the LCS adapter, then execute this command:

```
createIMPConnection(appName='<JavaEEApp>', name='presence', adapter='LCS',
url='<http://host:port/contextPath>', appId='IMP_EXT_APP',
poolName='<poolNameHere>', timeout=60, default=1,
server='<managedServerName>')
```

If you are using the OCS adapter, then execute this command:

```
createIMPConnection(appName='<JavaEEApp>', name='presence',
adapter='OCS2007', url='<http://host:port/contextPath>', appId='IMP_EXT_
APP', userDomain='<example.com>', poolName='<poolNameHere>', timeout=60,
default=1, server='<managedServerName>')
```

These fields are environment specific and require you to enter a value:

- appName
- adapter (**OCS2007** or **LCS**)
- url
- poolName

- default (**1** or **0**)

> **Note:** The connection will not be used unless this field is set to 1. If you use 0, then you essentially disable the connection.

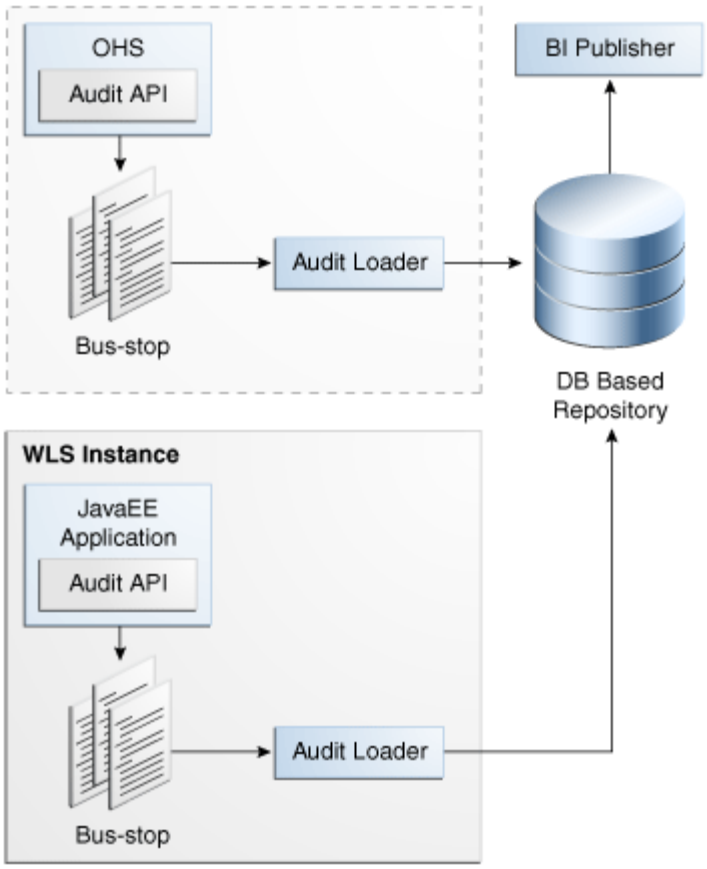
- server

16.20 Configuring Audit Trails for Oracle Fusion Middleware

The Oracle Fusion Middleware Audit Framework is a new service in Oracle Fusion Middleware 11*g*, designed to provide a centralized audit framework for the middleware family of products. The framework provides audit service for platform components such as Oracle Platform Security Services (OPSS) and Oracle Web Services. It also provides a framework for JavaEE applications, starting with Oracle's own JavaEE components. JavaEE applications will be able to create application-specific audit events. For non-JavaEE Oracle components in the middleware, such as C or JavaSE components, the audit framework also provides an end-to-end structure similar to that for JavaEE applications. For Oracle Fusion Applications, several Oracle Fusion Middleware products such as Oracle Data Integrator (ODI), Business Intelligence Publisher (BIP), Oracle Platform Security Services (OPSS), Oracle Web Service Management (OWSM), Oracle Business Intelligence Enterprise Edition (OBIEE), and Meta Data Services (MDS) leverage audit trails capability.

Figure 16–3 is a high-level architectural diagram of the Oracle Fusion Middleware Audit Framework.

Figure 16–3 Audit Event Flow



The Oracle Fusion Middleware Audit Framework consists of the following key components:

- **Audit APIs:** These are APIs provided by the audit framework for any audit-aware components integrating with the Oracle Fusion Middleware Audit Framework. During run time, applications may call these APIs, where appropriate, to audit the necessary information about a particular event happening in the application code. The interface allows applications to specify event details such as user name and other attributes needed to provide the context of the event being audited.
- **Audit Events and Configuration:** The Oracle Fusion Middleware Audit Framework provides a set of generic events for convenient mapping to application audit events. Some of these include common events such as authentication. The framework also allows applications to define application-specific events.

  These event definitions and configurations are implemented as part of the audit service in Oracle Platform Security Services. Configurations can be updated through Enterprise Manager (UI) and WebLogic Scripting Tool (WLST) command-line tool.
- **Audit Bus-stop:** Bus-stops are local files containing audit data before they are pushed to the audit repository. In the event where no database repository is configured, these bus-stop files can be used as a file-based audit repository. The bus-stop files are simple text files that can be queried easily to look up specific audit events. When a DB-based repository is in place, the bus-stop acts as an intermediary between the component and the audit repository. The local files are

periodically uploaded to the audit repository based on a configurable time interval.

- **Audit Loader:** As the name implies, the audit loader loads the files from the audit bus-stop into the audit repository. In the case of platform and JavaEE application audit, the audit loader is started as part of the JavaEE container start-up. In the case of system components, the audit loader is a periodically spawned process.
- **Audit Repository:** The audit repository contains a predefined Oracle Fusion Middleware Audit Framework schema, created by Repository Creation Utility (RCU). When configured, all the audit loaders are aware of the repository and upload data to it periodically. The audit data in the audit repository is expected to be cumulative and will grow over time. Ideally, this should not be an operational database used by any other applications; rather, it should be a standalone RDBMS used for audit purposes only. In a highly available configuration, Oracle recommends that you use an Oracle Real Application Clusters (RAC) database as the audit data store.
- **Oracle Business Intelligence Publisher:** The data in the audit repository is exposed through predefined reports in Oracle Business Intelligence Publisher. The reports allow users to drill down the audit data based on various criteria. For example:
  - User name
  - Time range
  - Application type
  - Execution context identifier (ECID)

The enterprise deployment topology does not include Oracle Fusion Middleware Audit Framework configuration. The ability to generate audit data to the bus-stop files and the configuration of the audit loader will be available after the products are installed. The main consideration is the audit database repository where the audit data is stored. Because of the volume and the historical nature of the audit data, it is strongly recommended that customers use a separate database from the operational store or stores being used for other middleware components.

16.21 Installing Print Servers

You must install print servers for external applications as part the implementation activity in Oracle Fusion Applications.

Note: This task is not applicable to Oracle Cloud implementations.

16.21.1 External Applications

Several external applications require specialized print servers. See the related product documentation for installing print servers for these applications.

- Oracle Business Intelligence Financial Reporting Studio and Financial Reporting Print Server.
- Primavera P6 Enterprise Project Portfolio Management.
- Informatica Identity Resolution. This product is associated with data quality as part of Oracle Fusion Trading Community Data Quality.

16.22 Configuring Oracle HTTP Server for Privileged Port (UNIX Only with No Load Balancer)

A secondary Oracle HTTP server needs to be added to the Oracle Fusion Applications environment to effectively handle the load and improve the application performance.

Before you proceed with the installation of the secondary HTTP server, you need to ensure that the following prerequisites are met.

- Availability of a free slot to install the secondary HTTP server.

  Note: Usually, the secondary HTTP server is installed on the same slot as the primary HTTP server. In such cases, the webgate used by the primary HTTP server can be used by the secondary HTTP server. However, if the secondary HTTP server is not installed on the same slot as the primary HTTP server, the webgate used by the primary HTTP server is not accessible by the secondary HTTP server. In that case, a separate webgate needs to be installed for the secondary HTTP server.

- Set up a directory structure similar to the directory structure of the primary HTTP server. The directory structure of the primary HTTP server is as follows.

```
First OHS mw home: /slot/ems5905/appmgr/APPLICATIONS_BASE/webtier_mwhome
First OHS OH: webtier
First OHS instance dir: /slot/ems5905/appmgr/APPLICATIONS_
BASE/instance/CommonDomain_webtier/
First OHS component name: ohs1
First OHS bin dir: /slot/ems5905/appmgr/APPLICATIONS_
BASE/instance/CommonDomain_webtier/bin
First OHS config dir: /slot/ems5905/appmgr/APPLICATIONS_
BASE/instance/CommonDomain_webtier/config/OHS/ohs1/moduleconf
```

  On the same lines, you can define a directory structure for the secondary HTTP server as shown here:

```
Second OHS mw home: /slot/ems5905/appmgr/APPLICATIONS_BASE/webtier_mwhome2
Second OHS OH: webtier2
Second OHS instance dir: /slot/ems5905/appmgr/APPLICATIONS_
BASE/instance/CommonDomain_webtier2
Second OHS component name: ohs2
```

16.23 What to Do Next

If you need information regarding scale out and server migration for Oracle Fusion Applications, go to Chapter 17. Otherwise, go to the chapter that corresponds to the product offering that is installed.

17

Completing Conditional Common High Availability Post-Installation Tasks for Oracle Identity Management

This chapter describes the conditional common high availability post-installation tasks for Oracle Identity Management that you should review and complete as required.

This chapter contains the following sections:

17.1 Introduction to Completing Conditional Common High Availability Post-Installation Tasks for Oracle Identity Management

After you have successfully completed the conditional common post-installation tasks review and perform the following conditional common high availability tasks.

Some components in the Oracle Fusion Applications environment are dependent on one another. Therefore, it is important to start and stop components in the proper order. In the course of normal IT operations, common operations include shutting down computers and starting them back up. Therefore, it is crucial to start and stop Oracle Fusion Applications in a sequential manner. For more information, see "Starting and Stopping the Entire Oracle Fusion Applications Environment" in the *Oracle Fusion Applications Administrator's Guide*.

17.2 Scaling Identity Management

The Identity Management topology is highly scalable. It can be scaled up and/or scaled out. This section explains how to do so.

To scale up the topology, you add a new component instance to a node already running one or more component instances. To scale out the topology, you add new component instances to new nodes.

17.2.1 Scaling Up the Topology

The Oracle Identity Management topology described in the guide has three tiers: the Directory Tier, Application Tier and Web Tier. The components in all the three tiers can be scaled up by adding a new server instance to a node that already has one or more server instances running.

The procedures described in this section show you how to create a new managed server or directory instance.

17.2.2 Scaling Out the Topology

You scale out a topology by adding new components to new nodes. The components in all three tiers of the Oracle Identity Management topology described in this guide can be scaled out by adding a new component instance to a new node.

17.2.3 Scaling Out the Database

The process of scaling out the Oracle Identity Management database involves installing new database instances, which is not described in this guide. The following steps assume that you have Real Application Clusters (RAC) and that the additional database instances have already been configured. For more information about RAC, see Section 7.4, "Installing Oracle Database or Oracle Real Application Clusters".

Oracle Identity Management components interface with the database using WebLogic Datasources. In systems that use Oracle RAC, Data sources are configured as Multi Datasources in Identity Management. A multi datasource is made up of several child datasources, one for each RAC database Instance. The Identity Management Applications interface with the RAC database by accessing the parent multi data source. If you add a new database instance, then you must create new datasources for each of the existing multi datasources and then add the new data source into the pre-existing multi data source. Because different applications use different datasources, you must add the database to each data source that is using the database.

To do this perform the following steps:

1. Log In to the WebLogic console using the URL:
   `http://admin.mycompany.com/console`
2. Select **Services > Messaging > Data Sources** from the Domain Structure window.
3. Click on a Data Source which has an ID of the type **Multi**
4. Click on the **Targets** tab and make a note of what targets the multi data source is assigned to.
5. Click on the **Configuration** tab and the **Data Sources** subtab. The chosen box shows you what Data sources are currently part of the multi datasource.
6. Select **Services > Messaging > Data Sources** from the Domain Structure window.
7. This time click on one of the data sources that are currently part of the multi datasource.
8. Make a note of the following attributes. (The example shown is the data source EDNDDatasource-rc0, which is part of the multi data source EDNDatasource.)

   General Tab

   JNDI Name: for example, `jdbc/EDNDatasource-rc0`

   Connection Pool Tab:

- **URL**: for example: `jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=idmdb-scan.mycompany.com)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=soa_edg.mycpmpany.com)(INSTANCE_NAME=idmdb1)))`
- **Driver Class**: for example: `oracle.jdbc.xa.client.OracleXADataSource`
- **Properties**: for example:

  `user=FA_SOAINFRA`

  `oracle.net.CONNECT_TIMEOUT=10000`
- **System Properties**: for example: `v$session.program=JDBCProgramName`
- **Password**: This is the database password you used when you ran the Oracle Identity Management RCU

9. Return to the Overview screen
10. Click **Lock and Edit**.
11. Click **New > Generic Datasource**
12. Select **Services - Messaging > Data Sources** from the Domain Structure window.
13. Provide the following:
    - **Name**: Choose a name for the datasource for example: `EDNDDatasource-rc3`
    - **JNDI Name**: Enter a jndi name, for example: **jdbc/EDNDatasource-rc3**
    - **Database Type**: `oracle`
14. Click **Next**.
    - **Database Driver**: This can be determined from the Driver class, that is, `xa` or `non xa`. For example: Oracle's Driver (thin XA) for RAC Service-Instance connections; Versions 10 and later
15. Click **Next**.
16. On the Transaction Options page, click **next**.
17. On the Connection Properties page enter:
    - **Service name**: Database service name for example: `soaedg.mycompany.com`
    - **Database Name**: Enter the name of the database for example: `IDMDB`
    - **Host Name**: If this is for an 11.2 database enter the database scan address. Otherwise enter the VIP of the host being added.
    - **Port**: Enter the listener port, for example: `1521`
    - **Database User Name**: enter the value from Properties, for example: `FA_SOAINFRA`
    - Enter the password assigned when the Oracle Fusion Middleware Repository Creation Utility (Oracle Fusion Middleware RCU) was run and confirm it.

    Click **Next**.
18. On the Test Configuration page, test the connection.

    Click Next
19. On the Targets page, assign the same targets as you noted for the mutli datasource.
20. Click **Finish**.

21. Now that the datasource has been defined, it can be added to the existing multi datasource.

    Select **Services > Messaging -> Data Sources** from the Domain Structure window.

22. Click on the multi datasource, for example: **EDNDDatasource**
23. Click on the **Targets** tab and add the newly created data source.
24. Click **Finish**
25. Click **Activate Changes**
26. Repeat for each data source that uses the database.

17.2.4 Scaling the Directory Tier

The Directory tier consists of two LDAP hosts, each running Oracle Internet Directory and Oracle Virtual Directory.

This section contains the following topics:

- Section 17.2.4.1, "Scaling Oracle Internet Directory"
- Section 17.2.4.2, "Scaling Oracle Virtual Directory"

17.2.4.1 Scaling Oracle Internet Directory

The Directory Tier has two Oracle Internet Directory nodes, *LDAP_PROVISIONED_HOST* and *LDAP_SCALED_OUT_HOST*, each running an Oracle Internet Directory instance.

When scaling up, use the existing Oracle Identity Management binaries on either node for creating the new Oracle Internet Directory instance.

To add a new Oracle Internet Directory instance to either Oracle Internet Directory node, or to scale out Oracle Internet Directory instances, perform the steps in the following subsections:

- Section 17.2.4.1.1, "Assembling Information for Scaling Oracle Internet Directory"
- Section 17.2.4.1.2, "Configuring an Additional Oracle Internet Directory Instance"
- Section 17.2.4.1.3, "Registering Oracle Internet Directory with the WebLogic Server Domain (IDMDomain)"
- Section 17.2.4.1.4, "Configuring Oracle Internet Directory to Accept Server Authentication Mode SSL Connections"
- Section 17.2.4.1.5, "Reconfiguring the Load Balancer."

17.2.4.1.1 Assembling Information for Scaling Oracle Internet Directory Assemble the following information before scaling Oracle Internet Directory.

Description	Variable	Documented Value	Customer Value
Host Name		*LDAP_SCALED_OUT_HOST*.mycompany.com	
OID Port	*OID_LDAP_PORT*		This value is available in the *Oracle Fusion Applications Installation Workbook* Network - Ports tab ->Identity Management Port Numbers -> OID.
OID SSL Port	*OID_LDAP_SSL_PORT*		This value is available in the *Oracle Fusion Applications Installation Workbook* Network - Ports tab ->Identity Management Port Numbers -> OID SSL.

Description	Variable	Documented Value	Customer Value
Oracle Instance Location	*OID_ORACLE_INSTANCE*		
Oracle Instance/component Name	oid*n*	oid3	
OID Admin Password			
Password to protect your SSL wallet/keystore	*COMMON_IDM_PASSWORD*		
Password for the CA wallet	*COMMON_IDM_PASSWORD*		
WebLogic Admin Host		ADMINVHN.mycompany.com	
WebLogic Admin Port	*WLS_ADMIN_PORT*	7001	
WebLogic Admin User		weblogic_idm	
WebLogic Admin Password			

17.2.4.1.2 Configuring an Additional Oracle Internet Directory Instance The schema database must be running before you perform this task. Follow these steps to install Oracle Internet Directory on the host:

1. Before starting the configuration, determine the ports you want to use for the new directory instance. For Scale out, these can be the same as the other instances you have. For Scale Up these ports must be unique to the new server instance.

   Ensure that ports you want are not in use by any service on the computer by issuing these commands for the operating system you are using.

   For example, on Linux, you would enter:

   ```
   netstat -an | grep "3060"
   netstat -an | grep "3131"
   ```

   If a port is not in use, no output is returned from the command. If the ports are in use (that is, if the command returns output identifying either port), you must free them.

   Remove the entries for the ports in the `/etc/services` file and restart the services, as described in Section 10.9.1, "Starting and Stopping Components," or restart the computer.

2. Create a file containing the ports used by Oracle Internet Directory. On Disk1 of the installation media, locate the file `stage/Response/staticports.ini`. Copy it to a file called `oid_ports.ini`. Delete all entries in `oid_ports.ini` except for `Non-SSL Port for Oracle Internet Directory` and `SSL Port for Oracle Internet Directory`. Change the values of those ports to the ports you want to use, for example: `3060` and `3131`.

   Note: If the port names in the file are slightly different from those listed in this step, use the names in the file.

3. Start the Oracle Identity Management 11*g* Configuration Wizard by running *OID_ORACLE_HOME*`/bin/config.sh`.

4. On the Welcome screen, click **Next**.

5. On the Select Domain screen, select **Configure without a Domain**.

   Click **Next**.

6. On the Specify Installation Location screen, specify the following values:

Oracle Instance Location: *OID_ORACLE_INSTANCE*

Oracle Instance Name: oid*n*, where *n* is a sequential number for the instance. For example, if you already have two instances configured, *n* will be 3, so you would enter oid3.

Click **Next**.

7. On the Specify Email for Security Updates screen, specify these values:
   - Email Address: Provide the email address for your My Oracle Support account.
   - Oracle Support Password: Provide the password for your My Oracle Support account.
   - Check the check box next to the **I wish to receive security updates via My Oracle Support** field.

   Click **Next**.
8. On the Configure Components screen, select Oracle Internet Directory, deselect all the other components, and click **Next**.
9. On the Configure Ports screen, you use the oid_ports.ini file you created in Step 2 to specify the ports to be used. This enables you to bypass automatic port configuration.
   a. Select **Specify Ports using a Configuration File**.
   b. In the file name field specify oid_ports.ini.
   c. Click **Save**, then click **Next**.
10. On the Specify Schema Database screen, select **Use Existing Schema** and specify the following values:
    - Connect String: This value is available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> OID Database (optional) -> OID DB Instances.

      If you are not using a separate OID database, then use the value available in the *Oracle Fusion Applications Installation Workbook* - Database tab -> IDM Database (optional) -> IDM DB Instances.

Notes:

- The Oracle RAC database connect string information must be provided in the format:

  host1:*port1*:*instance1*^*host2*:*port2*:*instance2*@*servicename*

- During this installation, it is not required that all the Oracle RAC instances to be up. If one Oracle RAC instance is up, the installation can proceed.
- You must provide complete and accurate information. Specifically, you must provide the correct host, port, and instance name for each Oracle RAC instance, and the service name you provide must be configured for all the specified Oracle RAC instances.

  Any incorrect information entered in the Oracle RAC database connect string must be corrected manually after the installation.

- User Name: `ODS`
- Password: *`password`*. This is the password of the ODS schema in the database as specified when Oracle Identity Management RCU was run.

Click **Next**.

11. The ODS Schema in use message appears. The ODS schema chosen is already being used by the existing Oracle Internet Directory instance. Therefore, the new Oracle Internet Directory instance being configured would reuse the same schema.

    Choose **Yes** to continue.

    A popup window with this message appears:

    ```
    "Please ensure that the system time on this Identity Management Node is
    in sync with the time on other Identity management Nodes that are part
    of the Oracle Application Server Cluster (Identity Management)
    configuration. Failure to ensure this may result in unwanted instance
    failovers, inconsistent operational attributes in directory entries and
    potential inconsistent behavior of password state policies."
    ```

    Ensure that the system time is synchronized among all the I*DM_PROVISIONED_HOST*s and *IDM_SCALED_OUT_HOST*s. See Section 5.3.1.13, "Synchronize Oracle Internet Directory Nodes" for more information.

    Click **OK** to continue.

12. On the Specify OID Admin Password screen, specify the Oracle Internet Directory administration password.

    > **Note:** If you see a message saying that OID is not running, verify that the orcladmin account has not become locked and try again. Do not continue until this message is no longer displayed.

    Click **Next**.

13. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not, click **Back** to modify selections on previous screens. When they are correct, click **Configure**.

14. On the Configuration screen, multiple configuration assistants are launched in succession. This process can be lengthy. Wait for the configuration process to finish.

15. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

16. To validate the installation of the Oracle Internet Directory instance on the new LDAP host, issue these commands:

    ```
    ldapbind -h LDAPHOST.mycompany.com -p 3060 -D "cn=orcladmin" -q
    ldapbind -h LDAPHOST.mycompany.com -p 3131-D "cn=orcladmin" -q -U 1
    ```

    where *LDAPHOST* is the host where the new instance is running.

Note: Ensure that the following environment variables are set before using `ldapbind`:

- *ORACLE_HOME*
- *ORACLE_INSTANCE*
- *PATH* - The following directory locations should be in your *PATH*:

  IDM_ORACLE_HOME/bin

  IDM_ORACLE_HOME/ldap/bin

  IDM_ORACLE_HOME/ldap/admin

17.2.4.1.3 Registering Oracle Internet Directory with the WebLogic Server Domain (IDMDomain)

All the Oracle Fusion Middleware components deployed in this enterprise deployment are managed by using Oracle Enterprise Manager Fusion Middleware Control. To manage the Oracle Internet Directory component with this tool, you must register the component and the Oracle Fusion Middleware instance that contains it with an Oracle WebLogic Server domain. A component can be registered either at install time or post-install. A previously un-registered component can be registered with a WebLogic domain by using the `opmnctl registerinstance` command.

To register the Oracle Internet Directory instances installed on the host where the new server instance is running, follow these steps for each instance:

1. On the new host:

   Set `ORACLE_HOME` to *IDM_ORACLE_HOME*.

   Set `ORACLE_INSTANCE` to *OID_ORACLE_INSTANCE*, where *OID_ORACLE_INSTANCE* is the location of the newly created instance.

2. Execute the `opmnctl registerinstance` command:

   ```
   OID_ORACLE_INSTANCE/bin/opmnctl registerinstance -adminHost WLSHostName
   -adminPort WLSPort -adminUsername adminUserName
   ```

   For example:

   ```
   OID_ORACLE_INSTANCE/bin/opmnctl registerinstance -adminHost
   ADMINVHN.mycompany.com -adminPort 7001 -adminUsername weblogic
   ```

   The command requires login to WebLogic Administration Server (`ADMINVHN.mycompany.com`)

   Username: `weblogic`

   Password: `*******`

   Note: For additional details on registering Oracle Internet Directory components with a WebLogic Server domain, see the "Registering an Oracle Instance or Component with the WebLogic Server" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

3. On the host where the new instance is running, update the Enterprise Manager Repository URL using the `emctl` utility with the `switchOMS` flag. This will enable the local emagent to communicate with the WebLogic Administration Server using

the virtual IP address. The `emctl` utility is located under the *`OID_ORACLE_INSTANCE`*`/EMAGENT/EMAGENT/bin` directory.

Syntax:

```
./emctl switchOMS ReposURL
```

For Example:

```
./emctl switchOMS http://ADMINVHN:7001/em/upload
```

Output:

```
./emctl switchOMS http://ADMINVHN.mycompany.com:7001/em/upload
Oracle Enterprise Manager 10g Release 5 Grid Control 10.2.0.5.0.
Copyright (c) 1996, 2009 Oracle Corporation.  All rights reserved.
SwitchOMS succeeded.
```

4. Force the agent to reload its configuration by issuing the command:

   ```
   ./emctl reload
   ```

5. Check that the agent is using the correct Upload URL using the command:

   ```
   ./emctl status agent
   ```

6. Validate that the agents on the host where the new server is running are configured properly to monitor their respective targets. Follow these steps to complete this task:

   - Use a web browser to access Oracle Enterprise Manager Fusion Middleware Control at:

     `http://ADMINVHN.mycompany.com:7001/em`

     Log in as the `weblogic_idm` user.

   - From the Domain Home Page navigate to the Agent-Monitored Targets page using the menu under **Farm** -> **Agent-Monitored Targets**.

   - Update the WebLogic monitoring user name and the WebLogic monitoring password.

     – Enter `weblogic_idm` as the WebLogic monitoring user name and the password for the `weblogic_idm` user as the WebLogic monitoring password.

     – Click **OK** to save your changes.

17.2.4.1.4 Configuring Oracle Internet Directory to Accept Server Authentication Mode SSL Connections

If you are using SSL Authentication Mode, you must perform the following to ensure that your Oracle Internet Directory instances are capable of accepting requests using this mode. You must configure each Oracle Internet Directory instance independently.

To enable Oracle Internet Directory to communicate using SSL Server Authentication Mode, perform the following steps on the host where the new server is running:

> **Note:** When you perform this operation, only the Oracle Internet Directory instance you are working on should be running.

1. Set the *`ORACLE_HOME`*, *`ORACLE_INSTANCE`* and *`JAVA_HOME`* variables. For example:

- Set ORACLE_HOME to *IDM_ORACLE_HOME*.
- Set ORACLE_INSTANCE to *OID_ORACLE_INSTANCE*.
- Set JAVA_HOME to *DIR_MW_HOME*/jdk6
- Set the PATH variable to include *JAVA_HOME*.

2. To enable SSL Server Authentication use the tool SSLServerConfig which is located in:

   ORACLE_COMMON_HOME/bin

   For example

   ```
   $ORACLE_COMMON_HOME/bin/SSLServerConfig.sh -component oid
   ```

3. When prompted, enter the following information:
   - LDAP Hostname: Central LDAP host, for example: POLICYSTORE.mycompany.com
   - LDAP port: *LDAP_POLICY_LBR_PORT*, for example: 389
   - Admin user DN: cn=orcladmin
   - Password: *orcladmin_password*
   - sslDomain for the CA: IDMDomain Oracle recommends that the SSLDomain name be the same as the Weblogic domain name to make reference easier.
   - Password to protect your SSL wallet/keystore: *COMMON_IDM_PASSWORD*
   - Enter confirmed password for your SSL wallet/keystore: *COMMON_IDM_PASSWORD*
   - Password for the CA wallet: *certificate_password*. This is the master password you used when you ran provisioning.
   - Country Name 2 letter code: Two letter country code, such as US
   - State or Province Name: State or province, for example: California
   - Locality Name: Enter the name of your city, for example: RedwoodCity
   - Organization Name: Company name, for example: mycompany
   - Organizational Unit Name: Leave at the default
   - Common Name: Name of this host, for example: LDAP_SCALED_OUT_HOST.mycompany.com
   - OID component name: Name of your Oracle Instance, for example: oid1. If you need to determine what your OID component name is, execute the command:

     OID_ORACLE_INSTANCE/bin/opmnctl status

   - WebLogic admin host: Host running the WebLogic Administration Server, for example:. ADMINVHN.mycompany.com
   - WebLogic admin port: *WLS_ADMIN_PORT*, for example: 7001
   - WebLogic admin user: Name of your WebLogic administration user, for example: weblogic
   - WebLogic password: *password*.

- AS instance name: Name of the new instance you entered in Step 6 of Section 17.2.4.1.2, "Configuring an Additional Oracle Internet Directory Instance," for example: `oid3`.
- SSL wallet name for OID component [oid_wallet1]: Accept the default
- Do you want to restart your OID component: `Yes`
- Do you want to test your SSL setup? `Yes`
- SSL Port of your OID Server: *`OID_LDAP_SSL_PORT`*, for example: `3131`

Sample output:

```
Server SSL Automation Script: Release 11.1.1.4.0 - Production
Copyright (c) 2010 Oracle. All rights reserved.

Downloading the CA wallet from the central LDAP location...
>>>Enter the LDAP Hostname [SLC00DRA.mycompany.com]: POLICYSTORE.mycompany.com
>>>Enter the LDAP port [3060]: 3060
>>>Enter an admin user DN [cn=orcladmin]
>>>Enter password for cn=orcladmin:
>>>Enter the sslDomain for the CA [idm]: IDMDomain
>>>Enter a password to protect your SSL wallet/keystore:
>>>Enter confirmed password for your SSL wallet/keystore:
>>>Enter password for the CA wallet:
>>>Searching the LDAP for the CA usercertificate ...
Importing the CA certifcate into trust stores...
>>>Searching the LDAP for the CA userpkcs12 ...

Invoking OID SSL Server Configuration Script...
Enter attribute values for your certificate DN
>>>Country Name 2 letter code [US]:
>>>State or Province Name [California]:
>>>Locality Name(eg, city) []:Redwood
>>>Organization Name (eg, company) [mycompany]:
>>>Organizational Unit Name (eg, section) [oid-20110524015634]:
>>>Common Name (eg, hostName.domainName.com) [SLC00XXX.mycompany.com]:
The subject DN is
cn=SLC00DRA.mycompany.com,ou=oid-20110524015634,l=Redwood,st=California,c=US

Creating an Oracle SSL Wallet for oid instance...
/u01/oracle/products/access/idm/../oracle_common/bin
>>>Enter your OID component name: [oid1]
>>>Enter the weblogic admin server host [SLC00XXX.mycompany.com] ADMINVHN
>>>Enter the weblogic admin port: [7001]
>>>Enter the weblogic admin user: [weblogic]
>>>Enter weblogic password:
>>>Enter your AS instance name:[asinst_1] oid1
>>>Enter an SSL wallet name for OID component [oid_wallet1]
Checking the existence of oid_wallet1 in the OID server...
Configuring the newly generated Oracle Wallet with your OID component...
Do you want to restart your OID component?[y/n]y

Do you want to test your SSL set up?[y/n]y
>>>Please enter your OID ssl port:[3131] 3131
Please enter the OID hostname:[SLC00DRA.mycompany.com] LDAP_SCALED_OUT_
HOST.mycompany.com
>>>Invoking IDM_ORACLE_HOM/bin/ldapbind -h LDAP_SCALED_OUT_HOST.mycompany.com -p
3131-U 2 -D cn=orcladmin ...
Bind successful
```

```
Your oid1 SSL server has been set up successfully
```

Confirm that the script has been successful.Repeat all the steps in this section, Section 17.2.4.1.4, "Configuring Oracle Internet Directory to Accept Server Authentication Mode SSL Connections." for each Oracle Internet Directory instance.

17.2.4.1.5 Reconfiguring the Load Balancer If you are accessing your Oracle Internet Directory instances through a load balancer, add the new Oracle Internet Directory instance to the existing server pool defined on the load balancer for distributing requests across the Oracle Internet Directory instances.

17.2.4.2 Scaling Oracle Virtual Directory

The Directory Tier has two nodes, *LDAP_PROVISIONED_HOST* and *LDAP_SCALED_OUT_HOST*, each running an Oracle Virtual Directory instance.

When scaling up, you can use existing Oracle Identity Management binaries on either node for creating the new Oracle Virtual Directory instance.

To add a new Oracle Virtual Directory instance to either Oracle Virtual Directory node, or to scale out Oracle Virtual Directory instances, perform the steps in the following subsections:

- Section 17.2.4.2.1, "Assembling Information for Scaling Oracle Virtual Directory"
- Section 17.2.4.1.2, "Configuring an Additional Oracle Internet Directory Instance"
- Section 17.2.4.2.3, "Post-Configuration Steps"
- Section 17.2.4.2.4, "Creating ODSM Connections to Oracle Virtual Directory"
- Section 17.2.4.2.5, "Creating Adapters in Oracle Virtual Directory"
- Section 17.2.4.2.6, "Reconfiguring the Load Balancer"

17.2.4.2.1 Assembling Information for Scaling Oracle Virtual Directory Assemble the following information before scaling Oracle Virtual Directory.

Description	Variable	Documented Value	Customer Value
Host Name		LDAP_SCALED_OUT_HOST.mycompany.com	
OVD Listen Port	*OVD_PORT*		This value is available in the *Oracle Fusion Applications Installation Workbook* Network - Ports tab ->Identity Management Port Numbers -> OVD.
OVD SSL Port	*OVD_SSL_PORT*		This value is available in the *Oracle Fusion Applications Installation Workbook* Network - Ports tab ->Identity Management Port Numbers -> OVD SSL.
Oracle Virtual Directory Proxy Port	*OVD_ADMIN_PORT*		This value is available in the *Oracle Fusion Applications Installation Workbook* Network - Ports tab ->Identity Management Port Numbers -> OVD Admin.
Oracle Instance Location	*OVD_ORACLE_INSTANCE*	/u02/local/oracle/config/instances/oid*n*	
OVD Existing Instance/Component Name	ovd*n*	ovd1	
Newly Created Instance/Component Name	ovd*n*	ovd3	
OVD Administrator Password			

Description	Variable	Documented Value	Customer Value
WebLogic Admin Host	*WLSHostName*	ADMINVHN.mycompany.com	
WebLogic Admin Port	*WLS_PORT*	7001	
WebLogic Admin User	*adminUserName*	weblogic_idm	
WebLogicAdmin Password			
Back end Identity Store host	*OID_LBR_HOST*	OIDIDSTORE.mycompany.com	
Back end Identity Store port	*OID_LDAP_PORT*		This value is available in the *Oracle Fusion Applications Installation Workbook* Network - Ports tab ->Identity Management Port Numbers -> OID.
Identity Store LDAP admin password			
Password to protect your SSL wallet/keystore	*COMMON_IDM_PASSWORD*		
Password for the CA wallet (created when you ran the Oracle Identity Management Provisioning Wizard)	*COMMON_IDM_PASSWORD*		

17.2.4.2.2 Configuring an Additional Oracle Virtual Directory Follow these steps to configure the new Oracle Virtual Directory instance:

1. Ensure that ports you are using (*OVD_PORT* and *OVD_SSL_PORT*) are not in use by any service on the computer by issuing these commands for the operating system you are using.

   On Linux:

   ```
   netstat -an | grep "6501"
   netstat -an | grep "7501"
   ```

   If a port is not in use, no output is returned from the command. If the ports are in use (that is, if the command returns output identifying either port), you must free the port.

   On Linux:

   Remove the entries for ports used by Oracle Virtual Directory in the `/etc/services` file and restart the services, as described in Section 10.9.1, "Starting and Stopping Components," or restart the computer.

2. Create a file containing the ports used by Oracle Virtual Directory. On Disk1 of the installation media, locate the file stage`/Response/staticports.ini`. Copy it to a file called `ovd_ports.ini`. Delete all entries in ovd_ports.ini except for Non-SSL Port for Oracle Virtual Directory and SSL Port for Oracle Virtual Directory. Change the values of those ports to the ports you want to use, for example: 3060 and 3131.

   Note: If the port names in the file are slightly different from those listed in this step, use the names in the file.

3. Start the Oracle Identity Management 11*g* Configuration Wizard by running *OID_ORACLE_HOME*`/bin/config.sh`.
4. On the Welcome screen, click **Next**.
5. On the Select Domain screen, select **Configure without a Domain**.
6. Click **Next**.

7. On the Specify Installation Location screen, specify the following values:

   Oracle Instance Location: *OVD_ORACLE_INSTANCE*

   Oracle Instance Name: ovd*n*, where *n* is a sequential number for the instance. For example, if you already have two instances configured, *n* will be 3, so you would enter ovd3.

8. Click **Next**.

9. On the Specify Email for Security Updates screen, specify these values:

   - **Email Address**: Provide the email address for your My Oracle Support account.
   - **Oracle Support Password**: Provide the password for your My Oracle Support account.
   - Check the checkbox next to the **I wish to receive security updates via My Oracle Support** field.

   Click **Next**.

10. On the Configure Components screen, select Oracle Virtual Directory, deselect all the other components, and click **Next**.

    a. On the Configure Ports screen, you use the ovd_ports.ini file you created in Step 2 to specify the ports to be used. This enables you to bypass automatic port configuration.

    a. Select **Specify Ports using a Configuration File**.

    b. In the file name field specify ovd_ports.ini.

    c. Click **Save**, then click **Next**.

11. On the Specify Virtual Directory screen: In the Client Listeners section, enter:

    - LDAP v3 Name Space: *REALM_DN*, for example: dc=mycompany,dc=com

    In the OVD Administrator section, enter:

    - Administrator User Name: cn=orcladmin
    - Password: *administrator_password*
    - Confirm Password: *administrator_password*

    Select **Configure the Administrative Server in secure mode**.

    Click **Next**.

12. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not, click **Back** to modify selections on previous screens. When they are correct, click **Configure**.

13. On the Configuration screen, multiple configuration assistants are launched in succession. This process can be lengthy. Wait for the configuration process to finish.

    Click **Next**.

14. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

    To validate the installation of the Oracle Virtual Directory instance on the host, issue these commands:

```
ldapbind -h LDAPHOST.mycompany.com -p 6501 -D "cn=orcladmin" -q
ldapbind -h LDAPHOST.mycompany.com -p 7501 -D "cn=orcladmin" -q -U 1
```

where *LDAPHOST* is the host where the new instance is running.

Note: Ensure that the following environment variables are set before using `ldapbind`:

- Set *ORACLE_HOME* to *OID_ORACLE_HOME*.
- Set *ORACLE_INSTANCE* to *OVD_ORACLE_INSTANCE*.
- *PATH* - The following directory locations should be in your *PATH*:

  OID_ORACLE_HOME/bin

  OID_ORACLE_HOME/ldap/bin

  OID_ORACLE_HOME/ldap/admin

17.2.4.2.3 Post-Configuration Steps

This section describes the post-configuration steps.

Registering Oracle Virtual Directory with the Oracle WebLogic Server Domain (IDMDomain)

All the Oracle Fusion Middleware components deployed in this enterprise deployment are managed by using Oracle Enterprise Manager Fusion Middleware Control. To manage the Oracle Virtual Directory component with this tool, you must register the component and the Oracle Fusion Middleware instance that contains it with an Oracle WebLogic Server domain. A component can be registered either at install time or post-install. A previously un-registered component can be registered with a WebLogic domain by using the `opmnctl registerinstance` command.

To register the Oracle Virtual Directory instances, follow these steps on the host where the new instance is running:

1. Set the *ORACLE_HOME* to *OID_ORACLE_HOME*.
2. Set *ORACLE_INSTANCE* to *OVD_ORACLE_INSTANCE1*, where *OVD_ORACLE_INSTANCE1* is the location of the newly-created instance.
3. Execute the `opmnctl registerinstance` command:

   OVD_ORACLE_INSTANCE/bin/opmnctl registerinstance -adminHost *WLSHostName* -adminPort *WLSPort* -adminUsername *adminUserName*

   For example:

   ```
   OVD_ORACLE_INSTANCE/bin/opmnctl registerinstance \
      -adminHost ADMINVHN.mycompany.com -adminPort 7001 -adminUsername weblogic
   ```

   The command requires login to WebLogic Administration Server.

   Username: `weblogic`

   Password: *password*

Note: For additional details on registering Oracle Virtual Directory components with a WebLogic Server domain, see the "Registering an Oracle Instance Using OPMNCTL" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

---

4. In order to manage Oracle Virtual Directory by using Oracle Enterprise Manager Fusion Middleware Control, you must update the Enterprise Manager Repository URL to point to the virtual IP address associated with the WebLogic Administration Server. Do this using the `emctl` utility with the `switchOMS` flag. This will enable the local emagent to communicate with the WebLogic Administration Server using the virtual IP address. The `emctl` utility is located under the *`OVD_ORACLE_INSTANCE`*`/EMAGENT/EMAGENT/bin` directory.

   Syntax:

   ```
   ./emctl switchOMS ReposURL
   ```

   For Example:

   ```
   ./emctl switchOMS http://ADMINVHN:7001/em/upload
   ```

   Output:

   ```
   ./emctl switchOMS http://ADMINVHN.mycompany.com:7001/em/upload
   Oracle Enterprise Manager 10g Release 5 Grid Control 10.2.0.5.0.
   Copyright (c) 1996, 2009 Oracle Corporation.  All rights reserved.
   SwitchOMS succeeded.
   ```

5. Force the agent to reload its configuration by issuing the command:

   ```
   ./emctl reload
   ```

6. Check that the agent is using the correct Upload URL using the command:

   ```
   ./emctl status agent
   ```

7. Validate if the agents on the host where the new instance is running are configured properly to monitor their respective targets. Follow these steps to complete this task:

   a. Use a web browser to access Oracle Enterprise Manager Fusion Middleware Control at `http://ADMINVHN.mycompany.com:7001/em`. Log in as the `weblogic_idm` user.

   b. From the Domain Home Page navigate to the Agent-Monitored Targets page using the menu under **Farm** -> **Agent-Monitored Targets**

   c. Update the WebLogic monitoring user name and the WebLogic monitoring password.

      – Enter `weblogic_idm` as the WebLogic monitoring user name and the password for the weblogic user as the WebLogic monitoring password.

      – Click **OK** to save your changes.

Configuring Oracle Virtual Directory for SSL

Before configuring Oracle Virtual Directory for SSL, set the *`ORACLE_HOME`*, *`ORACLE_INSTANCE`* and *`JAVA_HOME`* variables. For example, on the new *`LDAPHOST`*, set `ORACLE_HOME` to *`OID_ORACLE_HOME`*, set `ORACLE_INSTANCE` to *`OVD_ORACLE_INSTANCE`*, set `JAVA_HOME` to *`JAVA_HOME`*, and add *`JAVA_HOME`* to your *`PATH`* variable.

Start the SSL Configuration Tool by issuing the command `SSLServerConfig` command which is located in the directory *`ORACLE_COMMON_HOME`*`/bin` directory.

For example:
`ORACLE_COMMON_HOME``/bin/SSLServerConfig.sh -component ovd`

When prompted, enter the following information:

- LDAP Hostname: Central LDAP host, for example: `POLICYSTORE.mycompany.com`

  Note: It is recommended that you use the Policy Store directory, not the Identity Store.

- LDAP port: LDAP port, for example: `3060` (*`OID_LDAP_PORT`*)
- Admin user DN: `cn=orcladmin`
- Password: *`administrator_password`*
- sslDomain for the CA: `IDMDomain`
- Password to protect your SSL wallet/keystore: *`password_for_local_keystore`*
- Enter confirmed password for your SSL wallet/keystore: *`password_for_local_keystore`*
- Password for the CA wallet: certificate_password. This is the master password you crated when you ran provisioning.Fixed as in OID Section
- Country Name 2 letter code: Two letter country code, such as `US`
- State or Province Name: State or province, for example: `California`
- Locality Name: Enter the name of your city, for example: `RedwoodCity`
- Organization Name: Company name, for example: `mycompany`
- Organizational Unit Name: Leave at the default
- Common Name: Name of this host, for example: `LDAP_SCALED_OUT_HOST.mycompany.com`
- OVD Instance Name: for example, `ovd1`. If you need to determine what your OVD component name is, execute the command:

  `OVD_ORACLE_INSTANCE``/bin/opmnctl status`

- Oracle instance name: Name of your newly created Oracle instance, for example: ovd3Fixed as in OID Section
- WebLogic admin host: Host running the WebLogic Administration Server, for example:. `ADMINVHN.mycompany.com`
- WebLogic admin port: WebLogic Administration Server port, for example: `7001` (*`WLS_ADMIN_PORT`*)
- WebLogic admin user: Name of your WebLogic administration user, for example: `weblogic`
- WebLogic password: *`password`*.

SSL wallet name for OVD component [`ovdks1.jks`]: Accept the default

When asked if you want to restart your Oracle Virtual Directory component, enter `Yes`.

When asked if you would like to test your OVD SSL connection, enter `Yes`. Ensure that the test is a success.

17.2.4.2.4 Creating ODSM Connections to Oracle Virtual Directory Before you can manage Oracle Virtual Directory you must create connections from ODSM to each of your Oracle Virtual Directory instances. To do this, proceed as follows:

Access ODSM through the load balancer at: `http://ADMIN.mycompany.com/odsm`

8. Follow these steps to create connections to Oracle Virtual Directory:

   To create connections to Oracle Virtual Directory, follow these steps. Create connections to each Oracle Virtual Directory node separately. Using the Oracle Virtual Directory load balancer virtual host from ODSM is not supported:

   a. Create a direct connection to Oracle Virtual Directory on the new host providing the following information in ODSM:

      `Host`: *`LDAPHOST`*`.mycompany.com`

      `Port`: `8899` (The Oracle Virtual Directory proxy port, *`OVD_ADMIN_PORT`*)

      Enable the SSL option.

      `User`: `cn=orcladmin`

      `Password`: password_to_connect_to_OVD

   b. Create a direct connection to Oracle Virtual Directory on the host where your new instance is running, providing the following information in ODSM:

      `Host`: *`LDAPHOST`*`.mycompany.com`

      `Port`: `8899` (The Oracle Virtual Directory proxy port)

      Enable the SSL option.

      `User`: `cn=orcladmin`

      `Password`: password_to_connect_to_OVD

17.2.4.2.5 Creating Adapters in Oracle Virtual Directory Oracle Virtual Directory communicates with other directories through adapters.

The procedure is slightly different, depending on the directory you are connecting to. The following sections show how to create and validate adapters for supported directories:

Creating Oracle Virtual Directory Adapters for Oracle Internet Directory and Active Directory

You can use `idmConfigTool` to create the Oracle Virtual Directory User and Changelog adapters for Oracle Internet Directory and Active Directory. Oracle Identity Manager requires adapters. It is highly recommended, though not mandatory, that you use Oracle Virtual Directory to connect to Oracle Internet Directory.

To do this, perform the following tasks on *`IDM_PROVISIONED_HOST`*:

1. Set the environment variable *`ORACLE_HOME`* to *`IAM_ORACLE_HOME`*.
2. Create a properties file for the adapter you are configuring called `ovd1.props`. The contents of this file depends on whether you are configuring the Oracle Internet Directory adapter or the Active Directory Adapter.

   - **Oracle Internet Directory** adapter properties file:

     ```
     ovd.host:LDAPHOST.mycompany.com
     ovd.port:8899
     ovd.binddn:cn=orcladmin
     ovd.password:ovdpassword
     ovd.oamenabled:true
     ovd.ssl:true
     ldap1.type:OID
     ldap1.host:OIDIDSTORE.mycompany.com
     ldap1.port:3060
     ldap1.binddn:cn=oimLDAP,cn=systemids,dc=mycompany,dc=com
     ```

```
ldap1.password:oidpassword
ldap1.ssl:false
ldap1.base:dc=mycompany,dc=com
ldap1.ovd.base:dc=mycompany,dc=com
usecase.type: single
```

- **Active Directory** adapter properties file:

```
ovd.host:LDAPHOST.mycompany.com
ovd.port:8899
ovd.binddn:cn=orcladmin
ovd.password:ovdpassword
ovd.oamenabled:true
ovd.ssl:true
ldap1.type:AD
ldap1.host:ADIDSTORE.mycompany.com
ldap1.port:636
ldap1.binddn:cn=adminuser
ldap1.password:adpassword
ldap1.ssl:true
ldap1.base:dc=mycompany,dc=com
ldap1.ovd.base:dc=mycompany,dc=com
usecase.type: single
```

The following list describes the parameters used in the properties file.

- `ovd.host` is the host name of a server running Oracle Virtual Directory.
- `ovd.port` is the https port used to access Oracle Virtual Directory (*`OVD_ADMIN_PORT`*).
- `ovd.binddn` is the user DN you use to connect to Oracle Virtual Directory.
- `ovd.password` is the password for the DN you use to connect to Oracle Virtual Directory.
- `ovd.oamenabled` is always `true` in Oracle Fusion Applications deployments.
- `ovd.ssl` is set to `true`, as you are using an https port.
- `ldap1.type` is set to OID for the Oracle Internet Directory back end directory or set to AD for the Active Directory back end directory.
- `ldap1.host` is the host on which back end directory is located. Use the load balancer name.
- `ldap1.port` is the port used to communicate with the back end directory (*`OID_LDAP_PORT`* or *`OID_LDAP_SSL_PORT`*.
- `ldap1.binddn` is the bind DN of the `oimLDAP` user.
- `ldap1.password` is the password of the `oimLDAP` user
- `ldap1.ssl` is set to `true` if you are using the back end's SSL connection, and otherwise set to `false`. This should always be set to `true` when an adapter is being created for AD.
- `ldap1.base` is the base location in the directory tree.
- `ldap1.ovd.base` is the mapped location in Oracle Virtual Directory.
- `usecase.type` is set to `Single` when using a single directory type.

3. Configure the adapter by using the `idmConfigTool` command, which is located at:

   `IAM_ORACLE_HOME``/idmtools/bin`

Note: When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:

IAM_ORACLE_HOME`/idmtools/bin`

The syntax of the command is:

```
idmConfigTool.sh -configOVD input_file=configfile [log_file=logfile]
```

For example:

```
idmConfigTool.sh -configOVD input_file=ovd1.props
```

The command requires no input. The output looks like this:

```
The tool has completed its operation. Details have been logged to logfile
```

Run this command for the newly created Oracle Virtual Directory instance in your topology, with the appropriate value for `ovd.host` in the property file.

Validating the Oracle Virtual Directory Adapters

Perform the following tasks by using ODSM:

1. Access ODSM through the load balancer at: `http://ADMIN.mycompany.com/odsm`
2. Connect to Oracle Virtual Directory.
3. Go the **Data Browser** tab.
4. Expand **Client View** so that you can see each of your user adapter root DN's listed.
5. Expand the user adapter root DN, if there are objects already in the back end LDAP server, you should see those objects here.
6. ODSM doesn't support changelog query, so you cannot expand the `cn=changelog` subtree.

   Perform the following tasks by using the command-line:

   - Validate the user adapters by typing:

     ```
     ldapsearch -h directory_host -p ldap_port -D "cn=orcladmin" -q  -b user_
     search_base -s sub "objectclass=inetorgperson" dn
     ```

     For example:

     ```
     ldapsearch -h LDAPHOST.mycompany.com -p 6501 -D "cn=orcladmin" -q -b
     "cn=Users,dc=mycompany,dc=com" -s sub "objectclass=inetorgperson" dn
     ```

     Supply the password when prompted.

     You should see the user entries that already exist in the back end LDAP server.

   - Validate changelog adapters by typing:

     ```
     ldapsearch -h directory_host -p ldap_port -D "cn=orcladmin" -q  -b
     "cn=changelog" -s one "changenumber>=0"
     ```

     For example:

```
ldapsearch -h LDAPHOST -p 6501 -D "cn=orcladmin" -q -b "cn=changelog" -s
one "changenumber>=0"
```

The command returns logs of data, such as creation of all the users. It returns without error if the changelog adapters are valid.

- Validate `lastchangenumber` query by typing:

```
ldapsearch -h directory_host -p ldap_port -D "cn=orcladmin" -q -b
"cn=changelog" -s base 'objectclass=*' lastchangenumber
```

For example:

```
ldapsearch -h LDAP_SCALED_OUT_HOST -p 6501 -D "cn=orcladmin" -q -b
"cn=changelog" -s base 'objectclass=*' lastchangenumber
```

The command returns the latest change number generated in the back end LDAP server.

17.2.4.2.6 Reconfiguring the Load Balancer If you are accessing your Oracle Virtual Directory instances through a load balancer, add the new Oracle Virtual Directory instance to the existing server pool defined on the load balancer for distributing requests across the Oracle Virtual Directory instances.

17.2.5 Scaling the Application Tier

The Application Tier can be scaled out to multiple nodes. The following sections describe the details for scaling the Application Tier.

17.2.5.1 Mounting Middleware Home and Creating a New Machine when Scaling Out

When scaling out a component of the Application Tier, perform these steps first:

1. On the new node, mount the existing Middleware home, which should include the Oracle Fusion Middleware installation and the domain directory, and ensure that the new node has access to this directory, just like the rest of the nodes in the domain.
2. To attach *IAM_HOME* in shared storage to the local Oracle Inventory, execute the following command:

```
cd IAM_ORACLE_HOME/oui/bin
./attachHome.sh -jreLoc JAVA_HOME
```

3. To update the Middleware home list, create (or edit, if another WebLogic installation exists in the node) the *IAM_MW_HOME*`/bea/beahomelist` file and add *IAM_MW_HOME*`/oui/bin` to it.
4. Log in to the WebLogic Administration Console at: `http://ADMIN.mycompany.com/console`
5. Create a new machine for the new node to be used, and add the machine to the domain, as follows.
   a. Select **Environment -> Machines** from the Navigation menu.
   b. Click **Lock and Edit**.
   c. Click **New** on the Machine Summary screen.
   d. Enter the following information:

Name: Name of the machine. This is usually the host name.

Machine OS: Select UNIX.

e. Click **Next**.

f. On the Node Manager Properties page, enter the following information:

Type: SSL.

Listen Address: Use the host name.

g. Click **Finish**.

h. Click **Activate Changes**.

17.2.5.2 Creating a New Node Manager when Scaling Out

Node Manager is used to start and stop WebLogic managed servers on the new host. In order to create a new node manager for the new host perform the following steps:

1. Create a new directory for the new node manager by copying an existing one. Copy the directory *SHARED_CONFIG_DIR*/nodemanager/*IDM_PROVISIONED_HOST*.mycompany.com to: *SHARED_CONFIG_DIR*/nodemanager/*newidmhost*.mycompany.com

   For example:

   ```
   cp -r $SHARED_CONFIG_DIR/nodemanager/IDM_PROVISIONED_HOST.mycompany.com
   $SHARED_CONFIG_DIR/nodemanager/newidmhost.mycompany.com
   ```

2. Change to the newly created directory.

   ```
   cd SHARED_CONFIG_DIR/nodemanager/newidmhost.mycompany.com
   ```

3. Edit the nodemanager.properties file, changing all the entries for *IDM_PROVISIONED_HOST* to *newidmhost*. For example:

   ```
   DomainsFile=/u01/oracle//config/nodemanager/IDM_PROVISIONED_
   HOST.mycompany.com/nodemanager.domain
   ```

   becomes

   ```
   DomainsFile=/u01/oracle//config/nodemanager/newidmhost.mycompany.com/nodemanage
   r.domain
   ```

4. Edit the startNodeManagerWrapper.sh file, changing all the entries for *IDM_PROVISIONED_HOST* to *IDM_SCALED_OUT_HOST*. For example:

   ```
   NM_HOME=/u01/oracle/config/nodemanager/IDM_PROVISIONED_HOST.mycompany.com
   ```

   becomes

   ```
   NM_HOME=/u01/oracle/config/nodemanager/IDM_SCALED_OUT_HOST.mycompany.com
   ```

5. Start the node manager by invoking the command:

   ```
   ./startNodeManagerWrapper.sh
   ```

17.2.5.3 Scaling ODSM

To scale up ODSM, use the existing installations (WebLogic Server home, Oracle Fusion Middleware home, and domain directories) for creating a new Managed Server for the Oracle Directory Services Manager component.

To scale out, use the existing installations in shared storage for creating the new Managed Servers. You do not need to install WebLogic Server or Identity Management binaries in a new location but you do need to run `pack` and `unpack` to move files to *`MSERVER`* on the new node. This is described in Section 17.2.5.7.9, "Completing the Oracle Identity Manager Configuration Steps."

To scale ODSM instances, follow these steps:

1. Assemble the following information for scaling ODSM.

Description	Variable	Documented Value	Customer Value
Host name		*`IDM_SCALED_OUT_HOST`*`.mycompany.com`	
ODSM Port	*`ODSM_PORT`*		This value is available in the *Oracle Fusion Applications Installation Workbook* Network - Ports tab ->Identity Management Port Numbers -> IDMDomain ODSM.
Oracle Instance Location/Name	*`ODS_ORACLE_INSTANCE`*	*`LOCAL_CONFIG_DIR`*`/instances/odsm`	
Oracle Middleware Home Location	*`IAM_MW_HOME`*	`/u01/oracle/products/app`	
Oracle Home Directory		`idm`	
WebLogic Admin host		`ADMINVHN.mycompany.com`	
WebLogic Admin Port	*`WLS_ADMIN_PORT`*	7001	
WebLogic User Name		weblogic_idm	
WebLogic Password	*`COMMON_IDM_PASSWORD`*		
WebLogic Server Directory		*`IAM_MW_HOME`*`/wlserver_10.3`	

2. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* manual in the Oracle Fusion Middleware documentation library for the platform and version you are using.
3. If you plan on provisioning the Instance Home or the Managed Server domain directory on shared storage, ensure that the appropriate shared storage volumes are mounted on the new host as described in Section 17.2.5.1, "Mounting Middleware Home and Creating a New Machine when Scaling Out."
4. If you are scaling out, you can use the default port (*`ODSM_PORT`*). If you are scaling up, you must choose a unique port for this instance. Ensure that port number you are using is not in use by any service on the computer by issuing this command for the operating system you are using. If a port is not in use, no output is returned from the command.

   On Linux:

   ```
   netstat -an | grep "7005"
   ```

   If the port is in use (if the command returns output identifying the port), you must free it.

   On Linux:

   Remove the entries for port `7005` (*`ODSM_PORT`*) in the `/etc/services` file if the port is in use by a service and restart the services, as described in Section 10.9.1, "Starting and Stopping Components," or restart the computer.

5. Start the Oracle Identity Management 11g Configuration Wizard by running the `config.sh` script located under the *`IDM_ORACLE_HOME`*`/bin` directory on the new host. For example: *`IDM_ORACLE_HOME`*`/bin`
6. On the Welcome screen, click **Next**.
7. On the Select Domain screen, select the **Expand Cluster** option and specify these values:
   - **Hostname:** `ADMINVHN.mycompany.com`
   - **Port**: `7001` (*`WLS_ADMIN_PORT`*)
   - **UserName**: `weblogic_idm`
   - **User Password**: *`password for the webLogic user`*
8. Click **Next**.
9. A dialog box with the following message appears:

   ```
   The selected domain is not a valid Identity Management domain or the installer
   cannot determine if it is a valid domain. If you created the domain using the
   Identity Management installer, you can ignore this message and continue. If you
   did not create the domain using the Identity Management installer, refer to the
   Identity Management documentation for information on how to verify the domain
   is valid.
   ```

   Click **YES** to continue.

   This is a benign warning that you can safely ignore.
10. A dialog box with the following message appears:

    ```
    The selected domain is not a valid Identity Management domain or the installer
    cannot determine if it is a valid domain. If you created the domain using the
    Identity Management installer, you can ignore this message and continue. If you
    did not create the domain using the Identity Management installer, refer to the
    Identity Management documentation for information on how to verify the domain
    is valid.
    ```

    Click **YES** to continue.

    This is a benign warning that you can safely ignore.
11. On the Email for Security Updates screen, specify these values:
    - **Email Address**: Provide the email address for your My Oracle Support account.
    - **Oracle Support Password**: Provide the password for your My Oracle Support account.
    - Select the checkbox next to the **I wish to receive security updates via My Oracle Support** field.

    Click **Next**.
12. On the Configure Components screen, de-select all the products except ODSM and then click **Next**.
13. On the Configure Ports screen, you use the `odsm_ports.ini` file you created in Step 4 to specify the ports to be used. This enables you to bypass automatic port configuration.
    a. Select **Specify Ports using a Configuration File**.

b. In the file name field specify `odsm_ports.ini`.

c. Click **Save**, then click **Next**.

14. On the Installation Summary screen, review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Configure**.

15. On the Configuration Progress screen, multiple configuration assistants are launched in succession; this process can be lengthy. Wait until it completes.

16. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

17. Add the newly added Managed Server host name and port to the list WebLogicCluster parameter, as described in Section 17.2.5.10, "Adding New WebLogic Managed Server to Oracle HTTP Server Configuration Files."

17.2.5.4 Scaling Oracle Access Manager 11g

To scale up, use the existing installations (WebLogic Server home, Oracle Fusion Middleware home, and domain directories) for creating a new Managed Server for the Oracle Access Manager component.

Use the existing binaries in shared storage for creating the new Managed Servers. You do not need to install WebLogic Server or Identity Management binaries in a new location but you do need to run pack and unpack to bootstrap the domain configuration in the new node.

> **Note:** If you are using shared storage, allow the new host access to that shared storage area.

17.2.5.5 Scale Oracle Access Manager by performing the steps in the following subsections:

17.2.5.5.1 Assembling Information for Scaling Oracle Access Manager Assemble the following information before scaling Oracle Access Manager.

Description	Variable	Documented Value	Customer Value
Host Name	`IDMHOSTn`		
Existing OAM server		`WLS_OAM1`	
New OAM server name	`WLS_OAMn`	`WLS_OAM3`	
Server Listen Address			
Server Listen Port	*`OAM_PORT`*		This value is available in the *Oracle Fusion Applications Installation Workbook* Network - Ports tab -> Identity Management Port Numbers -> IDMDomain OAM.
WebLogic Admin Host		ADMINVHN.mycompany.com	
WebLogic Admin Port	*`WLS_ADMIN_PORT`*	7001	
WebLogic Admin User		weblogic_idm	
WebLogic Admin Password			

17.2.5.5.2 Prepare New Node for Scaling Out The following steps are necessary only if you are scaling out.

1. Ensure that shared storage is mounted on the new node, as described in Section 17.2.5.1, "Mounting Middleware Home and Creating a New Machine when

Scaling Out."

17.2.5.6 To update the Middleware home list, create (or edit, if another WebLogic installation exists in the node) the *IAM_MW_HOME*/bea/beahomelist file and add *IAM_MW_HOME* to it.

17.2.5.6.1 Configuring the New Oracle Access Manager Server

1. Log in to the Oracle WebLogic Administration Console at: http://ADMIN.mycompany.com/console
2. From the Domain Structure window of the Oracle WebLogic Server Administration Console, expand the **Environment** node and then **Servers**. The Summary of Servers page appears.
3. Click **Lock & Edit** from the Change Center menu.
4. Select an existing server on the host you want to extend, for example: WLS_OAM1.
5. Click **Clone**.
6. Enter the following information:
   - **Server Name**: A new name for the server, for example: WLS_OAM3.
   - **Server Listen Address**: The name of the host on which the Managed Server runs.
   - **Server Listen Port**: The port the new Managed Server uses. This port must be unique within the host.

     If you are scaling out, you can use the default port, 14100 (*OAM_PORT*). If you are scaling up, choose a unique port.
7. Click **OK**.
8. Click the newly created server **WLS_OAM3**
9. Set **Machine** to be the machine you created in Section 17.2.5.1, "Mounting Middleware Home and Creating a New Machine when Scaling Out."
10. Click **Save**.
11. Disable host name verification for the new Managed Server. Before starting and verifying the WLS_OAM3 Managed Server, you must disable host name verification. You can re-enable it after you have configured server certificates for the communication between the Oracle WebLogic Administration Server and the Node Manager in IDMHOST*n*.

    If the source server from which the new one was cloned had already disabled host name verification, these steps are not required, as the host name verification settings were propagated to the cloned server. To disable host name verification:

    a. In Oracle Enterprise Manager Fusion Middleware Control, select **Oracle WebLogic Server Administration Console**.

    b. Expand the **Environment** node in the Domain Structure window.

    c. Click **Servers**. The Summary of Servers page appears.

    d. Select **WLS_OAM3** in the Names column of the table. The Settings page for server appears.

    e. Click the **SSL** tab.

    f. Click **Advanced**.

g. Set **Hostname Verification** to `None`.

h. Click **Save**.

12. Click **Activate Changes** from the Change Center menu.

13. Run `pack` and `unpack` as described in Section 17.2.5.9, "Running Pack/Unpack."

17.2.5.6.2 Registering the Managed Server with Oracle Access Manager Register the new Managed Server with Oracle Access Manager. You now must configure the new Managed Server now as an Oracle Access Manager server. You do this from the Oracle OAM console. Proceed as follows:

1. Log in to the OAM console at `http://ADMIN.mycompany.com/oamconsole` as the Oracle Access Manager user.
2. Click the **System Configuration** tab.
3. Click **Server Instances**.
4. Select **Create** from the Actions menu.
5. Enter the following information:
   - **Server Name**: `WLS_OAM3`
   - **Host**: Host that the server runs on
   - **Port**: Listen port that was assigned when the Managed Server was created
   - **OAM Proxy Port**: Port you want the Oracle Access Manager proxy to run on. This is unique for the host
   - **Proxy Server ID**: `AccessServerConfigProxy`
   - **Mode**: Set to same mode as existing Oracle Access Manager servers.
6. Click **Coherence** tab.

   Set **Local Port** to a unique value on the host.
7. Click **Apply**.
8. Restart the WebLogic Administration Server as described in Section 10.9.1, "Starting and Stopping Components."

17.2.5.6.3 Update WebGate Profiles Add the newly created Oracle Access Manager server to all WebGate Profiles that might be using it, such as `Webgate_IDM`, `Webgate_IDM_11g`, and `IAMSuiteAgent`

For example, to add the Oracle Access Manager server to `Webgate_IDM`, access the OAM console at: `http://ADMIN.mycompany.com/oamconsole`

Then proceed as follows:

1. Log in as the Oracle Access Manager Admin User.
2. Click the **System Configuration** tab.
3. Expand **Access Manager Settings - SSO Agents - OAM Agents**.
4. Click the open folder icon, then click **Search**.

   You should see the WebGate agent **Webgate_IDM**.
5. Click the agent **Webgate_IDM**.
6. Select **Edit** from the **Actions** menu.

7. Click **+** in the **Primary Server** list (or the **Secondary Server** list if this is a secondary server).
8. Select the newly created managed server from the **Server** list.
9. Set **Maximum Number of Connections** to `20` for all of the OAM Servers listed in the primary servers list (10 x WLS_OAM1 connections + 10 x WLS_OAM2 connections).
10. Click **Apply**.

Repeat Steps 5 to 10 for **Webgate_IDM_11g**, **IAMSuiteAgent**, and all other WebGates that might be in use.

You can now start the new Managed Server, as described in Section 10.9.1, "Starting and Stopping Components."

17.2.5.6.4 Update the Web Tier Add the newly added Managed Server host name and port to the list WebLogicCluster parameter, as described in Section 17.2.5.10, "Adding New WebLogic Managed Server to Oracle HTTP Server Configuration Files."

Save the file and restart the Oracle HTTP server, as described in Section 10.9.1, "Starting and Stopping Components."

17.2.5.7 Scaling Oracle Identity Manager

You already have a node that runs a Managed Server configured with Oracle SOA Suite and Oracle Identity Manager components. The node contains a Middleware home, a SOA Oracle home, an Oracle Identity Manager Oracle home, and a domain directory for existing Managed Servers. Use the existing installations in shared storage for creating a new WLS_SOA and WLS_OIM managed server. There is no need to install the Oracle Identity and Access Management or Oracle SOA Suite binaries in a new location

When scaling up, you add WLS_SOA and WLS_OIM managed servers to existing nodes.

In either case, you must run pack and unpack.

When you scale out the topology, you add new Managed Servers configured with OIM and SOA to new nodes. First check that the new node can access the existing home directories for WebLogic Server, OIM, and SOA. You do need to run pack and unpack to bootstrap the domain configuration in the new node.

Follow the steps in the following subsections to scale the topology:

- Section 17.2.5.7.1, "Assembling Information for Scaling Oracle Identity Manager"
- Section 17.2.5.7.2, "Cloning an Existing Oracle Identity Manager Server when Scaling Up Oracle Identity Manager or SOA"
- Section 17.2.5.7.3, "Mounting Middleware Home and Creating a New Machine when Scaling Out"
- Section 17.2.5.7.4, "Configuring New JMS Servers"
- Section 17.2.5.7.5, "Performing Pack/Unpack When Scaling Out"
- Section 17.2.5.7.6, "Configuring Oracle Coherence for Deploying Composites"
- Section 17.2.5.7.9, "Completing the Oracle Identity Manager Configuration Steps"

17.2.5.7.1 Assembling Information for Scaling Oracle Identity Manager Assemble the following information before scaling Oracle Identity Manager.

Description	Variable	Documented Value	Customer Value
Host name	IDMHOST*n*	IDM_PROVISIONED_HOST	
SOA virtual server name		SOAHOST*x*VHN	
OIM virtual server name		OIMHOST*x*VHN	
SOA managed server to clone	WLS_SOA*n*	WLS_SOA_PROVISIONED_HOST	
OIM managed server to clone	WLS_OIM*n*	WLS_OIM_PROVISIONED_HOST	
SOA managed server name	WLS_SOA*n*	WLS_SOA_SCALED_OUT_HOST2	
OIM managed server name	WLS_OIM*n*	WLS_OIM_SCALED_OUT_HOST	
Numeric extension for new JMS servers	*n*	3	
WebLogic Admin Host		ADMINVHN.mycompany.com	
WebLogic Admin Port	*WLS_ADMIN_PORT*	7001	
WebLogic Admin User		weblogic_idm	
WebLogic Admin Password			

17.2.5.7.2 Cloning an Existing Oracle Identity Manager Server when Scaling Up Oracle Identity Manager or SOA Follow this procedure twice, once to clone *WLS_SOA_PROVISIONED_HOST* and once again to clone *WLS_OIM_PROVISIONED_HOST*.

1. Log in to the Administration Console at: `http://ADMIN.mycompany.com/console`
2. Clone the *WLS_OIM_PROVISIONED_HOST* or the *WLS_SOA_PROVISIONED_HOST* into a new Managed Server. The source Managed Server to clone should be one that already exists on the node where you want to run the new Managed Server.

   To clone a Managed Server:

   a. Select **Environment** -> **Servers** from the Administration Console.

   b. From the Change Center menu, click **Lock and Edit**.

   c. Select the Managed Server that you want to clone (for example, *WLS_OIM_PROVISIONED_HOST* or *WLS_SOA_PROVISIONED_HOST*).

   d. Select **Clone**.

   Name the new Managed Server *WLS_OIM_PROVISONED_HOSTn* or *WLS_SOA_PROVISIONED_HOSTn*, where *n* is a number to identify the new Managed Server.

   The rest of the steps assume that you are adding a new server to *IDM_PROVISIONED_HOST*, which is already running *WLS_SOA_PROVISIONED_HOST* and *WLS_OIM_PROVISIONED_HOST*.
3. For the listen address, assign the host name or IP address to use for this new Managed Server. If you are planning to use server migration as recommended for this server, this should be the VIP (also called a floating IP) to enable it to move to another node. The VIP should be different from the one used by the Managed Server that is already running.

17.2.5.7.3 Mounting Middleware Home and Creating a New Machine when Scaling Out Mount the Middleware home, as described in Section 17.2.5.1, "Mounting Middleware Home and Creating a New Machine when Scaling Out."

17.2.5.7.4 Configuring New JMS Servers Create JMS Servers for SOA, Oracle Identity Manager, UMS, and BPM on the new Managed Server. You do this as follows:

1. Log in to the WebLogic Administration Server and navigate to **Services -> Messaging -> JMS Servers**.
2. Click **New**.
3. Enter a value for **Name**, such as `BPMJMSServer_auto_3`.
4. Click **Create New Store**.
5. Select `FileStore` from the list
6. Click **Next**.
7. Enter a value for **Name**, such as `BPMJMSFileStore_auto_3`
8. Enter the following values:

   Target: The new server you are creating.

   Directory: *`ASERVER_HOME`*`/jms/BPMJMSFileStore_auto_3`
9. Click **OK**.
10. When you are returned to the JMS Server screen, select the newly created file store from the list.
11. Click **Next**.
12. On the next screen set the Target to the server you are creating.
13. Click **Finish**.

Create the following JMS Queues depending on the managed server you are creating:

Server	JMS Server Name	File Store Name	Directory	Target
WLS_SOA*n*	BPMJMSServer_auto_*n*	BPMJMSFileStore_auto_*n*	*`ASERVER_HOME`*`/jms/BPMJMSFileStore_auto_`*n*	WLS_SOA*n*
WLS_SOA*n*	SOAJMSServer_auto_*n*	SOAJMSFileStore_auto_*n*	*`ASERVER_HOME`*`/jms/SOAJMSFileStore_auto_`*n*	WLS_SOA*n*
WLS_SOA*n*	UMSJMSServer_auto_*n*	UMSJMSFileStore_auto_*n*	*`ASERVER_HOME`*`/jms/UMSJMSFileStore_auto_`*n*	WLS_SOA*n*
wls_OIM*n*	OIMJMSServer_auto_*n*	OIMJMSFileStore_auto_*n*	*`ASERVER_HOME`*`/jms/OIMJMSFileStore_auto_`*n*	wls_OIM*n*
wls_SOA*n*	PS6SOAJMSServer_auto_*n*	PS6SOAJMSFileStore_auto_*n*	*`ASERVER_HOME`*`/jms/PS6SOAJMSFileStore_auto_`*n*	wls_SOA*n*

Add the newly created JMS Queues to the existing JMS Modules by performing the following steps:

1. Log in to the WebLogic Administration Console
2. Navigate to **Services -> Messaging -> JMS Modules**
3. Click a JMSModule, such as **SOAJMSModule**
4. Click the **Sub Deployments** tab.
5. Click the listed sub deployment.

> **Note:** This subdeployment module name is a random name in the form of **JMSServerName*XXXXXX*** resulting from the Configuration Wizard JMS configuration.

6. Assign the newly created JMS server, for example **SOAJMSServer_auto*n***.
7. Click **Save**.
8. Perform this for each of the JMS modules listed in the following table:

JMS Module	JMS Server
BPMJMSModule	BPMJMSServer_auto_*n*
JRFWSAsyncJmsModule	JRFWSAsyncJmServer_auto_*n*
OIMJMSModule	OIMJMSServer_auto_*n*
SOAJMSModule	SOAJMSServer_auto_*n*
UMSJMSSystemResource	UMSJMSServe_auto_*n*

9. Click **Activate Configuration** from the Change Center menu.

17.2.5.7.5 Performing Pack/Unpack When Scaling Out

This section is necessary only when you are scaling out.

Run `pack` and `unpack` as described in Section 17.2.5.9, "Running Pack/Unpack."

17.2.5.7.6 Configuring Oracle Coherence for Deploying Composites

Although deploying composites uses multicast communication by default, Oracle recommends using unicast communication in SOA enterprise deployments. Use unicast if you disable multicast communication for security reasons.

Unicast communication does not enable nodes to discover other cluster members in this way. Consequently, you must specify the nodes that belong to the cluster. You do not need to specify all of the nodes of a cluster, however. You need only specify enough nodes so that a new node added to the cluster can discover one of the existing nodes. As a result, when a new node has joined the cluster, it is able to discover all of the other nodes in the cluster. Additionally, in configurations such as SOA enterprise deployments where multiple IPs are available in the same system, you must configure Oracle Coherence to use a specific host name to create the Oracle Coherence cluster.

> **Note:** An incorrect configuration of the Oracle Coherence framework used for deployment may prevent the SOA system from starting. The deployment framework must be properly customized for the network environment on which the SOA system runs. Oracle recommends the configuration described in this section.

17.2.5.7.7 Enabling Communication for Deployment Using Unicast Communication

Specify the nodes using the `tangosol.coherence.wkan` system property, where *n* is a number between 1 and 9. You can specify up to 9 nodes. Start the numbering at 1. This numbering must be sequential and must not contain gaps. In addition, specify the host name used by Oracle Coherence to create a cluster through the `tangosol.coherence.localhost` system property. This local host name should be the virtual host name used by the SOA server as the listener addresses, for example: SOAHOST3VHN. Set this property by adding the `-Dtangosol.coherence.localhost`

parameters to the Arguments field of the Oracle WebLogic Server Administration Console's Server Start tab. You will also need to add the new server to the existing entries.

> **Tip:** To guarantee high availability during deployments of SOA composites, specify enough nodes so that at least one of them is running at any given time.

> **Note:** *SOA_SCALED_OUT_HOST2VHN* is the virtual host name that maps to the virtual IP where *WLS_SOA_SCALED_OUT_HOST2* is listening.

17.2.5.7.8 Specifying the Host Name Used by Oracle Coherence

Use the Administration Console to specify a host name used by Oracle Coherence.

To add the host name used by Oracle Coherence:

1. Log into the Oracle WebLogic Server Administration Console.
2. In the Domain Structure window, expand the **Environment** node.
3. Click **Servers**. The Summary of Servers page appears.
4. Click the name of the server (*WLS_SOA_PROVISIONED_HOST* or *WLS_SOA_SCALED_OUT_HOST*, which are represented as hyperlinks) in Name column of the table. The settings page for the selected server appears.
5. Click **Lock & Edit**.
6. Click the **Server Start** tab.
7. Enter the following for *WLS_SOA_PROVISIONED_HOST*, *WLS_SOA_SCALED_OUT_HOST1*, and *WLS_SOA_SCALED_OUT_HOST2* into the Arguments field.

   For *WLS_SOA_PROVISIONED_HOST*, enter the following:

   ```
   -Dtangosol.coherence.wka1=SOAHOST1VHN
   -Dtangosol.coherence.wka2=SOAHOST2VHN
   -Dtangosol.coherence.wka3=SOAHOST3VHN
   -Dtangosol.coherence.localhost=SOAHOST1VHN
   ```

   For *WLS_SOA_SCALED_OUT_HOST1*, enter the following:

   ```
   -Dtangosol.coherence.wka1=SOAHOST1VHN
   -Dtangosol.coherence.wka2=SOAHOST2VHN
   -Dtangosol.coherence.wka3=SOAHOST3VHN
   -Dtangosol.coherence.localhost=SOAHOST2VHN
   ```

   For *WLS_SOA_SCALED_OUT_HOST2*, enter the following:

   ```
   -Dtangosol.coherence.wka1=SOAHOST1VHN
   -Dtangosol.coherence.wka2=SOAHOST2VHN
   -Dtangosol.coherence.wka3=SOAHOST3VHN
   -Dtangosol.coherence.localhost=SOAHOST3VHN
   ```

> **Note:** There should be no breaks in lines between the different `-D` parameters. Do not copy or paste the text to your Administration Console's arguments text field. It may result in HTML tags being inserted in the Java arguments. The text should not contain other text characters than those included the example above.

Note: The Coherence cluster used for deployment uses port 8088 by default. This port can be changed by specifying a different port (for example, 8089) with the -Dtangosol.coherence.wkan.port and -Dtangosol.coherence.localport startup parameters. For example:

WLS_SOA_PROVISIONED_HOST (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=SOAHOST1VHN
-Dtangosol.coherence.wka2=SOAHOST2VHN
-Dtangosol.coherence.wka3=SOAHOST3VHN
-Dtangosol.coherence.localhost=SOAHOST1VHN
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
-Dtangosol.coherence.wka3.port=8089
```

WLS_SOA_SCALED_OUT_HOST1 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=SOAHOST1VHN
-Dtangosol.coherence.wka2=SOAHOST2VHN
-Dtangosol.coherence.wka3=SOAHOST3VHN
-Dtangosol.coherence.localhost=SOAHOST2VHN
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
-Dtangosol.coherence.wka3.port=8089
```

WLS_SOA_SCALED_OUT_HOST2 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=SOAHOST1VHN
-Dtangosol.coherence.wka2=SOAHOST2VHN
-Dtangosol.coherence.wka3=SOAHOST3VHN
-Dtangosol.coherence.localhost=SOAHOST3VHN
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
-Dtangosol.coherence.wka3.port=8089
```

8. Click **Save** and **Activate Changes**.

Note: You must ensure that these variables are passed to the managed server correctly. They should be reflected in the server's output log. Failure of the Oracle Coherence framework can prevent the soa-infra application from starting.

Note: The multicast and unicast addresses are different from the ones used by the WebLogic Server cluster for cluster communication. SOA guarantees that composites are deployed to members of a single WebLogic Server cluster even though the communication protocol for the two entities (the WebLogic Server cluster and the groups to which composites are deployed) are different.

17.2.5.7.9 Completing the Oracle Identity Manager Configuration Steps

1. Configure TX persistent store for the new server. This should be a location visible from other nodes as indicated in the recommendations about shared storage.

   From the WebLogic Administration Console, select the **Server_name** > **Services** tab. Under Default Store, in **Directory**, enter the path to the folder where you want the default persistent store to store its data files.

2. Disable host name verification for the new Managed Server. Before starting and verifying the `WLS_SOA`*`n`* Managed Server, you must disable host name verification. You can re-enable it after you have configured server certificates for the communication between the Oracle WebLogic Administration Server and the Node Manager in `IDMHOST`*`n`*. If the source server from which the new one has been cloned had already disabled host name verification, these steps are not required (the host name verification settings is propagated to the cloned server).

   To disable host name verification:

   a. In the Oracle Enterprise Manager Console, select **Oracle WebLogic Server Administration Console**.

   b. Expand the **Environment** node in the Domain Structure window.

   c. Click **Servers**. The Summary of Servers page appears.

   d. Select **WLS_SOA*n*** in the Names column of the table. The Settings page for the server appears.

   e. Click the **SSL** tab.

   f. Click **Advanced**.

   g. Set **Hostname Verification** to `None`.

   h. Click **Save**.

3. Repeat Steps 6a through 6h to disable host name verification for the `WLS_OIM`*`n`* Managed Servers. In Step d, select **WLS_OIM*n*** in the Names column of the table.

4. Click **Activate Changes** from the Change Center menu.

5. Restart the WebLogic Administration Server as described in Section 10.9.1, "Starting and Stopping Components."

6. Start and test the new Managed Server from the Administration Console.

   a. Shut down the existing Managed Servers in the cluster.

   b. Ensure that the newly created Managed Server, `WLS_SOA`*`n`*, is up.

   c. Access the application on the newly created Managed Server (`http://vip:port/soa-infra`). The application should be functional.

7. Configure the newly created managed server for server migration. Follow the steps in Section 17.3.6, "Configuring Server Migration Targets" to configure server migration.

Note: Since this new node is using an existing shared storage installation, the node is already using a Node Manager and an environment configured for server migration that includes netmask, interface, `wlsifconfig` script superuser privileges. The floating IP addresses for the new Managed Servers are already present in the new node.

---

8. Test server migration for this new server. Follow these steps from the node where you added the new server:

   a. Stop the `WLS_SOA`*n* Managed Server.

      To do this, run:

      ```
      kill -9 pid
      ```

      on the process ID (PID) of the Managed Server. You can identify the PID of the node using

      ```
      ps -ef | grep WLS_SOAn
      ```

   b. Watch the Node Manager Console. You should see a message indicating that the floating IP address for *`WLS_SOA_PROVISIONED_HOST`* has been disabled.

   c. Wait for the Node Manager to try a second restart of WLS_SOA*n*. Node Manager waits for a fence period of 30 seconds before trying this restart.

   d. Once Node Manager restarts the server, stop it again. Now Node Manager should log a message indicating that the server will not be restarted again locally.

   e. Repeat Steps a-d for WLS_OIM*n*.

17.2.5.8 Scaling Oracle Identity Federation

The Oracle Identity Federation instances can be scaled out by adding a new node with a Managed Server to the existing cluster.

The existing installations (WebLogic Server home, Oracle Fusion Middleware home, and domain directories) can be used for creating a new Managed Server for Oracle Identity Federation.

The Oracle Identity Federation instances can be scaled out by adding a new node with a Managed Server to the existing cluster.

Perform the steps in the following sections to scale Oracle Identity Federation.

- Section 17.2.5.8.1, "Assembling Information for Scaling Oracle Identity Federation"
- Section 17.2.5.8.2, "Configuring Oracle Identity Federation"
- Section 17.2.5.8.3, "Performing Pack/Unpack when Scaling Out"
- Section 17.2.5.8.4, "Complete Oracle Identity Federation Server Configuration"
- Section 17.2.5.8.5, "Add New Managed Server to OHS Configuration"

17.2.5.8.1 Assembling Information for Scaling Oracle Identity Federation Assemble the following information before scaling Oracle Identity Federation.

Description	Variable	Documented Value	Customer Value
Host name		*`IDM_SCALED_OUT_HOST`*`.mycompany.com`	
OIF Port	*`OIF_PORT`*	7499	This value is available in the *Oracle Fusion Applications Installation Workbook* Network - Ports tab -> Identity Management Port Numbers -> IDMDomain OIF.
Instance name	`oif`*n*	`oif3`	
WebLogic Admin Host		`ADMINVHN.mycompany.com`	
WebLogic Admin Port	*`WLS_ADMIN_PORT`*	7001	

Description	Variable	Documented Value	Customer Value
WebLogic Admin User		weblogic_idm	
WebLogic Admin Password			

17.2.5.8.2 Configuring Oracle Identity Federation **1.** Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* in the Oracle Fusion Middleware documentation library for the platform and version you are using.

2. Create a file containing the ports used by Oracle Internet Directory. On Disk1 of the installation media, locate the file `stage/Response/staticports.ini`. Copy it to a file called `oif_ports.ini`. Delete all entries in `oif_ports.ini` except for `Oracle Identity Federation Server Port`. Change the value of that port to the port you are using for this instance.

   If you are scaling out, you can use the default port, 7499 (*`OIF_PORT`*). If you are scaling up, you must choose a unique port for this instance.

   Note: If the port name in the file is slightly different from those listed in this step, use the name in the file.

3. Ensure that the appropriate shared storage volumes are mounted on the new *`IDMHOST`*, as described in Section 17.2.5.1, "Mounting Middleware Home and Creating a New Machine when Scaling Out."

4. Ensure that the port you want to use is not in use by any service on the computer by issuing these commands for the operating system you are using, specifying the port you want to use. If a port is not in use, no output is returned from the command.

   UNIX:

   ```
   netstat -an | grep "7499"
   ```

   If the port is in use (if the command returns output identifying the port), you must free it.

   UNIX:

   Remove the entries for port `7499` in the `/etc/services` file.

5. Start the Oracle Identity Management 11*g* Configuration Wizard located under the *`IDM_ORACLE_HOME`*`/bin` directory as follows:

   Issue this command:

   ```
   ./config.sh
   ```

6. On the Welcome screen, click **Next**.

7. On the Select Domain screen, select the **Expand Cluster** option and specify these values:

   - **HostName**: `ADMINVHN.mycompany.com`
   - **Port**: `7001`
   - **UserName**: `weblogic_idm`
   - **User Password**: *`weblogic_user_password`*

Click **Next**.

8. A dialog box with the following message appears:

   ```
   The selected domain is not a valid Identity Management domain or the installer
   cannot determine if it is a valid domain. If you created the domain using the
   Identity Management installer, you can ignore this message and continue. If you
   did not create the domain using the Identity Management installer, refer to the
   Identity Management documentation for information on how to verify the domain
   is valid.
   ```

   This is a benign warning that you can ignore.

   Click **Yes** to continue.

9. On the Specify Installation Location screen, specify the following values:

   - **Oracle Middleware Home Location**: *OIF_MW_HOME* (This value is prefilled and cannot be updated.)
   - **Oracle Home Directory**: `idm` (This value is prefilled and cannot be updated.)
   - **WebLogic Server Directory**: *OIF_MW_HOME*`/wlserver_10.3`
   - **Oracle Instance Location**: *OIF_ORACLE_INSTANCE*
   - **Instance Name**: `oif`*n*, where *n* is a sequential number, for example `oif3`.

   Click **Next**.

10. On the Specify Security Updates screen (if shown), specify the values shown in this example:

    - **Email Address**: Provide the email address for your My Oracle Support account.
    - **Oracle Support Password**: Provide the password for your My Oracle Support account.
    - Select **I wish to receive security updates via My Oracle Support**.

    Click **Next**.

11. On the Configure Components screen, de-select all the components except Oracle Identity Federation components. Select only Oracle Identity Federation from the Oracle Identity Federation components. Do not select Oracle HTTP Server.

    Click **Next**.

12. On the Configure Ports screen, you use the `oif_ports.ini` file you created in Step 2 to specify the ports to be used. This enables you to bypass automatic port configuration.

    a. Select **Specify Ports using a Configuration File**.

    b. In the file name field specify `oif_ports.ini`.

    c. Click **Save**, then click **Next**.

13. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not correct, click **Back** to modify selections on previous screens. Then click **Configure**.

14. On the Configuration Progress screen, view the progress of the configuration.

15. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

17.2.5.8.3 Performing Pack/Unpack when Scaling Out This section is necessary only when you are scaling out.

From *IDM_PROVISIONED_HOST*, copy the applications directory under the *ASERVER_HOME*/config/fmwconfig/servers/wls_oif1 directory to the *ASERVER_HOME*/config/fmwconfig/servers/wls_oif*n* directory, where wls_oif*n* is the new server being added, for example:

```
cp -rp ASERVER_HOME/config/fmwconfig/servers/wls_oif1/applications  user@IDM_
PROVISIONED_HOST:ASERVER_HOME/config/fmwconfig/servers/wls_oif3
```

Then run pack and unpack as described in Section 17.2.5.9, "Running Pack/Unpack."

17.2.5.8.4 Complete Oracle Identity Federation Server Configuration Perform the steps in Section 16.10.3.3, "Validating Oracle Identity Federation" and Section 16.10.3.4, "Configuring the Enterprise Manager Agents" to completed the configuration of your new server.

17.2.5.8.5 Add New Managed Server to OHS Configuration Add the newly added Managed Server host name and port to the list WebLogicCluster parameter, as described in Section 17.2.5.10, "Adding New WebLogic Managed Server to Oracle HTTP Server Configuration Files."

17.2.5.9 Running Pack/Unpack

Whenever you extend a domain to include a new managed server, you must extract the domain configuration needs from the *ASERVER_HOME* location to the *MSERVER_HOME* location. This applies whether you are scaling up or out. To do this perform the following steps.

1. Pack the domain on *IDM_PROVISIONED_HOST* to create a template pack using the command:

   ```
   pack.sh -domain=ASERVER_HOME -template =/templates/managedServer.jar -template_
   name="template_name" -managed=true
   ```

   The pack.sh script is located in *ORACLE_COMMON_HOME*/common/bin.

2. Unpack the domain on the new host for scale out, or on the existing host for scale up, using the command:

   ```
   unpack.sh -domain=MSERVER_HOME -template=/templates/managedServer.jar -app_
   dir=MSERVER_HOME/applications
   ```

   The unpack.sh script is located in *ORACLE_COMMON_HOME*/common/bin.

3. If you are scaling out, start Node Manager and update the property file.

   a. Start and stop Node Manager as described in Section 10.9.1, "Starting and Stopping Components."

   b. Run the script setNMProps.sh, which is located in *ORACLE_COMMON_HOME*/common/bin, to update the node manager properties file, for example:

      ```
      cd ORACLE_COMMON_HOME/common/bin
      ./setNMProps.sh
      ```

   c. Start Node Manager once again as described in Section 10.9.1, "Starting and Stopping Components."

17.2.5.10 Adding New WebLogic Managed Server to Oracle HTTP Server Configuration Files

Scaling an Application Tier component typically requires you to create a new WebLogic managed server. If you add a new managed server to your topology, after adding the managed server you must update your Oracle HTTP Server configuration files (on all nodes) and add the new server to the existing WebLogic cluster directives.

In the Web tier, there are several configuration files under *WEB_ORACLE_INSTANCE*/config/OHS/componentname/moduleconf, including admin_vh.conf, sso_vh.conf and idminternal_vh.conf. Each contain a number of entries in location blocks. If a block references two server instances and you add a third one, you must update that block with the new server.

For example if you add a new Oracle Access Manager server, you must update sso_vh.conf to include the new managed server. You add the new server to the WebLogicCluster directive in the file, for example, change:

```
<Location /oam>
   SetHandler weblogic-handler
   WebLogicCluster IDM_PROVISIONED_HOST.mycompany.com:14100,IDM_SCALED_OUT_
HOST.mycompany.com:14100
</Location>

<Location /fusion_apps>
   SetHandler weblogic-handler
   WebLogicCluster IDM_PROVISIONED_HOST.mycompany.com:14100,IDM_SCALED_OUT_
HOST.mycompany.com:14100
</Location>
```

to:

```
<Location /oam>
   SetHandler weblogic-handler
   WebLogicCluster IDM_PROVISIONED_HOST.mycompany.com:14100,IDM_SCALED_OUT_
HOST.mycompany.com:14100,IDM_PROVISIONED_HOST.mycompany.com:14101
</Location>

<Location /fusion_apps>
   SetHandler weblogic-handler
   WebLogicCluster IDM_PROVISIONED_HOST.mycompany.com:14100,IDM_SCALED_OUT_
HOST.mycompany.com:14100,IDM_SCALED_OUT_HOST.mycompany.com:14100
</Location>
```

Similarly, if you add a new ODSM server, you must update ODSM entries in the file admin_vh.conf.

Once you have updated the configuration file, restart the Oracle HTTP server(s) as described in Section 10.9.1, "Starting and Stopping Components." Oracle recommends that you do this sequentially to prevent loss of service.

17.2.6 Scaling the Web Tier

The Web Tier already has a node running an instance of the Oracle HTTP Server. The existing Oracle HTTP Server binaries can be used for creating the new Oracle HTTP Server instance.

To scale the Oracle HTTP Server, perform the steps in the following subsections:

- Section 17.2.6.1, "Assembling Information for Scaling the Web Tier"

- Section 17.2.6.2, "Mounting Middleware Home and Copying Oracle HTTP Server Files when Scaling Out"
- Section 17.2.6.3, "Running the Configuration Wizard to Configure the HTTP Server"
- Section 17.2.6.4, "Registering Oracle HTTP Server with WebLogic Server"
- Section 17.2.6.5, "Reconfiguring the Load Balancer"

17.2.6.1 Assembling Information for Scaling the Web Tier

Assemble the following information before scaling the Web Tier.

Description	Variable	Documented Value	Customer Value
Host name		WEBHOST1.mycompany.com	
OHS port	*OHS_PORT*	7777	
Instance Name	webn	web1 or web2	
Component Name	webn	web1 or web2	
WebLogic Admin Host		ADMINVHN.mycompany.com	
WebLogic Admin Port	*WLS_ADMIN_PORT*	7001	
WebLogic Admin User		weblogic_idm	
WebLogic Admin Password			

17.2.6.2 Mounting Middleware Home and Copying Oracle HTTP Server Files when Scaling Out

On the new node, mount the existing Middleware home.

Copy all files created in *ORACLE_INSTANCE*/config/OHS/*component*/moduleconf from the existing Web Tier configuration to the new one.

17.2.6.3 Running the Configuration Wizard to Configure the HTTP Server

Perform these steps to configure the Oracle Web Tier:

1. Create a file containing the ports used by Oracle HTTP Server. On Disk1 of the installation media, locate the file stage/Response/staticports.ini. Copy it to a file called ohs_ports.ini. Delete all entries in ohs_ports.ini except for OHS PORT and OPMN Local Port. Change the value of OPMN Local Port to 6700. If you are scaling out, you can use the default value, 7777, for OHS PORT. If you are scaling up, you must choose a unique value for that instance on the machine.

   Note: If the port names in the file are slightly different from OHS PORT and OPMN Local Port, use the names in the file.

2. Change the directory to the location of the Oracle Fusion Middleware Configuration Wizard:

   ```
   cd WEB_ORACLE_HOME/bin
   ```

3. Start the Configuration Wizard:

   ```
   ./config.sh
   ```

Enter the following information into the configuration wizard:

1. On the Welcome screen, click **Next**.
2. On the Configure Component screen, select: **Oracle HTTP Server**.

   Ensure that Associate Selected Components with WebLogic Domain is selected.

   Ensure Oracle Web Cache is **NOT** selected.

   Click **Next**.
3. On the Specify WebLogic Domain Screen, enter
   - **Domain Host Name**: `ADMINVHN.mycompany.com`
   - **Domain Port No**: `7001`, where `7001` is *`WLS_ADMIN_PORT`*.
   - **User Name**: Weblogic Administrator User (For example: `weblogic`)
   - **Password**: Password for the Weblogic Administrator User account

   Click **Next**.
4. On the Specify Component Details screen, specify the following values:

   Enter the following values for WEBHOST*n*, where *n* is the number of the new host, for example, `3`:
   - **Instance Home Location**: *WEB_ORACLE_INSTANCE* (`/u02/local/oracle/config/instances/ohs`*n*, for example, `/u02/local/oracle/config/instances/ohs1`)
   - **Instance Name**: `web`*n*
   - **OHS Component Name**: `web`*n*

   Click **Next**.
5. On the Configure Ports screen, you use the `ohs_ports.ini` file you created in Step 1to specify the ports to be used. This enables you to bypass automatic port configuration.
   a. Select **Specify Ports using a Configuration File**.
   b. In the file name field specify `ohs_ports.ini`.
   c. Click **Save**, then click **Next**.
6. On the Specify Security Updates screen, specify these values:
   - **Email Address**: The email address for your My Oracle Support account.
   - **Oracle Support Password**: The password for your My Oracle Support account.

   Select: **I wish to receive security updates via My Oracle Support**.

   Click **Next**.
7. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not, click **Back** to modify selections on previous screens.

   Click **Configure**.

   On the Configuration screen, the wizard launches multiple configuration assistants. This process can be lengthy. When it completes, click **Next**.

   On the Installation Complete screen, click **Finish** to confirm your choice to exit.

17.2.6.4 Registering Oracle HTTP Server with WebLogic Server

For Oracle Enterprise Manager Fusion Middleware Control to be able to manage and monitor the new Oracle HTTP server, you must register the Oracle HTTP server with IDMDomain. To do this, register Oracle HTTP Server with WebLogic Server by running the following command on the host where the new server is running:

```
cd WEB_ORACLE_INSTANCE/bin
./opmnctl registerinstance -adminHost ADMINVHN.mycompany.com \
   -adminPort 7001 -adminUsername weblogic
```

17.2.6.5 Reconfiguring the Load Balancer

Add the new Oracle HTTP Server instance to the existing server pool defined on the load balancer for distributing requests across the HTTP instances.

17.2.7 Post-Scaling Steps for All Components

Provisioning creates a set of scripts to start and stop managed servers defined in the domain. When you create a new managed server in the domain you need to update the domain configuration so that these start and stop scripts can also start the newly created managed server.

To update the domain configuration, edit the file `serverInstancesCustom.txt`, which is located in the directory: *SHARED_CONFIG_DIR*`/scripts`

If you want to start a node manager on a new machine, add an entry which looks like this:

newmachine`.mycompany.com NM` *nodemanager_pathname nodemanager_port*

For example:

```
IDM_SCALED_OUT_HOST.mycompany.com NM /u01/oracle/config/nodemanager/IDM_SCALED_
OUT_HOST.mycompany.com 5556
```

If you want to start a managed server called *WLS_OIM_SCALED_OUT_HOST* add an entry which looks like this:

newmachine`.mycompany.com OIM` *ManagedServerName*

For example:

```
IDM_SCALED_OUT_HOST OIM WLS_OIM_SCALED_OUT_HOST
```

Save the file

17.3 Setting Up Server Migration for Identity Management

Configuring server migration allows SOA-managed and OIM-managed servers to be migrated from one host to another, so that if a node hosting one of the servers fails, the service can continue on another node. This chapter describes how to configure server migration for an Identity Management enterprise deployment.

17.3.1 Overview of Server Migration for an Enterprise Deployment

Perform the steps in the following sections to configure server migration for the following Managed Servers:

- *WLS_OIM_PROVISIONED_HOST*
- *WLS_SOA_PROVISIONED_HOST*
- *WLS_OIM_SCALED_OUT_HOST*

- *WLS_SOA_SCALED_OUT_HOST*

The *WLS_OIM_PROVISIONED_HOST* and *WLS_SOA_PROVISIONED_HOST* Managed Server are configured to restart on *IDM_SCALED_OUT_HOST* should a failure occur.

The *WLS_OIM_SCALED_OUT_HOST* and *WLS_SOA_SCALED_OUT_HOST* Managed Servers are configured to restart on *IDM_PROVISIONED_HOST* should a failure occur.

The *WLS_OIM_PROVISIONED_HOST*, *WLS_SOA_PROVISIONED_HOST*, *WLS_OIM_SCALED_OUT_HOST* and *WLS_SOA_SCALED_OUT_HOST* servers listen on specific floating IPs that are failed over by WebLogic Server Migration.

17.3.2 Setting Up a User and Tablespace for the Server Migration Leasing Table

In this section, you set up a user and tablespace for the server migration leasing table:

> **Note:** If other servers in the same domain have already been configured with server migration, the same tablespace and data sources can be used. In that case, the data sources and multi data source for database leasing do not need to be re-created, but they must be retargeted to the clusters being configured with server migration.

1. Create a tablespace called `leasing`. For example, log on to SQL*Plus as the sysdba user and run the following command:

```
create tablespace leasing
logging datafile 'DB_HOME/oradata/orcl/leasing.dbf'
size 32m autoextend on next 32m maxsize 2048m extent management local;
```

2. Create a user named `leasing` and assign to it the `leasing` tablespace:

```
create user leasing identified by password;
grant create table to leasing;
grant create session to leasing;
alter user leasing default tablespace leasing;
alter user leasing quota unlimited on LEASING;
```

3. Create the `leasing` table using the `leasing.ddl` script:
   a. Copy the `leasing.ddl` file located in either of the following directories to your database node:

```
WL_HOME/server/db/oracle/817
WL_HOME/server/db/oracle/920
```

   b. Connect to the database as the `leasing` user.
   c. Run the `leasing.ddl` script in SQL*Plus:

```
@Copy_Location/leasing.ddl;
```

17.3.3 Creating a Multi Data Source Using the Oracle WebLogic Administration Console

The second step is to create a multi data source for the leasing table from the Oracle WebLogic Server Administration Console. Console URLs are provided in Section 10.9.2, "About Oracle Identity Management Console URLs". You create a data source to each of the Oracle RAC database instances during the process of setting up

the multi data source, both for these data sources and the global leasing multi data source. When you create a data source:

- Ensure that this is a non-XA data source.
- The names of the multi data sources are in the format of *MultiDS*-rac0, *MultiDS*-rac1, and so on.
- Use Oracle's Driver (Thin) Version 9.0.1, 9.2.0, 10, 11.
- Data sources do not require support for global transactions. Therefore, do *not* use any type of distributed transaction emulation/participation algorithm for the data source (do not choose the **Supports Global Transactions** option, or the **Logging Last Resource**, **Emulate Two-Phase Commit**, or **One-Phase Commit** options of the **Supports Global Transactions** option), and specify a service name for your database.
- Target these data sources to the oim_cluster and the soa_cluster.
- Ensure the data source's connection pool initial capacity is set to 0 (zero). To do this, select **Services**, **JDBC**, and then **Datasources**. In the Datasources screen, click the **Datasource Name**, then click the **Connection Pool** tab, and enter **0** (zero) in the **Initial Capacity** field.

Creating a Multi Data Source

Perform these steps to create a multi data source:

1. From Domain Structure window in the Oracle WebLogic Server Administration Console, expand the **Services** node. The Summary of JDBC Data Source page appears.
2. Click **Data Sources**. The Summary of JDBC Multi Data Source page is displayed.
3. Click **Lock and Edit**.
4. Click **New Multi Data Source**. The Create a New JDBC Multi Data Source page is displayed.
5. Enter `leasing` as the name.
6. Enter `jdbc/leasing` as the JNDI name.
7. Select **Failover** as algorithm (default).
8. Click **Next.**
9. Select **oim_cluster** and **soa_cluster** as the targets.
10. Click **Next**.
11. Select **non-XA driver** (the default).
12. Click **Next**.
13. Click **Create New Data Source**.
14. Enter `leasing-rac0` as the name. Enter `jdbc/leasing-rac0` as the JNDI name. Enter `oracle` as the database type. For the driver type, select Oracle Driver (Thin) for Oracle RAC Service-Instance connections, Versions:10 and later.

    Note: When creating the multi data sources for the leasing table, enter names in the format of *MultiDS*-rac0, *MultiDS*-rac1, and so on.

15. Click **Next**.

16. On JDBC Data Source Properties, select **Database Driver: Oracle's Driver (Thin) for RAC Service-Instance connections**.
17. Deselect **Supports Global Transactions**.
18. Click **Next**.
19. Enter the service name, database name, host port, and password for your leasing schema.
20. Click **Next**.
21. Click **Test Configuration** and verify that the connection works.
22. Click **Next**.
23. Target the data source to **oim_cluster** and **SOA cluster**.
24. Click **Finish**.
25. Select the data source you just created, for example `leasing-rac0`, and add it to the right screen.
26. Click **Create a New Data Source** for the second instance of your Oracle RAC database, target it to the oim_cluster and soa_cluster, repeating the steps for the second instance of your Oracle RAC database.
27. Add the second data source to your multi data source.
28. Click **Activate Changes**.

17.3.4 Editing Node Manager's Properties File

In this section, you edit Node Manager's properties file. This must be done for the Node Managers on the nodes where the servers are running, *IDM_PROVISIONED_HOST* and *IDM_SCALED_OUT_HOST*.

The `nodemanager.properties` file is located in the directory

SHARED_CONFIG_DIR`/nodemanager/`*hostname*

where *hostname* is the name of the host where the node manager is running.

Add the following properties to enable server migration to work properly:

- `Interface:`

  `Interface=eth0`

  This property specifies the interface name for the floating IP (for example, eth0).

  > **Note:** Do not specify the sub-interface, such as `eth0:1` or `eth0:2`. This interface is to be used without `:0` or `:1`. Node Manager's scripts traverse the different :*X*-enabled IPs to determine which to add or remove. For example, the valid values in Linux environments are `eth0`, `eth1`, `eth2`, `eth3`, `eth`*n*, depending on the number of interfaces configured.

- `NetMask:`

  `NetMask=255.255.255.0`

This property specifies the net mask for the interface for the floating IP. The net mask should the same as the net mask on the interface.

- `UseMACBroadcast`:

  `UseMACBroadcast=true`

  This property specifies whether to use a node's MAC address when sending ARP packets, that is, whether to use the `-b` flag in the `arping` command.

Verify in Node Manager's output (shell where Node Manager is started) that these properties are being used, or problems may arise during migration. You should see something like this in Node Manager's output:

```
StateCheckInterval=500
eth0=*,NetMask=255.255.255.0
UseMACBroadcast=true
```

Notes:

- `LogToStderr` must be set to true (in `node.propertes`), in order for you to see the properties in the output.
- The following steps are not required if the server properties (start properties) have been properly set and Node Manager can start the servers remotely.

1. If not done already, set the `StartScriptEnabled` property in the `nodemanager.properties` file to true. This is required to enable Node Manager to start the managed servers.
2. Start Node Manager on *`IDM_PROVISIONED_HOST`* and *`IDM_SCALED_OUT_HOST`* by running the `startNodeManagerWrapper.sh` script, which is located in the *`SHARED_CONFIG_DIR/nodemanager/hostname`* directory.

Note: When running Node Manager from a shared storage installation, multiple nodes are started using the same `nodemanager.properties` file. However, each node may require different NetMask or `Interface` properties. In this case, specify individual parameters on a per-node basis using environment variables. For example, to use a different interface (`eth3`) in HOST*n*, use the `Interface` environment variable by setting `JAVA_OPTIONS` to: `-DInterface=eth3`.

Then start Node Manager.

17.3.5 Setting Environment and Superuser Privileges for the wlsifconfig.sh Script

On Linux, you must set environment and superuser privileges for the `wlsifconfig.sh` script:

Ensure that your PATH environment variable includes the files listed in Table 17–1.

Table 17–1 Files Required for the PATH Environment Variable

File	Located in this directory
`wlsifconfig.sh`	*`MSERVER_HOME`*`/bin/server_migration`

Table 17–1 (Cont.) Files Required for the PATH Environment Variable

File	Located in this directory
wlscontrol.sh	*WL_HOME*/common/bin
nodemanager.domains	*SHARED_CONFIG_DIR*/nodemanager/HostName

For security reasons, sudo should be restricted to the subset of commands required to run the wlsifconfig.sh script. For example, perform the following steps to set the environment and superuser privileges for the wlsifconfig.sh script.

Note: Ask the system administrator for the appropriate sudo and system rights to perform this step.

Grant sudo privilege to the WebLogic user oracle with no password restriction, and grant execute privilege on the /sbin/ifconfig and /sbin/arping binaries.

Make sure the script is executable by the WebLogic user ('oracle'). The following is an example of an entry inside /etc/sudoers granting sudo execution privilege for oracle and also over ifconfig and arping.

To grant sudo privilege to the WebLogic user ('oracle') with no password restriction, and grant execute privilege on the /sbin/ifconfig and /sbin/arping binaries:

```
Defaults:oracle !requiretty
oracle ALL=NOPASSWD: /sbin/ifconfig,/sbin/arping
```

17.3.6 Configuring Server Migration Targets

In this section, you configure server migration targets. Configuring Cluster Migration sets the DataSourceForAutomaticMigration property to true.

To configure migration in a cluster:

1. Log in to the Oracle WebLogic Server Administration Console at: http://ADMIN.mycompany.com/console.
2. In the Domain Structure window, expand Environment and select Clusters. The Summary of Clusters page is displayed.
3. Click the cluster for which you want to configure migration (oim_cluster) in the Name column of the table.
4. Click the **Migration** tab.
5. Click **Lock and Edit**.
6. In the Candidate Machines for Migratetable Servers field, select the machine to which to allow migration and click the right arrow. In this case, select *IDM_PROVISIONED_HOST* and *IDM_SCALED_OUT_HOST*.
7. Select the data source to be used for automatic migration. In this case, select the leasing data source.
8. Click **Save**.
9. In the Domain Structure window of the Oracle WebLogic Server Administration Console, expand Environment and select Servers.
10. Select the server for which you want to configure migration.
11. Click the **Migration** tab.

12. Select **Automatic Server Migration Enabled** and click **Save**.
13. Click **Activate Changes**.
14. Repeat steps 2 to 13 for the SOA cluster.
15. Restart WebLogic Administration Server, Node Managers, and the servers for which server migration has been configured, as described in Section 10.9.1, "Starting and Stopping Components".

Note: If migration is only going to be allowed to specific machines, do not specify candidates for the cluster, but rather specify candidates only on a server per server basis.

17.3.7 Testing the Server Migration

In this section, you test the server migration. Perform these steps to verify that server migration is working properly:

To test from *IDM_PROVISIONED_HOST*:

1. Stop the *WLS_OIM_PROVISIONED_HOST* Managed Server. To do this, run this command:

   ```
   kill -9 pid
   ```

   where *pid* specifies the process ID of the Managed Server. You can identify the pid in the node by running this command:

   ```
   ps -ef | grep WLS_OIM_PROVISIONED_HOST
   ```

2. Watch the Node Manager console. You should see a message indicating that WLS_*OIM_PROVISIONED_HOST*'s floating IP has been disabled.
3. Wait for Node Manager to try a second restart of *WLS_OIM_PROVISIONED_HOST*. It waits for a fence period of 30 seconds before trying this restart.
4. Once Node Manager restarts the server, stop it again. Node Manager should now log a message indicating that the server will not be restarted again locally.

To test from *IDM_SCALED_OUT_HOST*:

1. Watch the local Node Manager console. After 30 seconds since the last try to restart *WLS_OIM_PROVISIONED_HOST* on *IDM_PROVISIONED_HOST*, Node Manager on *IDM_SCALED_OUT_HOST* should prompt that the floating IP for *WLS_OIM_PROVISIONED_HOST* is being brought up and that the server is being restarted in this node.
2. Access the OIM Console using the Virtual Host Name, for example: OIMVH1. Console URLs are provided in Section 10.9.2, "About Oracle Identity Management Console URLs".

Follow the previous steps to test server migration for the *WLS_OIM_SCALED_OUT_HOST*, *WLS_SOA_PROVISIONED_HOST*, and *WLS_SOA_SCALED_OUT_HOST* Managed Servers.

Table 17–2 shows the Managed Servers and the hosts they migrate to in case of a failure.

Table 17–2 Managed Server Migration

Managed Server	Migrated From	Migrated To
WLS_OIM_PROVISIONED_HOST	*IDM_PROVISIONED_HOST*	*IDM_SCALED_OUT_HOST*
WLS_OIM_SCALED_OUT_HOST	*IDM_SCALED_OUT_HOST*	*IDM_PROVISIONED_HOST*
WLS_SOA_PROVISIONED_HOST	*IDM_PROVISIONED_HOST*	*IDM_SCALED_OUT_HOST*
WLS_SOA_SCALED_OUT_HOST	*IDM_SCALED_OUT_HOST*	*IDM_PROVISIONED_HOST*

Verification From the Administration Console

Migration can also be verified in the Administration Console:

1. Log in to the Administration Console. Console URLs are provided in Section 10.9.2, "About Oracle Identity Management Console URLs".
2. Click **IDMDomain** on the left console.
3. Click the **Monitoring** tab and then the **Migration** sub tab.

   The Migration Status table provides information on the status of the migration.

> **Note:** After a server is migrated, to fail it back to its original node/machine, stop the Managed Server from the Oracle WebLogic Administration Console and then start it again. The appropriate Node Manager starts the Managed Server on the machine to which it was originally assigned.

17.3.8 Backing Up the Server Migration Configuration

Back up the database and the WebLogic domain, as described in Section 10.9.3, "Performing Backups During Installation and Configuration".

17.4 Setting Up Fail Over for the Administration Server

This section discusses how to fail over the Administration Server to IDMHOST2 and how to fail it back to IDMHOST1.

This section contains the following topics:

- Section 17.4.1, "Failing Over the Administration Server to IDMHOST2"
- Section 17.4.2, "Starting the Administration Server on IDMHOST2"
- Section 17.4.3, "Validating Access to IDMHOST2 Through Oracle HTTP Server"
- Section 17.4.4, "Failing the Administration Server Back to IDMHOST1"

17.4.1 Failing Over the Administration Server to IDMHOST2

If a node fails, you can fail over the Administration Server to another node. This section describes how to fail over the Administration Server from IDMHOST1 to IDMHOST2.

Assumptions:

- The Administration Server is configured to listen on `ADMINVHN.mycompany.com`, and not on `ANY` address.

- The Administration Server is failed over from IDMHOST1 to IDMHOST2, and the two nodes have these IP addresses:
  - IDMHOST1: `100.200.140.165`
  - IDMHOST2: `100.200.140.205`
  - ADMINVIP: `100.200.140.206`

    This is the Virtual IP address where the Administration Server is running, assigned to *interface*:*index* (for example, eth1:2), available in IDMHOST1 and IDMHOST2.
- The domain directory where the Administration Server is running in IDMHOST1 is on a shared storage and is mounted also from IDMHOST2.

> **Note:** NM in IDMHOST2 does not control the domain at this point, since `unpack/nmEnroll` has not been run yet on IDMHOST2. But for the purpose of AdminServer failover and control of the AdminServer itself, Node Manager is fully functional

- Oracle WebLogic Server and Oracle Fusion Middleware Components have been installed inIDMHOST2 as described in previous chapters. That is, the same path for *`IDM_ORACLE_HOME`* and *`MW_HOME`* that exists in IDMHOST1 is available in IDMHOST2.

The following procedure shows how to fail over the Administration Server to a different node, IDMHOST2.

1. Stop the Administration Server as described in Section 10.9.1, "Starting and Stopping Components."
2. Migrate the IP address to the second node.
   a. Run the following command as root on IDMHOST1 (where *x*:*y* is the current interface used by `ADMINVHN.mycompany.com`):

      ```
      /sbin/ifconfig x:y down
      ```

      For example:

      ```
      /sbin/ifconfig eth0:1 down
      ```

   b. Run the following command on IDMHOST2:

      ```
      /sbin/ifconfig interface:index IP_Address netmask netmask
      ```

      For example:

      ```
      /sbin/ifconfig eth0:1 100.200.140.206 netmask 255.255.255.0
      ```

      > **Note:** Ensure that the netmask and interface to be used match the available network configuration in IDMHOST2.

3. Update routing tables by using `arping`, for example:

   ```
   /sbin/arping -q -U -c 3 -I eth0 100.200.140.206
   ```

17.4.2 Starting the Administration Server on IDMHOST2

Perform the following steps to start Node Manager on IDMHOST2.

1. On IDMHOST2, mount the Administration Server domain directory if it is not already mounted. For example:

   ```
   mount /u01/oracle
   ```

2. Start Node Manager by using the following commands:

   ```
   cd WL_HOME/server/bin
   ./startNodeManager.sh
   ```

3. Stop the Node Manager by killing the Node Manager process.

   Note: Starting and stopping Node Manager at this point is only necessary the first time you run Node Manager. Starting and stopping it creates a property file from a predefined template. The next step adds properties to that property file.

4. Run the setNMProps.sh script to set the `StartScriptEnabled` property to `true` before starting Node Manager:

   ```
   cd ORACLE_COMMON_HOME/common/bin
   ./setNMProps.sh
   ```

   Note: You must use the `StartScriptEnabled` property to avoid class loading failures and other problems.

5. Start the Node Manager as described in Section 10.9.1, "Starting and Stopping Components."

6. Start the Administration Server on IDMHOST2.

   ```
   cd ORACLE_COMMON_HOME/common/bin
   ./wlst.sh
   ```

   Once in the WLST shell, execute the following commands:

   ```
   nmConnect('admin','Admin_Password', 'IDMHOST2','5556',
   'IDMDomain','/u1/oracle/config/domains/IDMDomain')
   nmStart('AdminServer')
   ```

7. Test that you can access the Administration Server on IDMHOST2 as follows:

   a. Ensure that you can access the Oracle WebLogic Server Administration Console at:

      `http://ADMINVHN.mycompany.com:7001/console.`

   b. Check that you can access and verify the status of components in the Oracle Enterprise Manager at: `http://ADMINVHN.mycompany.com:7001/em`.

17.4.3 Validating Access to IDMHOST2 Through Oracle HTTP Server

Perform the same steps as in Section 10.8.1.1, "Verify Connectivity" This is to check that you can access the Administration Server when it is running on IDMHOST2.

17.4.4 Failing the Administration Server Back to IDMHOST1

This step checks that you can fail back the Administration Server, that is, stop it on IDMHOST2 and run it on IDMHOST1. To do this, migrate ADMINVHN back to IDMHOST1 node as described in the following steps.

1. Ensure that the Administration Server is not running. If it is, stop it from the WebLogic console, or by running the command `stopWeblogic.sh` from *ASERVER_HOME*`/bin`.
2. On IDMHOST2, unmount the Administration server domain directory. For example:

   ```
   umount /u01/oracle
   ```

3. On IDMHOST1, mount the Administration server domain directory. For example:

   ```
   mount /u01/oracle
   ```

4. Disable the `ADMINVHN.mycompany.com` virtual IP address on IDMHOST2 and run the following command as `root` on IDMHOST2:

   ```
   /sbin/ifconfig x:y down
   ```

   where *x*`:`*y* is the current interface used by `ADMINVHN.mycompany.com`.

5. Run the following command on IDMHOST1:

   ```
   /sbin/ifconfig interface:index 100.200.140.206 netmask 255.255.255.0
   ```

   Note: Ensure that the netmask and interface to be used match the available network configuration in IDMHOST1

6. Update routing tables by using arping. Run the following command from IDMHOST1.

   ```
   /sbin/arping -q -U -c 3 -I interface 100.200.140.206
   ```

7. If Node Manager is not already started on IDMHOST1, start it, as described in Section 10.9.1, "Starting and Stopping Components."
8. Start the Administration Server again on IDMHOST1.

   ```
   cd ORACLE_COMMON_HOME/common/bin
   ./wlst.sh
   ```

   Once in the WLST shell, execute

   ```
   nmConnect(admin,'Admin_Pasword, IDMHOST1,'5556',
        'IDMDomain','/u01/oracle/config/domains/IDMDomain'
   nmStart('AdminServer')
   ```

9. Test that you can access the Oracle WebLogic Server Administration Console at:

   ```
   http://ADMINVHN.mycompany.com:7001/console
   ```

   where `7001` is *WLS_ADMIN_PORT*

10. Check that you can access and verify the status of components in the Oracle Enterprise Manager at:

    ```
    http://ADMINVHN.mycompany.com:7001/em
    ```

17.5 What to Do Next

If you need information regarding scale out and server migration for Oracle Fusion Applications, go to Chapter 18. Otherwise, go to the chapter that corresponds to the product offering that is installed.

18

Completing Conditional Common High Availability Post-Installation Tasks for Oracle Fusion Applications

This chapter describes the conditional common high availability post-installation tasks for Oracle Fusion Applications that you should review and complete as required.

This chapter contains the following sections:

18.1 Introduction to Completing Conditional Common High Availability Post-Installation Tasks for Oracle Fusion Applications

After you have successfully completed the conditional common post-installation tasks review and perform the following conditional common high availability tasks.

Some components in the Oracle Fusion Applications environment are dependent on one another. Therefore, it is important to start and stop components in the proper order. In the course of normal IT operations, common operations include shutting down computers and starting them back up. Therefore, it is crucial to start and stop Oracle Fusion Applications in a sequential manner. For more information, see "Starting and Stopping the Entire Oracle Fusion Applications Environment" in the *Oracle Fusion Applications Administrator's Guide*.

18.2 Scaling Oracle Fusion Applications

The Oracle Fusion Applications topology is highly scalable, and can be scaled up or out. When you scale up the topology, you add a new Managed Server to provisioning hosts that are already running one or more Managed Servers. When you scale out the topology, you add one or more instances of Managed Servers to new hosts.

18.2.1 Scaling Out Oracle HTTP Server

The first Oracle HTTP Server (`WEBHOST1`) was configured during the provisioning process. This section describes how to scale out Oracle HTTP Server to additional hosts.

18.2.1.1 Prerequisites for Performing the Scale Out

Before you scale out Oracle HTTP Server to additional hosts, ensure you do the following:

1. Reboot *WEBHOST2* to start the scaleout where *WEBHOST2* is a clean machine.

   > **Note:** *WEBHOST2* and *WEBHOST1* should be running the same version of the operating system certified for Oracle Fusion Applications as other provisioning hosts.

2. On *WEBHOST2*, create the directory *REPOSITORY_LOCATION*/installers with the same user that installed Oracle HTTP Server on *WEBHOST1*.
3. Copy or ftp the entire content of the following directories from installers and jdk6 to *WEBHOST2*. Depending on network access available to *WEBHOST2*, you can copy or ftp from *REPOSITORY_LOCATION* or *WEBHOST1*:
   - *REPOSITORY_LOCATION*/installers/webgate
   - *REPOSITORY_LOCATION*/installers/webtier
   - *REPOSITORY_LOCATION*/jdk6

18.2.1.2 Installing the Oracle Web Tier

To install Oracle Web Tier, do the following:

1. Run the following command to install Oracle Web Tier on *WEBHOST2*:

   REPOSITORY_LOCATION/installers/webtier/Disk1/runInstaller

   The Oracle Fusion Middleware 11*g* Oracle Web Tier Utilities Configuration Welcome screen opens.
2. Specify the same values for inventory directory and operating system group as those set for *WEBHOST1*. (These values can be found in the /etc/oraInst.loc file that you specified for *WEBHOST1*.)

   Click **OK**.
3. Follow the instructions in the Inventory Location Confirmation Dialog box to execute the createCentralInventory.sh script as root user, and then click **OK** to dismiss the dialog box.
4. Select the appropriate options, and then click **Next** to start the installation.

   The Select Installation Type screen opens.
5. Select **Install Software - Do Not Configure** and click **Next**.

   The Prerequisite Checks screen opens.

   After all prerequisite checks have successfully completed, click **Next**. The Specify Installation Location screen opens. (If any prerequisite check fails, you first must resolve the issue, and then click **Retry** to run the prerequisite checks again.)

   Select the path to Oracle Middleware Home and enter a name for the home directory. For example, /u01/oracle/products/webtier_mwhome/. Click **Next**.
6. In the Specify Security Updates screen, do the following:
   - Enter an email address
   - Indicate that you wish to receive security updates from My Oracle Support

- Enter your My Oracle Support password

Click **Next**. The Installation Summary screen opens.

7. Click **Install**. The Installation Progress screen opens.

   Click **Next** when the installation has finished. The Installation Complete screen opens.

   Click **Finish**.

8. Review the directory structure that has been created:

   ```
   cd APPLICATIONS_BASE/webtier_mwhome
   ```

18.2.1.3 Installing Oracle Web Tier Patches

> **Note:** If any directory under *REPOSITORY_LOCATION*/installers/webtier/prepatch and/or *REPOSITORY_LOCATION*/installers/webtier/patch exists, perform the steps in this section. If no directory exists, perform only Steps 1 and 3 on both *WEBHOST1* and *WEBHOST2* (skip Step 2).

To install Web Tier patches, do the following:

1. Set or change the environment variable $*ORACLE_HOME* to *APPLICATIONS_BASE*/webtier_mwhome/webtier/, as shown in the following example:

   ```
   export ORACLE_HOME=APPLICATIONS_BASE/webtier_mwhome/webtier
   ```

2. To install the patches:

   a. If a subfolder exists in the prepatch folder of the Web Tier installer, change directory to the prepatch folder and run the following command:

      ```
      ORACLE_HOME/OPatch/opatch napply
      ```

   b. Change directory to the patch folder and run the command again.

3. Make sure the same patches are installed on both *WEBHOST1* and *WEBHOST2* by running the following command on both *WEBHOST1* and *WEBHOST2*, comparing the output to ensure the patches are the same:

   ```
   APPLICATIONS_BASE/webtier_mwhome/webtier/OPatch/opatch lsinventory
   ```

18.2.1.4 Configuring Oracle Web Tier

To configure Oracle Web Tier, do the following:

1. Begin configuring the Oracle Web Tier components:

   ```
   cd APPLICATIONS_BASE/webtier_mwhome/webtier/bin

   run ./config.sh
   ```

   The Oracle Fusion Middleware 11*g* Oracle Web Tier Utilities Configuration Welcome screen opens.

   Click **Next**. The Configure Components screen opens.

2. Select **Oracle HTTP Server** and **Associate Selected Components with WebLogic Domain**.

3. Click **Next**. The Specify WebLogic Domain screen opens.
4. Enter the following:
   - Common domain host name; for example, *PROVISIONED_HOST*
   - Common domain port number; for example, COMMONDOMAIN ADMIN PORT
   - Common domain Administration Server user name
   - Common domain Administration Server password

   Note: Associate Oracle HTTP Server with the CommonDomain that Provisioning installed.
5. Click **Next**. The Specify Component Details screen opens.
6. Do the following:
   - Select the instance home location; for example, APPLICATIONS_CONFIG/CommonDomain_webtier1
   - Enter the instance name; for example, CommonDomain_webtier1
   - Enter the Oracle HTTP Server component name; for example ohs2
7. Click **Next**. The Configure Ports screen opens.

   Note: Copy the staticports.ini file from repository/installers/webtier/Disk1/stage/Response to *ORACLE_BASE*/staticports.ini.
8. Select **Specify Ports using Configuration file** and click **View/Edit**.

   In the text field that displays enter OHS port = 10601 (or whichever OHS Port was used on *PROVISIONED_HOST* during Provisioning).

   Click **Save** and then click **Next**.

   The Specify Security Updates screen opens.
9. Do the following:
   - Enter an email address
   - Indicate that you wish to receive security updates from My Oracle Support
   - Enter your My Oracle Support password
10. Click **Next**. The Installation Summary screen opens.
11. Click **Configure** to install the configuration. The Configuration Progress screen opens.
12. Click **Next**.

    When the installation completes, the Installation Complete screen opens.
13. Click **Finish**.
14. Copy or ftp the FusionVirtualHost files from *WEBHOST1* to *WEBHOST2*:

    WEBHOST1> *APPLICATIONS_CONFIG*/CommonDomain_webtier/config/OHS/ohs1/moduleconf

    to

```
WEBHOST2> APPLICATIONS_CONFIG/CommonDomain_webtier1/config/OHS/ohs2/moduleconf/
```

15. After the copy is complete, replace all occurrences of *WEBHOST1* with *WEBHOST2* in all of the files with names ending in `.conf` that you copied to *WEBHOST2*.
16. Start the Oracle HTTP Server instance:

```
WEBHOST2> cd APPLICATIONS_CONFIG/CommonDomain_webtier1/bin
WEBHOST2> ./opmnctl startall
```

> **Note:** If you get an error message saying that the `FusionSSL.conf` file is missing, copy the file from *APPLICATIONS_CONFIG*`/CommonDomain_webtier/config/OHS/ohs1` on *WEBHOST1* to the *APPLICATIONS_CONFIG*`/CommonDomain_webtier1/config/OHS/ohs2` folder on *WEBHOST2*.

18.2.1.5 Installing WebGate

To install WebGate on *WEBHOST2*, do the following:

1. From *REPOSITORY_LOCATION*`/installers/webgate/Disk1`, start the WebGate installation:

```
./runInstaller -jreLoc REPOSITORY_LOCATION/jdk6
```

2. When the Welcome screen opens, click **Next**. The Prerequisite Checks screen opens.
3. When the checking process completes, click **Next**. The Installation Location screen opens.
4. Enter an Oracle Middleware Home location Oracle Home Directory, *APPLICATIONS_BASE*`/webtier_mwhome`, and click **Next**. The GCC Library Details screen opens.
5. Enter an Oracle Middleware Home location Oracle Home Directory, *APPLICATIONS_BASE*`/webtier_mwhome`, and click **Next**. The Installation Summary screen opens.
6. Click **Save** if you wish to save the response file. Click **Install** to start the installation. Following an interim screen, the Installation Progress screen opens.

   During installation, a progress screen opens.
7. When the installation finishes, click **Next**. The Installation Complete screen opens.
8. Click **Save** if you wish to save the installation details. Click **Finish** to complete the WebGate installation.

18.2.1.6 Installing WebGate Patches

> **Note:** If any directory under *REPOSITORY_LOCATION*`/installers/webgate/prepatch` and/or *REPOSITORY_LOCATION*`/installers/webgate/patch` exists, perform the steps in this section. If no directory exists, perform only Steps 1 and 3 on both *WEBHOST1* and *WEBHOST2* (skip Step 2).

To install WebGate patches, do the following:

1. Set or change the environment variable $*ORACLE_HOME* to *APPLICATIONS_BASE*/webtier_mwhome/webgate/, as shown in the following example:

   ```
   export ORACLE_HOME=APPLICATIONS_BASE/webtier_mwhome/webgate
   ```

2. To install the patches:

   a. If a subfolder exists in the prepatch folder of the WebGate installer, change directory to the prepatch folder and run the following command:

      ```
      ORACLE_HOME/OPatch/opatch napply
      ```

   b. Change directory to the patch folder and run the command again.

3. Make sure the same patches are installed on both *WEBHOST1* and *WEBHOST2* by running the following command on both hosts:

   ```
   APPLICATIONS_BASE/webtier_mwhome/webgate/OPatch/opatch lsinventory
   ```

18.2.1.7 Configuring WebGate

After installing WebGate, do the following:

1. Append environment variable LD_LIBRARY_PATH with the Web Tier library path *APPLICATIONS_BASE*/webtier_mwhome/webtier/lib:

   ```
   WEBHOST2> export LD_LIBRARY_PATH=APPLICATIONS_BASE/webtier_mwhome/
   webtier/lib:$LD_LIBRARY_PATH
   ```

2. Run the commands that follow.

   Note that the usage of the deployWebGateInstance.sh script is:

   ```
   # Usage: deployWebGateInstance.sh -w <WebGate_instancedir> -oh WebGate_Oracle_
   Home

   $  cd APPLICATIONS_BASE/webtier_mwhome/webgate/webgate/ohs/tools/
   deployWebGate

   $ ./deployWebGateInstance.sh -w APPLICATIONS_CONFIG/CommonDomain_webtier1/
   config/OHS/ohs2 -oh APPLICATIONS_BASE/webtier_mwhome/webgate

   $  cd APPLICATIONS_BASE/webtier_mwhome/webgate/webgate/ohs/tools/setup/
   InstallTools

   $ ./EditHttpConf -w APPLICATIONS_CONFIG/CommonDomain_webtier1/config/OHS/
   ohs2 -oh APPLICATIONS_BASE/webtier_mwhome/webgate -o webgate.conf
   ```

3. Do the following on *WEBHOST1*:

   a. From *APPLICATIONS_CONFIG*/CommonDomain_webtier/config/OHS/ohs1/webgate/config, copy the following to *APPLICATIONS_CONFIG*/CommonDomain_webtier1/config/OHS/ohs2/webgate/config on *WEBHOST2*:

      ```
      "ObAccessClient.xml","cwallet.sso","password.xml"
      ```

   b. From *APPLICATIONS_CONFIG*/CommonDomain_webtier/config/OHS/ohs1/webgate/config/simple, copy the following to *APPLICATIONS_CONFIG*/CommonDomain_webtier1/config/OHS/ohs2/webgate/config/simple on *WEBHOST2*:

      ```
      "aaa_key.pem","aaa_cert.pem"
      ```

4. Restart Oracle HTTP Server:

```
WEBHOST2> cd APPLICATIONS_CONFIG/CommonDomain_webtier1/bin
WEBHOST2> ./opmnctl stopall
WEBHOST2> ./opmnctl startall
```

Oracle HTTP Server scaleout is now complete, and *WEBHOST1* and *WEBHOST2* should behave identically.

18.2.1.8 Validating Oracle HTTP Server on WEBHOST2

To validate after the installation is complete:

1. Check that it is possible to access the Oracle HTTP Server home page on *WEBHOST1* and *WEBHOST2* using the following URLs:
   - `http://webhost1.mycompany.com:10601`
   - `http://webhost2.mycompany.com:10601`
2. Stop *WEBHOST1*:

```
WEBHOST1> cd APPLICATIONS_CONFIG/CommonDomain_webtier/bin

WEBHOST1> ./opmnctl stopall
```

3. Access the following URLs to ensure that the WebLogic Administration console of applicable Oracle Fusion Applications domain is visible, and that Oracle HTTP Server on *WEBHOST2* is configured correctly:

> **Note:** The host and port of these URLs come from the internal virtual hosts and ports listed in the Virtual Hosts Configuration screen of the Oracle Fusion Applications Provision Wizard. You can also find the URLs in the provisioning summary file. (For more information, see the "Installation Complete" row in Table 13–1, " Provisioning a New Applications Environment".) Depending on the provisioning offerings that you selected, you may not have all of the domains.

   - `http://crminternal.mycompany.com/console`
   - `http://fininternal.mycompany.com/console`
   - `http://hcminternal.mycompany.com/console`
   - `http://scminternal.mycompany.com/console`
   - `http://commoninternal.mycompany.com/console`
   - `http://biinternal.mycompany.com/console`
   - `http://icinternal.mycompany.com/console`
   - `http://prjinternal.mycompany.com/console`
   - `http://prcinternal.mycompany.com/console`
4. Access the following URLs to ensure that the WebLogic Administration console of applicable Oracle Fusion Applications domain is visible, and that Oracle HTTP Server on *WEBHOST2* is configured correctly:

Note: The host and port of these URLs come from the external virtual hosts and ports listed in the Virtual Hosts Configuration screen of the Oracle Fusion Applications Provision Wizard. Depending on the provisioning offerings that you selected, you may not have all of the domains.

  - https://crmexternal.mycompany.com/sales/faces/mooOpportunityHome
  - https://crmexternal.mycompany.com/crmPerformance/faces/TerritoriesMain
  - https://crmexternal.mycompany.com/contractManagement/faces/ContractsDashboard
  - https://crmexternal.mycompany.com/customer/faces/CustomerCtrWorkarea
  - https://finexternal.mycompany.com/ledger/faces/LedgerWorkArea
  - https://finexternal.mycompany.com/payables/faces/PaymentLandingPage
  - https://prcexternal.mycompany.com/procurement/faces/PrcPoPurchasingWorkarea
  - https://prjexternal.mycompany.com/projectsFinancials/faces/PRJProjectWorkarea
  - https://commonexternal.mycompany.com/homePage/faces/AtkHomePageWelcome
  - https://biexternal.mycompany.com/analytics
  - https://icexternal.mycompany.com/incentiveCompensation/faces/IcCnCompPlanWorkarea

5. Run the following commands:

```
WEBHOST1> cd APPLICATIONS_CONFIG/CommonDomain_webtier/bin

WEBHOST1> ./opmnctl startall
```

18.2.2 Scaling Out Node Manager

This section describes how to setup and configure Node Manager to a new host to be used as a scaled-out host.

18.2.2.1 Prerequisites for Setting Up Node Manager

Before setting up Node Manager, ensure the following:

- You are starting with a clean machine (denoted as SCALED_OUT_HOST), if it is the first time it is being set up
- The `/etc/hosts` file has proper entries. To verify this from the clean machine, ping the hosts listed in `/etc/hosts` files with the fully qualified name of the hosts.
- The user created on *SCALED_OUT_HOST* to perform the scale out should be the same as the user on *PROVISIONED_HOST*
- The directory structure *APPLICATIONS_BASE* is mounted on *SCALED_OUT_HOST* and it is the same shared file system as used by *PROVISIONED_HOST*
- The directory structure *APPLICATIONS_CONFIG*`nodemanager` on *SCALED_OUT_HOST* has been created

- Provisioning the initial Oracle Fusion Applications environment on *PROVISIONED_HOST* has already completed and verified

18.2.2.2 Setting Up Node Manager for SCALED_OUT_HOST

Do the following:

1. Run the following command:

   ```
   SCALED_OUT_HOST> cd APPLICATIONS_CONFIG/nodemanager
   ```

2. In the `nodemanager` directory, copy the content of the node-specific directory to *SCALED_OUT_HOST*. In this case, *PROVISIONED_HOST* is the node-specific directory.

   ```
   SCALED_OUT_HOST> cp -r PROVISIONED_HOST SCALED_OUT_HOST
   ```

3. Change directory to *SCALED_OUT_HOST*. You should see the following files:

   ```
   nm_data.properties   nodemanager.log   startNodeManagerWrapper.sh
   nodemanager.domains  nodemanager.properties
   ```

   Note: Manually delete any lock files that may be present. For example, `nodemanager.log.lck`.

4. In the `nodemanager.domains` file, edit all the domain paths that are local to *SCALED_OUT_HOST*. For example, *Domain*=/u02/local/oracle/config/domains/*SCALED_OUT_HOST*/*domain_name*.

   Note: In this chapter, replace *domain_name* with the domain-specific syntax. For example, *CRMDomain*, *FINDomain*, *HCMDomain*, and so on.

   Note: Because the Oracle Business Intelligence domain is a bit different, an example path would be `BIDomain=/u02/local/oracle/config/domains/`*PROVISIONED_HOST*`/BIDomain`.

5. In the `startNodeManagerWrapper.sh` file, change `NM_HOME` to *APPLICATIONS_CONFIG*`/nodemanager/`*SCALED_OUT_HOST*.

6. In the `nodemanager.properties` file:

   - Add or modify the following lines:

     ```
     KeyStores=CustomIdentityAndCustomTrust
     CustomIdentityKeyStoreFileName=APPLICATIONS_CONFIG/keystores/
     SCALED_OUT_HOST_fusion_identity.jks
     CustomIdentityPrivateKeyPassPhrase=keypassword
     CustomIdentityAlias=SCALED_OUT_HOST_fusion
     ```

     Note: *keypassword* is the password given in the provisioning response file for the Oracle Fusion Applications Administration user.

     Since the passwords in the response and plan files are encrypted, take note of or save the Node Manager password you enter when creating the provisioning response file.

- Ensure that the path to the local machine `/u02/local/oracle/nodemanager/` exists, and that the `LogFile` value is pointing to `/u02/local/oracle/nodemanager/`*`SCALED_OUT_HOST`*`.log`.
- Ensure that the path for `DomainsFile` and `NodeManagerHome` are correct for *`SCALED_OUT_HOST`*.

18.2.2.3 Creating the Identity Keystore on SCALED_OUT_HOST

Provisioning has created the identity keystore *`PROVISIONED_HOST`*`_fusion_identity.jks` for *`PROVISIONED_HOST`*. Subsequently, the identity keystore *`SCALED_OUT_HOST`*`_fusion_identity.jks` must be created for *`SCALED_OUT_HOST`*.

Do the following to create the keystore:

1. Change directory to *`APPLICATIONS_CONFIG`*`/keystores`.

   Ensure the *`PROVISIONED_HOST`*`_fusion_identity.jks` and `fusion_trust.jks` files are present.

2. Back up `fusion_trust.jks` to `fusion_trust.jks.org`.

3. Run the following command to set the CLASSPATH:

   ```
   SCALED_OUT_HOST> source APPLICATIONS_BASE/fusionapps/wlserver_10.3/server/
   bin/setWLSEnv.sh
   ```

   Ensure that the CLASSPATH has been set:

   ```
   SCALED_OUT_HOST> which keytool
   ```

   The output should point to the *`APPLICATIONS_BASE`*`/fusionapps/jdk6/jre/bin/keytool`.

4. Run the following command to create the keypair for *`SCALED_OUT_HOST`*`_fusion_identity.jks`:

   ```
   SCALED_OUT_HOST> keytool -genkeypair -keyalg RSA
   -alias SCALED_OUT_HOST_fusion -keypass
   keypassword -keystore SCALED_OUT_HOST_fusion_identity.jks
   -storepass keystorepassword
   -validity 180 -dname 'CN=SCALED_OUT_HOST, OU=defaultOrganizationUnit,
   O=defaultOrganization, C=US'
   ```

   where

   - *`keystorepassword`* is the password given in the *`APPLICATIONS_BASE`*`/provisioning/plan/provisioning.plan` file
   - *`keypassword`* is the password given in the *`APPLICATIONS_BASE`*`/provisioning/plan/provisioning.plan` file

   Notes:

   - It is recommended to keep the commands in a file and then execute it.
   - Since the passwords in the response and plan files are encrypted, take note of or save the Node Manager password you enter when creating the provisioning response file.

5. Run the following command to export the certificates:

```
SCALED_OUT_HOST> keytool -exportcert -alias SCALED_OUT_HOST_fusion
-keystore SCALED_OUT_HOST_fusion_identity.jks
-storepass keystorepassword -rfc -file /tmp/appIdentityKeyStore.jks
```

Note: If the alias *SCALED_OUT_HOST*_fusion exists, run this command to delete it:

```
keytool -delete -alias SCALED_OUT_HOST_fusion
-keystore fusion_trust.jks -storepass keystorepassword
```

The following command will display the certificates in the trust keystore:

```
keytool -list -keystore fusion_trust.jks -storepass
keystorepassword
```

6. Run the following command to import the certificates:

```
SCALED_OUT_HOST> keytool -importcert -noprompt -alias
SCALED_OUT_HOST_fusion -file /tmp/appIdentityKeyStore.jks
-keystore fusion_trust.jks -storepass keystorepassword
```

7. Verify that the file *SCALED_OUT_HOST*_fusion_identity.jks has been created in the directory *APPLICATIONS_CONFIG*/keystores directory.
8. Start Node Manager on *SCALED_OUT_HOST* by running the following command:

```
APPLICATIONS_CONFIG/nodemanager/SCALED_OUT_HOST/startNodeManagerWrapper.sh &
```

Note: The & in the command runs the script in the background.

18.2.3 Performing Scale-Out Tasks Common to All Domains

There are the scale-out tasks that are common to all Oracle Fusion Applications Managed Servers in all domains (Common, Oracle Fusion CRM, Oracle Fusion Financials, Oracle Fusion Human Capital Management, Oracle Fusion Incentive Compensation, Oracle Fusion Project Portfolio Management, Oracle Fusion Procurement, and Oracle Fusion Supply Chain Management) except Oracle Business Intelligence. These tasks are the following:

- Starting *SCALED_OUT_HOST* Node Manager in SSL mode
- Adding a new machine in the Oracle WebLogic Server console
- Packing and unpacking the Managed Server domain home
- Cloning Managed Servers and assigning them to SCALED_OUT_HOST
- Configuring Oracle HTTP Server
- Configuring server migration for the Managed Servers
- Validating the system

For specific information about scaling the Oracle Business Intelligence domain, see Section 18.2.7, "Scaling Out the Oracle Business Intelligence Domain."

18.2.3.1 Starting SCALED_OUT_HOST Node Manager in SSL Mode

To start Node Manager in the Secure Sockets Layer (SSL) mode, follow the instructions in Section 18.2.2, "Scaling Out Node Manager."

18.2.3.2 Adding a New Machine In the Oracle WebLogic Server Console

To add a new machine:

1. Stop the domain's Administration Server:

   ```
   PROVISIONED_HOST> APPLICATIONS_CONFIG/domains/PROVISIONED_HOST/domain_
   name/bin/stopWebLogic.sh
   ```

2. Set the following environment variable on *SCALED_OUT_HOST*:

   ```
   export WLST_PROPERTIES="-Dweblogic.security.SSL.trustedCAKeyStore=ORACLE_BASE/
   config/keystores/fusion_trust.jks"
   ```

3. Start the domain's Administration Server:

   ```
   SCALED_OUT_HOST> APPLICATIONS_BASE/fusionapps/wlserver_10.3/common/bin/wlst.sh

   SCALED_OUT_HOST> nmConnect(username='username', password='password',
   domainName='domain_name', host='PROVISIONED_HOST',port='5556',
   nmType='ssl', domainDir='APPLICATIONS_CONFIG/domains/
   PROVISIONED_HOST/domain_name')

   SCALED_OUT_HOST> nmStart('AdminServer')
   SCALED_OUT_HOST> exit ()
   ```

   Note: The *username* and *password* used in the `nmConnect` are the Node Manager credentials (user name and password) specified when creating the provisioning response file.

4. Log in to the Administration Server:
   `http://domaininternal.mycompany.com/console`.
5. Navigate to ***Domain_Name*** **> Environment > Machines**.

   LocalMachine is located in the right-hand pane.
6. In the left-hand pane, click **Lock & Edit**.
7. In the right-hand pane, first click **New** to add the remote machine, and then specify the following:
   - Name - enter *SCALED_OUT_HOST*
   - Machine operating system - Unix
8. Click **Next**.
9. In the window that opens, set the following attributes:
   - Type - SSL
   - Listen Address - <*SCALED_OUT_HOST*>

     Note: The "localhost" default value here is wrong.

   - Listen port - 5556
10. Click **Finish** and activate the changes.

18.2.3.3 Packing and Unpacking the Managed Server Domain Home to SCALED_OUT_HOST

Since the *PROVISIONED_HOST* domain directory file system is also available from *SCALED_OUT_HOST*, both the `pack` and `unpack` commands can be executed from *SCALED_OUT_HOST*.

To pack and unpack the Managed Server domain home:

1. Change directory to *APPLICATIONS_BASE*`/fusionapps/oracle_common/common/bin`.
2. Run the `pack` command:

   ```
   SCALED_OUT_HOST> ./pack.sh -managed=true -domain=APPLICATIONS_LOCAL_CONFIG/
   domains/PROVISIONED_HOST/domain_name -template=APPLICATIONS_BASE/
   user_templates/domain_name_managed.jar -template_name="
   domain_name_Managed_Server_Domain"
   ```

3. Ensure that *APPLICATIONS_LOCAL_CONFIG* `/domains/`*SCALED_OUT_HOSTdomain_name* is empty, and then run the `unpack` command:

   ```
   SCALED_OUT_HOST> ./unpack.sh -domain=APPLICATIONS_LOCAL_CONFIG/domains/
   SCALED_OUT_HOST/domain_name -template=APPLICATIONS_BASE_BASE/user_templates/
   domain_name_managed.jar
   ```

   Here, *APPLICATIONS_LOCAL_CONFIG* is local to *SCALED_OUT_HOST*.

18.2.3.4 Cloning Managed Servers and Assigning Them to SCALED_OUT_HOST

Note: The following naming conventions are used in the procedure that follows:

- *ManagedServerName*_1 is the name of the Managed Server to be cloned.
- *ClonedManagedServer* is the name you give to the Managed Server that you are cloning. For consistency, its name should follow the same naming convention as *ManagedServerName*, in this format: *ClonedManagedServer_n*, where *n* is a number starting with 2, and is incremented when you clone multiple instances. For example, *ClonedManagedServer*_3, *ClonedManagedServer*_4, and so on.

To add a Managed Server and assign it to *SCALED_OUT_HOST*:

1. Log in to the Administration Server: `http://`*domain_name*`internal.mycompany.com/console`.

   (*domain_name* is the domain containing the Managed Server that you want to clone.)
2. Navigate to ***Domain_Name*** **> Environment > Servers**.
3. Switch to **Lock & Edit** mode.
4. Select the ***ManagedServerName*_1** check box and then click **Clone**.
5. Specify the following Server Identity attributes:
   - Server Name - *ClonedServerName* _2

Note: To ensure consistency in naming, copy the name of the server shown in **Server Identity** and paste it into the **Server Name** field. Then change the number to "_2".

- Server Listen Address - <*SCALED_OUT_HOST*>
- Server Listen Port - leave "as is"

6. Click **OK**.

   You now should see the newly cloned server, *ClonedServerName*`_2`.

7. Click ***ClonedServerName*_2** and change the following attributes:
   - Machine - <*SCALED_OUT_HOST*>
   - Cluster Name - accept the default, *ClonedServerName*Cluster

   Note: Ensure that this cluster name is the same as the cluster name of the original Managed Server.

8. Click **Save** and then **Activate Changes**.
9. Navigate to ***Domain_Name*** **> Environment > Servers**.
10. From the **Name** column, click the ***ClonedServerName*_2** scaled-out server link.
11. Click **Lock & Edit**, and then select the **Configuration** tab.
12. Select the **Keystores** tab, and ensure that the keystores value is **Custom Identity and Custom Trust**.
13. Do the following:
    a. Change the Custom Identity Keystore path to point to the *APPLICATIONS_CONFIG*`/keystores/`*SCALED_OUT_HOST*`_fusion_identity.jks` file.
    b. Leave the Custom Identity Keystore type blank.
    c. Change the Custom Identity Keystore Passphrase entry. This should be the same as the *keystorepassword* field described in the first bullet in Step 4 in Section 18.2.2.3, "Creating the Identity Keystore on SCALED_OUT_HOST."
    d. Re-enter the Confirm Custom Identity Keystore Passphrase.
    e. Ensure that the Confirm Custom Trust Keystore path is pointing to the *APPLICATIONS_CONFIG*`/keystores/fusion_trust.jks` file.
    f. Leave the Custom Trust Keystore type blank.
    g. Change the Custom Trust Keystore Passphrase entry. This should be the same as the *keystorepassword* field described in the first bullet in Step 4 in Section 18.2.2.3, "Creating the Identity Keystore on SCALED_OUT_HOST."
    h. Re-enter the Custom Trust Keystore Passphrase.
    i. Click **Save**.
14. Select the **SSL** tab.
    a. Make sure that Identity and Trust Locations is set to **Keystores**.
    b. Change the Private Key Alias to *SCALED_OUT_HOST*`_fusion`.

c. Change the Private Key Passphrase to the *keypassword*, as described in the second bullet in Step 4 in Section 18.2.2.3, "Creating the Identity Keystore on SCALED_OUT_HOST."

d. Re-enter the *keypassword* from Step c for the Confirm Private Key Passphrase.

e. Click **Save**.

15. Select the **Server Start** tab.

    Change the Arguments to reflect the name of your cloned Managed Server and make sure the server group is the correct cluster name. For example, you should see the following:

    ```
    -DJDBCProgramName=DS/domain_name/ClonedServerName_2
    -Dserver.group=ClonedServerNameCluster
    ```

    Click **Save**.

16. Select the **Logging** tab, and then select the **HTTP** tab.

17. Do the following:

    a. Change the Log file name to `logs/access.log.%yyyyMMdd%`.

    b. Change the rotation type to **By Time**.

    c. Leave the **Limit number of retained files** option unchecked.

    d. Leave the **Rotate log file on startup** option unchecked.

    e. Click **Save**.

    f. Expand **Advanced**.

    g. Change the format to **Extended**.

    h. Change the extended logging format fields to the following:

    ```
    date time time-taken cs-method cs-uri
    sc-status sc(X-ORACLE-DMS-ECID)
    cs(ECID-Context) cs(Proxy-Remote-User)
    cs(Proxy-Client-IP)
    ```

    i. Click **Save**.

18. Click **Activate Changes**.

19. Repeat Steps 2 to 18 for all the Managed Servers on this domain.

20. Run the newly created Managed Servers:

    a. Log in to the Administration Server: `http://domain_nameinternal.mycompany.com/console`.

    b. Navigate to ***Domain_Name*** **> Environment > Servers > Control**.

    c. Select the newly created Managed Servers and click **Start**.

    d. Navigate to ***Domain_Name*** **> Environment > Servers** and check the **State** to verify that the newly created Managed Servers are running.

18.2.3.5 Configuring Oracle HTTP Server

To configure Oracle HTTP Server:

1. Do the following:

- On *WEBHOST1*, change directory to *APPLICATIONS_CONFIG*/CommonDomain_webtier/config/OHS/ohs1/moduleconf
- On *WEBHOST2*, change directory to *APPLICATIONS_CONFIG*/CommonDomain_webtier1/config/OHS/ohs2/moduleconf

2. Copy FusionVirtualHost_*domain*.conf to FusionVirtualHost_*domain*.conf.org.

   where *domain* is replaced with the syntax of your specific product domain.

   The following table shows how the FusionVirtualHost configuration file names map to each domain.

Table 18–1 FusionVirtualHost Configuration File-to-Domain Mapping

Domain	File Name
Oracle Fusion Common	FusionVirtualHost_fs.conf
Oracle Business Intelligence	FusionVirtualHost_bi.conf
Oracle Fusion Customer Relationship Management	FusionVirtualHost_crm.conf
Oracle Fusion Financials	FusionVirtualHost_fin.conf
Oracle Fusion Human Capital Management	FusionVirtualHost_hcm.conf
Oracle Fusion Incentive Compensation	FusionVirtualHost_ic.conf
Oracle Fusion Procurement	FusionVirtualHost_prc.conf FusionVirtualHost_prc.supplierportal.conf
Oracle Fusion Project Portfolio Management	FusionVirtualHost_prj.conf
Oracle Fusion Supply Chain Management	FusionVirtualHost_scm.conf

3. Edit the FusionVirtualHost_*domain*.conf file, adding the scaled-out host and port to all the WebLogic Application Clusters. Add this to both the Internal and External part of the FusionVirtualHost_*domain*.conf file. The example shows sample code for *ManagedServer*.

   Notes:

   - Do not add these values for Oracle Enterprise Manager, Oracle WebLogic Server Administration Console, or Oracle Authorization Policy Manager.
   - If the Managed Servers are running on VIPs, replace *PROVISIONED_HOST* and *SCALED_OUT_HOST* with the VIP addresses shown in the example code.

Example 18–1 Sample "ManagedServer" Code

```
<Location /managedServer>
    SetHandler weblogic-handler
    WebLogicCluster <PROVISIONED_HOST:port>,<SCALED_OUT_HOST:port>
</Location>
```

4. Repeat Step 3 for all applications.
5. Do the following to restart Oracle HTTP Server:

   On *WEBHOST1*:

- Change directory to *APPLICATIONS_CONFIG*/CommonDomain_webtier/bin
- Enter the following:

```
WEBHOST1> ./opmnctl stopall
WEBHOST1> ./opmnctl startall
```

On *WEBHOST2*:

- Change directory to *APPLICATIONS_CONFIG*/CommonDomain_webtier1/bin
- Enter the following:

```
WEBHOST2> ./opmnctl stopall
WEBHOST2> ./opmnctl startall
```

18.2.3.6 Configuring Server Migration for the Managed Servers

Server migration is required for proper failover of Oracle Fusion Applications components in the event of failure in any of the *PROVISIONED_HOST* and *SCALED_OUT_HOST* nodes. For more information, see Section 18.3, "Setting Up Server Migration for Oracle Fusion Applications."

18.2.3.7 Validating the System

You should verify URLs to ensure that the appropriate routing and failover are working.

To verify the URLs:

1. Log in to the domain's Oracle WebLogic Server Administration Console and stop all the Managed Servers on *PROVISIONED_HOST* while the Managed Servers on *SCALED_OUT_HOST* are running.
2. Before cloning a Managed Server, do the following:
   a. Log in to Oracle Fusion Applications with the correct user ID.
   b. Select the appropriate menu to access the application provisioned to that managed server.
   c. Copy the URL by keeping the portion/segment of https://*host*[:*port*]/*ApplicationName*/faces/*NameOfWebPage*.

   The following URLs are examples of Managed Servers in various domains:

   - https://crmexternal.mycompany.com/contractManagement/faces/ContractsDashboard
   - https://finexternal.mycompany.com/ledger/faces/JournalEntryPage
   - https://finexternal.mycompany.com/payables/faces/InvoiceWorkbench
   - https://finexternal.mycompany.com/receivables/faces/ReceiptsWorkArea
   - https://finexternal.mycompany.com/receivables/faces/TransactionsWorkArea
   - https://commonexternal.mycompany.com/helpPortal/faces/AtkHelpPortalMain
   - https://commonexternal.mycompany.com/homePage/faces/AtkHomePageWelcome
   - https://hcmexternal.mycompany.com/hcmCore/faces/AddPersonUiShellMainPage
   - https://hcmexternal.mycompany.com/hcmCore/faces/PersonSearch

- https://scmexternal.mycompany.com/productManagement/faces/ItemDashboard
- https://scmexternal.mycompany.com/costManagement/faces/ItemCostProfileWorkarea
- https://icexternal.mycompany.com/incentiveCompensation/faces/IcCnCompPlanWorkarea
- https://prjexternal.mycompany.com/projectsFinancials/faces/PRJProjectWorkarea
- https://prjexternal.mycompany.com/projectsFinancials/faces/PrjCostWorkArea

3. Log in to the domain's Oracle WebLogic Server Administration Console and stop all the Managed Servers on *SCALED_OUT_HOST*.
4. Start the Managed Servers on *PROVISIONED_HOST*.
5. Repeat Step 2. (Ensure the log in prompt is visible.)
6. Start all the Managed Servers on *SCALED_OUT_HOST* and verify that they are running on *PROVISIONED_HOST* and *SCALED_OUT_HOST*.

18.2.4 Performing Scale-Out Tasks Specific to the Oracle Fusion Customer Relationship Management Domain

In addition to the scale-out tasks found in Section 18.2.3, "Performing Scale-Out Tasks Common to All Domains," refer to Section 19.3, "Setting Up Informatica Identity Resolution for Data Quality" if you need to scale out the Oracle Fusion CRM Data Quality feature.

18.2.5 Performing Scale-Out Tasks Specific to the Common Domain

In addition to the scale-out tasks found in Section 18.2.3, "Performing Scale-Out Tasks Common to All Domains," you also must do the following for the Oracle Fusion Common domain:

- Perform one additional step when cloning Managed Servers
- Remove Oracle Coherence start-up properties from the `wlcs_server1` server
- Add a `sip` data-tier channel to the `wlcs_sipstate2` server
- Unpack the `UCM_server2` server
- Configure the Oracle WebCenter product suite
- Scale out Oracle WebCenter Content inbound refinery server
- Add the `UCM_server1` and `UCM_server2` servers to the connection pool

18.2.5.1 Cloning Managed Servers and Assigning Them to SCALED_OUT_HOST

To add a Managed Server to the Common domain, do the following:

1. Follow the steps in Section 18.2.3.4, "Cloning Managed Servers and Assigning Them to SCALED_OUT_HOST."
2. Ensure that the `UCM_server2` Managed Server is functioning properly. You should be able to access and log in to the following:
   - http://*SCALED_OUT_HOST*:7012/cs

- http://*SCALED_OUT_HOST*:7012/ibr

18.2.5.2 Removing Oracle Coherence Start-up Properties from the wlcs_server1 Server

You must remove Oracle Coherence startup properties from the wlcs_server1 Managed Server's **Startup** tab before scaling out the wlcs_server2 Manager Server.

> **Note:** Although the provisioning process adds Oracle Coherence startup properties to the wlcs_server1 Managed Server, Oracle Coherence is not configured and is not currently used in Oracle Fusion Applications on-premise deployments.

To remove the startup properties:

1. Log in to the Oracle WebLogic Server Administration Console (http://commoninternal.mycompany.com/console).
2. In the Domain Structure window, expand the **Environment** node.
3. Click **Servers**.

   The Summary of Servers page appears.
4. Select **wlcs_server1** (represented as a hyperlink) from the column of the table.

   The Settings page appears.
5. Click **Lock & Edit**.
6. Click the **Server Start** tab.
7. Remove the following Oracle Coherence properties from the Arguments field:

   ```
   -DUCS.coherence.localhost=PROVISIONED_HOST
   -DUCS.coherence.localport=7061
   -DUCS.coherence.wka1.port=7061
   -DUCS.coherence.wka1=PROVISIONED_HOST
   ```
8. Click **Save** and **Activate Changes**.
9. Navigate to **CommonDomain > Environment > Servers** and select the **Control** tab.
10. Select the wlcs_server1 Managed Server in the table, click **Shutdown**, and then select the **Force Shutdown Now** option from dropdown list.
11. Start the wlcs_server1 Managed Server.

18.2.5.3 Adding a sip Data-Tier Channel to the wlcs_sipstate2 Server

Unless you add a sip data-tier channel, the wlcs_sipstate2 server start-up fails with the following error:

```
There are no sip nor diameter channels targeted to server "wlcs_sipstate2"
```

Therefore, do the following for the wlcs_sipstate2 scaled-out server only:

1. Change directory to:

   APPLICATIONS_CONFIG/domains/*PROVISIONED_HOST*/CommonDomain/config/custom
2. After the following line in the datatier.xml file:

```
<server-name>wlcs_sipstate1</server-name>
```

add

```
<server-name>wlcs_sipstate2</server-name>
```

18.2.5.4 Unpacking the UCM_server2 Server

To provision the UCM_server2 server cluster with a shared configuration, copy the *APPLICATIONS_CONFIG*/domains/*PROVISIONED_HOST*/CommonDomain/ucm folder structure, including files, to /u02/local/oracle/config/domains/*SCALED_OUT_HOST*/CommonDomain for the UCM_Server2 local configuration.

18.2.5.5 Configuring Oracle WebCenter

This section describes the additional steps you must perform to complete the Oracle WebCenter product suite scale out.

This section tells you how to do the following:

- Configure the Oracle WebCenter Portal wc_spaces and wc_spaces 2 servers
- Configure persistence stores for JMS servers
- Configure a default persistence store for transaction recovery
- Set the listen address for the IPM_server1 and IPM_server2 servers
- Add IPM_server1 and IPM_server2 VIP addresses to the list of allowed hosts
- Add the UCM_server1 and UCM_server2 servers to the connection pool

18.2.5.5.1 Configuring the Oracle WebCenter Portal wc_spaces and wc_spaces2 Servers After scaling out the Oracle WebCenter Portal Managed Server, do the following:

1. Log in to: http://commoninternal.mycompany.com/em.
2. Navigate to **Farm_CommonDomain > WebCenter > Portal > Spaces > WebCenter Portal (11.1.*) (WC_Spaces) > WebCenter Portal (top left of right pane) > Settings > Service configuration**.

   Click **Content Repository**.
3. Highlight **FusionAppsContentRepository** and click **Edit**.
4. Select **Socket** and enter *COMMONUCMLBRVH* as the host and the LBR port for the server.
5. If updating the first instance of wc_spaces did not automatically update the second instance, repeat Step 2 through Step 4 for wc_spaces2.
6. Restart the Oracle WebCenter Portal wc_spaces and wc_spaces2 Managed Servers.

Verifying the Location of FusionAppsContentRepository

When configuring Oracle WebCenter Content Server, the FusionAppsContentRepository content repository should move from the file system to the Fusion database. To verify the move of the repository to the database, upload the /etc/hosts file on *PROVISIONED_HOST* to WebCenter Content Server by running the following commands, in order:

```
$ export RIDC_JAR=/u01/oracle/products/fusionapps/ecm/ucm/Distribution/RIDC/
oracle.ucm.ridc-11.1.1.jar

$ export UCMSCRIPT_JAR=/u01/oracle/products/fusionapps/ecm/ucm/Distribution/
```

```
FAProv/ucmscript.jar

$ java -cp $UCMSCRIPT_JAR:$RIDC_JAR oracle.ucm.client.UploadTool
--url=idc://PROVISIONED_HOST:7034 --username=sysadmin
--uploadFile=/etc/hosts --dSecurityGroup=public --dDocTitle=hosts --quiet
```

Notes:

- In the `java -cp` command, the Intradoc protocol is being used in the URL option `--url=idc://`, and not `http`.
- Get the IntradocServerPort number `7034` used in the URL above from the `/u02/local/oracle/config/domains/`*`PROVISIONED_HOST`*`/CommonDomain/ucm/cs/config/config.cfg` file.
- After the `/etc/hosts` file successfully uploads to the Fusion database, something similar to the following displays:

  ```
  Upload successful.
  [dID=1 | dDocName=UCMFA000001]
  ```

  You will use the `dID` number in the next `sqlplus` command.

```
$ sqlplus FUSION_OCSERVER11G/password@fusionDB

SQL> select dID, dRenditionID, dFileSize, DLastModified,
from FileStorage where dID=1;
SQL>
```

The following is sample output from the SQL command:

```
DID     DRENDITIONID         DFILESIZE     DLASTMODIFIED
1       primaryFile          702           21-MAY-13 12.16.03.524000 PM
1       webViewableFile      702           21-MAY-13 12.16.03.687000 PM
```

18.2.5.5.2 Configuring Persistence Stores for JMS Servers You must set the location for all persistence stores targeted to the `IPM_server1` and `IPM_server2` Managed Servers to a directory that is visible from both *`PROVISIONED_HOST`* and *`SCALED_OUT_HOST`*.

To configure the persistence stores:

1. Log in to the Oracle WebLogic Server Administration Console (`http://commoninternal.mycompany.com/console`).
2. Click **Lock & Edit**.
3. In the Domain Structure window, expand the **Services** node and then click the **Persistence Stores** node.

   The Summary of Persistent Stores page displays.
4. Click **New**, and then select the **Create File Store** option from dropdown list.
5. Enter the following directory information:
   - **Name**: For example, `IPMJMSFileStore1`
   - **Target**: `IPM_server1`
   - **Directory**: *`APPLICATIONS_CONFIG`*`/domains/`*`PROVISIONED_HOST`*`/CommonDomain`
6. Click **OK**.
7. Repeat Steps 3 through 6 to create the following persistence stores:

- ViewerJMSFileStore1, targeting to IPM_server1
- ViewerJMSFileStore2, targeting to IPM_server2
- IPMJMSFileStore2, targeting to IPM_server2

8. Click **Activate Changes**.
9. Click **Lock & Edit**.
10. In the Domain Structure window, expand the **Services** node and then click the **Messaging > JMS Servers** node.

    The Summary of JMS Servers page displays.
11. Click the name of the server, **IpmJmsServer1**.
12. From the **Configuration > General** tab, select **IPMJMSFileStore1** from the **Persistence Store** dropdown list.
13. Click **Save**.
14. Repeat Steps 10 through 13 for the JMS server **ViewerJmsServer1** using ViewerJMSFileStore1.
15. Click **Activate Changes**.
16. Click **Lock & Edit**.
17. In the Domain Structure window, expand the **Services** node and then click the **Messaging > JMS Servers** node.

    The Summary of JMS Servers page displays.
18. Click **New**.
19. Enter a name (for example, IpmJmsServer2), then select **IPMJMSFileStore2** from the **Persistence Store** dropdown list.
20. Click **Next**.
21. Select **IPM_server2** as the target.
22. Click **Finish**.
23. Repeat Steps 17 through 22 to create the new JMS server **ViewerJmsServer2** using ViewerJMSFileStore2 targeting theIPM_server2 Managed Server.
24. Click **Activate Changes**.
25. Restart the IPM_server1 and IPM_server2 Managed Servers.

18.2.5.5.3 Configuring a Default Persistence Store for Transaction Recovery

Each server has a transaction log which stores information about committed transactions that are coordinated by the server that may not have been completed. Oracle WebLogic Server uses this transaction log for recovery from system crashes or network failures. To leverage the migration capability of the Transaction Recovery Service for the servers within a cluster, store the transaction log in a location accessible to a server and its backup servers.

> **Note:** Preferably, this location should be a dual-ported SCSI disk or on a Storage Area Network (SAN).

To set the location for the default persistence store:

1. Log in to the Oracle WebLogic Server Administration Console (`http://commoninternal.mycompany.com/console`).
2. In the Change Center, click **Lock & Edit**.
3. In the Domain Structure window, expand the **Environment** node and then click the **Servers** node.

   The Summary of Servers page displays.
4. Click the name of the server (represented as a hyperlink) in the **IPM_server1** table. The settings page for the selected server opens with the **Configuration** tab active.
5. Open the **Services** tab.
6. In the Default Store section of the page, enter the path to the folder where the default persistent stores will store its data files. For example, create a directory

   PROVISIONED_HOST> *APPLICATIONS_CONFIG*/domains/*PROVISIONED_HOST*/CommonDomain/tlogs
7. Click **Save**.
8. Repeat Steps 1 through 7 for the `IPM_server2` Managed Server.
9. Click **Activate Changes**.
10. Restart the Managed Servers to activate the changes (ensure that Node Manager is up and running):
    a. Log in to the Oracle WebLogic Server Administration Console (`http://commoninternal.mycompany.com/console`).
    b. In the Summary of Servers screen, select the **Control** tab.
    c. Select **IPM_server1** and **IPM_server2** in the table and then click **Shutdown**.
    d. After the servers have shut down, select **IPM_server1** and **IPM_server2** in the table and click **Start**.

Notes:

- To enable migration of the Transaction Recovery service, specify a location on a persistent storage solution that is available to other servers in the cluster. Both `IPM_server1` and `IPM_server2` must be able to access this directory.
- Ensure the following the path exists on your machine: `/usr/share/X11/fonts/TTF`.

18.2.5.5.4 Setting the Listen Address for IPM_server1 and IPM_server2 Ensure that you have enabled virtual IPs on *PROVISIONED_HOST* and *SCALED_OUT_HOST* before setting the `IPM_server1` and `IPM_server2` listen addresses.

To set the listen address for the Managed Servers:

1. Log in to the Administration Console (`http://commoninternal.mycompany.com/console`).
2. In the Change Center, click **Lock & Edit**.
3. Expand the Environment node in the Domain Structure window.
4. Click **Servers**.

The Summary of Servers page displays.

5. Select **IPM_server1** in the table.

   The Settings page for `IPM_server1` Managed Server displays.

6. Set the listen address to **COMMONIPMVH1** and click **Save**.

7. Navigate to the Summary of Servers page and select **IPM_server2** in the table.

   The Settings page for the `IPM_server2` Managed Server displays.

8. Set the listen address to **COMMONIPMVH2** and click **Save**.

   Note: Both *COMMONIPMVH1* and *COMMONIPMVH2* are pingable.

9. Click **Activate Changes.**

   The changes will not take effect until the `IPM_server1` and `IPM_server2` Managed Servers are restarted. To restart the Managed Servers, do the following:

   a. Ensure that Node Manager is up and running.

   b. On the Summary of Servers page, select the **Control** tab.

   c. Navigate to the Summary of Servers page, select **IPM_server1** and**IPM_server2** in the table, and then click **Shutdown**.

   d. After the servers have shut down, select **IPM_server1** and **IPM_server2** in the table and click **Start**.

18.2.5.5.5 Adding IPM_server1 and IPM_server2 VIP Addresses to the List of Allowed Hosts

Perform these steps to add the `IPM_server1` and `IPM_server2` virtual-host names to the `SocketHostNameSecurityFilter` parameter list:

1. Edit the `config` file on *PROVISIONED_HOST*: *APPLICATIONS_CONFIG*`/domains/`*PROVISIONED_HOST*`/CommonDomain/ucm/cs/config/config.cfg`, with the following:

   `SocketHostNameSecurityFilter=localhost|localhost.localdomain|localhost6|localhost6.localdomain6|`*WEBHOST1*`|`*PROVISIONED_HOST*`|`*WEBHOST2*`|`*SCALED_OUT_HOST*`|`*COMMONUCMLBRVH*`|`*COMMONIPMVH1*`|`*COMMONIPMVH2*

2. Restart the `UCM_server1` and `UCM_server2` Oracle WebCenter Content Management Servers for the changes to take effect.

18.2.5.6 Scaling Out Oracle WebCenter Content Inbound Refinery Server

Follow the steps below to scale out the Oracle WebCenter Content Inbound Refinery (IBR) server. Note that IBR is provisioned only if the provisioning offering(s) you select needs it. Subsequently, your environment may not need IBR.

Note: If *APPLICATIONS_LOCAL_CONFIG*`/domains/`*PROVISIONED_HOST*`/CommonDomain/ucm/ibr` is present on *PROVISIONED_HOST*, then IBR is provisioned in the environment.

1. Edit the *APPLICAITONS_LOCAL_CONFIG*`/domains/`*PROVISIONED_HOST*`/CommonDomain/ucm/ibr/config/config.cfg` file on *PROVISIONED_HOST* with the following:

- IDC_Name=*PROVISIONED_HOST*7012
- InstanceMenuLabel=*PROVISIONED_HOST*7012
- SocketHostNameSecurityFilter=localhost|localhost.localdomain|localhost6|localhost6.localdomain6|*PROVISIONED_HOST*|*SCALED_OUT_HOST*
- HttpServerAddress=*PROVISIONED_HOST*:7012 (*PROVISIONED_HOST*'s server address instead of load balancer, as it is a singleton node.)

2. Restart the ucm_server1 server.
3. Navigate to http://*SCALED_OUT_HOST*:7012/ibr (*SCALED_OUT_HOST*'s ibr) and log in when prompted.

   The post-installation configuration page displays, as it is not a clustered node.
4. On the post-installation configuration page:
   a. Set the server socket port to **7035**.
   b. Ensure the port has a unique server instance name and unique local paths on *SCALED_OUT_HOST*.
   c. Set the Incoming Socket Connection Address Security Filter:

      SocketHostNameSecurityFilter=localhost|localhost.localdomain|localhost6|localhost6.localdomain6|*PROVISIONED_HOST*|*SCALED_OUT_HOST*
   d. Click **Submit**.
   e. Restart the ucm_server2 server.
5. Navigate to http://*PROVISIONED_HOST*:7012/cs and select **Administration > providers**.

   ibrprovider is already defined in this list.
6. Add a new outgoing provider:
   a. Click **Add**.
   b. Set the values to match the values of **ibrprovider**.

      Note: The value for the new outgoing ibrprovider must differ from the value of the default ibrprovider.

   c. Assign the following unique values: to Provider Name, Provider Description, Server Host Name, Server Port, Instance Name, and Relative Web Root.
      – Provider Name: ibr_provider2
      – Provider Description: ibrprovider for second server
      – Server Host Name: *SCALED_OUT_HOST*
      – Server Port: 7035
      – Instance Name: *SCALED_OUT_HOST_HOST*7012
      – Relative Web Root: /cs
7. Navigate to Inbound Refinery on second node: http://*SCALED_OUT_HOST*:7012/ibr.
8. Select **Conversion Settings** and update the primary web rendition.

9. Navigate to **Third-Party Applications Settings > General OutsideIn Filter Options > Options** and set the following path to the fonts: `/usr/share/X11/fonts/TTF`.

> **Note:** The font location can be specific to the operating system.

10. Restart the `UCM_server1` and `UCM_server2` Managed Servers.

18.2.5.7 Adding UCM_server1 and UCM_server2 to the Connection Pool

To add `UCM_server1` and `UCM_server2` to the connection pool, do the following:

1. Log in to the Oracle WebCenter Content: Imaging application at: `https://commonexternal.mycompany.com/imaging`.
2. In the left-hand pane, expand **Manage Connections**.
3. Click the **Fusion Applications UCM Connection** link.
4. In the right-hand Fusion Applications UCM Connection: Connection Summary pane, click **Modify**.
5. In the Basic Information screen, click **Next**.
6. In the Connection Settings screen, add two servers to the Content Server pool:
   - *PROVISIONED_HOST*: `7034`
   - *SCALED_OUT_HOST*: `7034`
7. Click **Next**.
8. In the Connection Security screen, leave all four default selections for the **FUN_FINANCIAL_APPLICATION_ADMINISTRATOR_JOB** WebLogic user, and then click **Next**.
9. In the Review Settings screen, review the connection details and click **Submit**.

18.2.6 Configuring Oracle Coherence for the odi_server Managed Server

Oracle Data Integrator Managed Servers are present in four domains:

- Oracle Fusion CRM
- Oracle Fusion HCM
- Oracle Fusion Human Capital Management
- Oracle Fusion Incentive Compensation

Oracle recommends using unicast communication in `odi_server` enterprise deployments, unless use of multicast is a must. Consider using multicast communication for large Oracle Data Integrator clusters with approximately 20 or more Oracle Data Integrator Managed Servers

> **Note:** An incorrect configuration of the Oracle Coherence framework that is used for deployment may prevent the `odi_server` Managed Server from starting. Oracle recommends the configuration described in this section.

Unicast communication does not enable nodes to discover other cluster members automatically when a new Oracle Data Integrator server is added to a cluster. Consequently, you must specify the nodes that belong to the cluster. You do not need to specify all of the nodes of a cluster, however. You need only specify enough nodes so that a new node added to the cluster can discover one of the existing nodes. Consequently, when a new node has joined the cluster, it is able to discover all of the other nodes in the cluster. Additionally, in configurations such as Oracle Data Integrator enterprise deployments, where multiple IPs are available in the same box, you must configure Oracle Coherence to use a specific host name to create the Oracle Coherence cluster.

> **Tip:** To guarantee high availability during deployments of `odi_server` Managed Servers, specify enough nodes so that at least one of them is running at any given time.

Specify the nodes using the `-Doracle.odi.coherence.wka` *n* system property, where *n* is the number for each Oracle HTTP Server. The numbering starts at 1. This numbering must be sequential and must not contain gaps. In addition, specify the host name used by Oracle Coherence to create a cluster through the `tangosol.coherence.localhost` system property. Set this property by adding the `-Dtangosol.coherence.localhost` parameters to the Arguments field of the Oracle WebLogic Server Administration Console's **Server Start** tab.

To add the virtual-host names to Oracle Coherence:

1. Log in to the Oracle WebLogic Server Administration Console (`http://`*domain_name*`internal.mycompany.com/console`).
2. In the Domain Structure window, expand the **Environment** node.
3. Click **Servers**.

   The Summary of Servers page appears.
4. Select **odi_server1** (represented as a hyperlink) from the column of the table.

   The Settings page appears.
5. Click **Lock & Edit**.
6. Click the **Server Start** tab.
7. Change the existing properties if necessary, and enter new properties into the Arguments field:

```
-Dtangosol.coherence.localport=9066
-Dtangosol.coherence.localhost=PROVISIONED_HOST
-Doracle.odi.coherence.wka1=PROVISIONED_HOST
-Doracle.odi.coherence.wka1.port=9066
-Doracle.odi.coherence.wka2=SCALED_OUT_HOST
-Doracle.odi.coherence.wka2.port=9066
-DJDBCProgramName=DS/domain_nameDomain/odi_server1
-Dserver.group=ODICluster
```

> **Note:** There should be no breaks in lines between the different `-D` parameters. Do not copy or paste the code from above to your Administration Console's Arguments text field. This may result in HTML tags being inserted in the Java arguments. The code should not contain other characters than those included in the example above.

8. Click **Save** and **Activate Changes**.
9. Navigate to *Domain_Name* > **Environment** > **Servers** and select the **Control** tab.
10. Select the `odi_server1` Managed Server in the table, click **Shutdown**, and then select the **Force Shutdown Now** option from dropdown list.
11. Start the `odi_server1` Managed Server.

18.2.7 Scaling Out the Oracle Business Intelligence Domain

This chapter describes how to scale the Oracle Business Intelligence domain.

18.2.7.1 Overview of the Oracle Business Intelligence Domain

Oracle Fusion Applications offerings use following Oracle Business Intelligence components from the Oracle Business Intelligence domain:

- Oracle Business Intelligence Analytics
- Essbase
- Oracle Real-Time Decisions
- Oracle Business Intelligence Publisher
- Oracle Business Intelligence Publisher (Oracle BI Publisher)
- Oracle Transaction Business Intelligence

Oracle Essbase

Oracle Fusion General Ledger combines the traditional general ledger functionality with Oracle Essbase functionality, which is embedded seamlessly within Oracle Fusion General Ledger. At the time users create their chart of accounts, the balances cube is created automatically. Later, if you make a change such as a cost center is added or a date effective hierarchy is modified, the General Ledger automatically creates or modifies the corresponding balances cube hierarchy. As transactions or journals are posted, the General Ledger automatically updates the multidimensional cube. Unlike a data warehouse, no batch programs need to be run to populate the balances cube; it is all happening in real time when a journal is posted.

Oracle Business Intelligence Publisher

Oracle BI Publisher provides the ability to create and format high quality reports across Oracle Fusion Financials applications. It applies templates, which users design in familiar desktop tools, to standard extracts and reports. For example, it is used widely used in Oracle Fusion Payments for formatting of the check payments and electronic payment files.

Oracle Transaction Business Intelligence

Oracle Transaction Business Intelligence is widely used in Oracle Fusion Financials as a reporting tool. Using Oracle Transaction Business Intelligence, users can perform adhoc queries directly from transaction tables using drag-and-drop functionality to build custom reports in real time from the various Oracle Fusion Financials applications. It helps immensely in reducing the need to build and maintain customized reports.

Oracle Business Intelligence Analytics

Oracle Business Intelligence Analytics provides day-to -day key performance indicators (KPIs) of any item in Oracle Fusion Financials. Intelligence and analytics are

embedded within the context of business transactions to help users complete the transitions. For example, before users post a journal, the system will tell them the impact the journal will have on the account balances. This eliminates the need to navigate to a separate page to run a query or run a report. End users will not be distracted from the task at hand, reporting and process demand is reduced, and smarter decisions are made in the context of the transaction.

18.2.7.2 Prerequisites for Scaling the Oracle Business Intelligence Domain

Before you begin, ensure the following:

- Node Manager has been started in the Secure Sockets Layer (SSL) mode by following the instructions in Section 18.2.2, "Scaling Out Node Manager."
- The Administration Console's **Follow Configuration Changes** feature has been disabled (to eliminate redirections):
  1. Log into the Administration Console (`http://biinternal.mycompany.com/console`) and go to **Preferences > Shared Preferences**.
  2. Deselect **Follow Configuration Changes** and click **Save**.

18.2.7.3 Starting the Default Node Manager

To start the default Node Manager:

1. Stop any Node Manager running on *BIHOST2* using one of the following methods:
   - Use Ctrl+C in the shell where it was started.
   - Use the standard process-identification and kill commands in the operating system appropriate to your specific product offering and the Oracle Fusion Applications enterprise deployment.
2. Change directory to *APPLICATIONS_BASE*`/fusionapps/wlserver_10.3/common/nodemanager` and edit the `nodemanager.properties` file with the following:

   ```
   SecureListener=false
   ```

3. Change directory to *APPLICATIONS_BASE*`/fusionapps/oracle_common/common/bin` and run the following script:

   ```
   ./setNMProps.sh
   ```

4. Change directory to *APPLICATIONS_BASE*`/fusionapps/wlserver_10.3/server/bin` and run the following script:

   ```
   ./startNodeManager.sh
   ```

   Node Manager starts on *BIHOST2*.

> **Note:** Steps 2 through 4 will enable Node Manager on *BIHOST2* and the Administrator Console to communicate on Plain Socket.

18.2.7.4 Prerequisites for Scaling Oracle Business Intelligence on BIHOST2

Prerequisites include the following:

- Configuring a JMS file persistence store on *BIHOST1*
- Setting the listen address for the `bi_server1` server

- Updating the `FusionVirtualHost_bi.conf` configuration file

18.2.7.4.1 Configuring a JMS File Persistence Store in BIHOST1 You must configure the location for the Java Message Service (JMS) file persistence store to a directory visible from both nodes. Change the persistent store to use this shared base directory.

1. Log in to the Administration Console (`http://biinternal.mycompany.com/console`).
2. In the Domain Structure window, expand the **Services** node.
3. In the Change Center, click **Lock & Edit**.
4. Click the **Persistent Stores** node.

   The Summary of Persistent Stores page displays.
5. Click **JRFWSAsyncFileStore** and enter a directory that is located in the shared storage. This shared storage is accessible from both *BIHOST1* and *BIHOST2*:

   APPLICATIONS_CONFIG`/domains/`*BIHOST1*`/BIDomain/JRFWSAsyncFileStore`
6. Click **Save**.
7. Click **Activate Changes**.

   The changes will not take effect until the Managed Server is restarted.
8. Do the following:
   a. Ensure that Node Manager is up and running.
   b. On the Summary of Servers page, select the **Control** tab.
   c. Select **bi_server1** in the table and then click **Shutdown**.
   d. After the server has shut down, select **bi_server1** in the table and then click **Start**.
9. Run the following commands on *BIHOST1* to restart the Oracle Business Intelligence system components:

```
$ cd APPLICATIONS_CONFIG/BIInstance/bin
$ ./opmnctl stopall
$ ./opmnctl startall
```

18.2.7.4.2 Setting the Listen Address for the bi_server1 Managed Server Make sure that you have performed the steps described in Section 18.2.9.2, "Enabling Virtual IPs on PROVISIONED_HOST and SCALED_OUT_HOST" before setting the `bi_server1` listen address.

To set the listen address for the Managed Server:

1. Log in to the Administration Console (`http://biinternal.mycompany.com/console`).
2. In the Change Center, click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Select **bi_server1** in the table. The Settings page for `bi_server1` is displayed.
6. Set the **Listen Address** to *BIVH1*.

> **Note:** Both *BIVH1* and *BIVH2* are pingable.

7. Click **Save**.
8. Click **Activate Changes**.
9. The changes will not take effect until the `bi_server1` Managed Server is restarted (ensure that Node Manager is up and running):
   a. On the Summary of Servers page, select the **Control** tab.
   b. Select **bi_server1** in the table and then click **Shutdown**.
   c. After the server has shut down, select **bi_server1** in the table and then click **Start**.
10. Restart the Oracle Business Intelligence system components on *BIHOST1*:

```
$ cd APPLICATIONS_CONFIG/BIInstance/bin
$ ./opmnctl stopall
$ ./opmnctl startall
```

18.2.7.4.3 Updating the FusionVirtualHost_bi.conf Configuration File To enable Oracle HTTP Server to route to `bi_cluster`, which contains the `bi_servern` Managed Servers, you must set the WebLogicCluster parameter to the list of nodes in the cluster:

1. Update the WebLogicCluster parameter in the `FusionVirtualHost_bi.conf` file to contain a cluster list of virtual *host*:*port* entries. (On *WEBHOST1*: *APPLICATIONS_CONFIG*/CommonDomain_webtier/config/OHS/ohs1/moduleconf/FusionVirtualHost_bi.conf. On *WEBHOST2*: *APPLICATIONS_CONFIG*/CommonDomain_webtier1/config/OHS/ohs2/moduleconf/FusionVirtualHost_bi.conf.)

   > **Note:** You must update the `FusionVirtualHost_bi.conf` file in two locations:
   >
   > - Under the internal virtual host for Oracle Business Intelligence
   > - Under the external virtual host for Oracle Business Intelligence

   For example, for the internal virtual host:

```
<LocationMatch ^/analytics/>
SetHandler weblogic-handler
WebLogicCluster BIVH1:10217,BIVH2:10217
</LocationMatch>
```

   For the external virtual host:

```
<LocationMatch ^/analytics/>
SetHandler weblogic-handler
WebLogicCluster BIVH1:10217,BIVH2:10217
WLProxySSL ON
WLProxySSLPassThrough ON
RewriteEngine ON
RewriteOptions inherit
</LocationMatch>
```

2. Restart Oracle HTTP Server on both *WEBHOST1* and *WEBHOST2*:

```
WEBHOST1> APPLICATIONS_CONFIG/CommonDomain_webtier/bin/opmnctl restartproc
ias-component=ohs1
WEBHOST2> APPLICATIONS_CONFIG/CommonDomain_webtier1/bin/opmnctl restartproc
ias-component=ohs2
```

The servers specified in the WebLogicCluster parameters are only important at startup time for the plug-in. The list must provide at least one running cluster member for the plug-in to discover other members in the cluster. The listed cluster member must be running when Oracle HTTP Server is started. Oracle WebLogic Server and the plug-in work together to update the server list automatically with new, failed, and recovered cluster members.

Sample scenarios include:

- **Example 1:** If you have a two-node cluster and then add a third member, you do not need to update the configuration to add the third member. The third member will be discovered dynamically at run time.
- **Example 2:** You have a three-node cluster, but only two nodes are listed in the configuration. However, if both listed nodes are down when you start Oracle HTTP Server, then the plug-in would fail to route to the cluster. You must ensure that at least one of the listed nodes is running when you start Oracle HTTP Server.

  If you list all the members of the cluster, then you guarantee you can route to the cluster, assuming at least one member is running when Oracle HTTP Server is started. For more information on configuring the Oracle WebLogic Serverplug-in, see *Oracle Fusion Middleware Using Web Server 1.1 Plug-Ins with Oracle WebLogic Server*.

18.2.7.5 Scaling Oracle Business Intelligence Components

This section describes how to scale out the Oracle Business Intelligence system using the Configuration Assistant. It is assumed that an Oracle Business Intelligence *ORACLE_BASE* (binaries) has already been installed and is available from *BIHOST1* and *BIHOST2*, and that a domain with an Administration Server has been created. This is the domain that will be extended in this chapter to support Oracle Business Intelligence components.

Important: Oracle strongly recommends that you read the Oracle Fusion Middleware release notes for any additional installation and deployment considerations before starting the setup process.

This section tells you how to do the following:

- Scale out Oracle Business Intelligence on *BIHOST2*
- Start Node Manager in SSL mode
- Scale out the system components
- Configure secondary instances of singleton system components
- Configure the `bi_server2` Managed Server
- Perform additional configuration for Oracle Business Intelligence high availability
- Configure a default persistence store for transaction recovery
- Start and validate Oracle Business Intelligence on *BIHOST2*

- Validate access through Oracle HTTP Server
- Configure Node Manager for the Managed Servers
- Configure server migration for the Managed Servers

18.2.7.5.1 Scaling Out the Oracle Business Intelligence System on BIHOST2 To scale out the Oracle Business Intelligence system:

1. Ensure that the `bi_server1` server is running.
2. Change directory to the location of the Configuration Assistant:

   BIHOST2`> `*APPLICATIONS_BASE*`/fusionapps/bi/bin`

3. Start the Oracle Business Intelligence Configuration Assistant:

   BIHOST2`> ./config.sh`

4. In the Welcome screen, click **Next**.
5. In the Prerequisite Checks screen, verify that all checks complete successfully, and then click **Next**.
6. In the Create, Scale Out or Extend BI System screen, select **Scale Out BI System** and enter the following:
   - **Host Name:** *BIHOST1*
   - **Port:** `10201`
   - **User name:** *WLS_Administrator*
   - **User Password:** *WLS_Administrator_password*

   Click **Next**.
7. In the Scale Out BI System Details screen, enter the following:
   - **Middleware Home:** *APPLICATIONS_BASE*`/fusionapps` (dimmed)
   - **Oracle Home:** *APPLICATIONS_BASE*`/fusionapps/bi` (dimmed)
   - **WebLogic Server Home:** *APPLICATIONS_BASE*`/fusionapps/wlserver_10.3` (dimmed)
   - **Domain Home:** *APPLICATIONS_CONFIG*`/domains/`*BIHOST1*`/BIDomain`
   - **Applications Home:** *APPLICATIONS_CONFIG*`/applications/BIDomain`
   - **Instance Home:** Defaults to *APPLICATIONS_CONFIG*`/BIInstance1`
   - **Instance Name:** `BIInstance1` (dimmed)

   Click **Next**.
8. In the Configure Ports screen, select "Specify Ports using Configuration File."

   Use the `bi_staticports.ini` file from the *APPLICATIONS_BASE*`/ports` directory.

   Click **Next**.
9. In the Specify Security Updates screen, choose whether you want to receive security updates from Oracle support and if you do, enter your e-mail address.

   Click **Next**.
10. In the Summary screen, click **Configure**.

11. In the Configuration Progress screen, verify that all the Configuration Tools have completed successfully and click **Next**.
12. In the Complete screen, click **Finish**.

18.2.7.5.2 Starting Node Manager in SSL Mode

To start Node Manager in SSL mode:

1. Stop the default Node Manager running on *BIHOST2* using one of the following methods:
   - Use CTRL+C in the shell where it was started
   - Use the standard process-identification and kill commands in the operating system appropriate to the product and the Oracle Fusion Applications enterprise deployment.
2. Start Node Manager in SSL mode on *BIHOST2*:

```
BIHOST2> cd APPLICATIONS_CONFIG/nodemanager/BIHOST2

BIHOST2> ./startNodeManagerWrapper.sh &
```

3. Update the Node Manager for the *BIHOST2* machine using the Oracle WebLogic Server Console by doing the following:
   a. Log in to the Administration Server: `http://biinternal.mycompany.com/console`.
   b. Navigate to **BIDomain> Environment > Machines**.
   c. In the left-hand pane, click **Lock & Edit**.
   d. In the right-hand pane, click *BIHOST2*.
   e. In the window that opens, click the **Node Manager** tab and set the following attributes:
      – Type - SSL
      – Listen Address - <*BIHOST2*>
      – Listen Port - 5556
4. Click **Save** and then **Activate Changes**.

   The changes will not take effect until the `bi_server2` Managed Server is restarted.
5. Do the following:
   a. Stop the Administration Server:

```
BIHOST1> APPLICATIONS_CONFIG/domains/BIHOST1/BIDomain/bin/stopWebLogic.sh
```

   b. Connect to the Administration Server through `nmConnect` and start the Administration Server using `nmstart`:
      – Set the following environment variable:

```
export WLST_PROPERTIES="-Dweblogic.security.SSL.trustedCAKeyStore=
APPLICATIONS_CONFIG/keystores/fusion_trust.jks"
```

      – Start the Administration Server:

```
BIHOST1> cd APPLICATIONS_BASE/fusionapps/
wlserver_10.3/common/bin

BIHOST1> ./wlst.sh
```

– In the WLST shell, execute the following command:

```
wls:/offline> nmConnect (username='Admin_User',password='Admin_
Password',host='BIHOST1',port='5556', nmType='ssl', domainDir=
'APPLICATIONS_CONFIG/domains/BIHOST1/BIDomain')

wls:/nm/domain_name> nmStart ('AdminServer')
wls:/nm/domain_name> exit ()
```

Note: The *username* and *password* used in `nmConnect` are the Node Manager credentials (user name and password) specified when creating the provisioning response file.

c. Restart the `bi_server2` Managed Server:

– On the Summary of Servers page, select the **Control** tab.

– Select **bi_server2** in the table and then click **Shutdown**.

– After the server has shut down, select **bi_server2** in the table and then click **Start**.

18.2.7.5.3 Scaling the System Components To scale out the system components, do the following in Oracle Enterprise Manager Fusion Middleware Control:

1. Log in to Fusion Middleware Control (`http://biinternal.mycompany.com/em`).
2. Expand the **Business Intelligence** node in the Farm_BIDomain window.
3. Click **coreapplication**.
4. Click **Capacity Management**, then click **Scalability**.
5. Click **Lock and Edit Configuration**.
6. For the *BIHOST2* BIInstance1 Oracle instance, increment the Oracle Business Intelligence components by 1:
   - BI Servers
   - Presentation Servers
   - JavaHosts
7. Change the **Port Range From** and **Port Range To** to be the same as the *BIHOST1* BIInstance Oracle instance.
8. Click **Apply**.
9. Click **Activate Changes**.

You do not need to restart at this point, because you will perform a restart after completing the steps in Section 18.2.7.5.4, "Configuring Secondary Instances of Singleton Components."

18.2.7.5.4 Configuring Secondary Instances of Singleton Components Oracle Business Intelligence Scheduler and Oracle Business Intelligence Cluster Controller are singleton components that operate in active/passive mode. Configure a secondary instance of these components so that they are distributed for high availability.

To configure secondary instances, do the following in Fusion Middleware Control:

1. Log in to Fusion Middleware Control (`http://biinternal.mycompany.com/em`).

2. Expand the **Business Intelligence** node in the Farm_BIDomain window.
3. Click **coreapplication**.
4. Click **Availability**, then click **Failover**.
5. Click **Lock and Edit Configuration** to activate the Primary/Secondary Configuration section of the Availability tab.
6. Specify the Secondary Host/Instance for BI Scheduler and BI Cluster Controller.
7. Click **Apply**.
8. Click **Activate Changes**.
9. Click **Restart to apply recent changes**.
10. From **Manage System**, click **Restart**.
11. Click **Yes** when prompted to confirm that you want to restart all Business Intelligence components.

> **Note:** Under Potential Single Points of Failure, no problem should be reported for BI Scheduler and BI Cluster Controller.

18.2.7.5.5 Configuring the bi_server2 Managed Server This section explains what you need to do to configure the `bi_server2` Managed Server.

Setting the Listen Address for the bi_server2 Managed Server

Make sure that you have performed the steps described in Section 18.2.9.2, "Enabling Virtual IPs on PROVISIONED_HOST and SCALED_OUT_HOST" before setting the `bi_server2` listen address.

To set the listen address for the Managed Server:

1. Log in to the Oracle WebLogic Server Administration Console (`http://biinternal.mycompany.com/console`).
2. In the Change Center, click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Select **bi_server2** in the table. The settings page for `bi_server2` is displayed.
6. Set the **Listen Address** to *`BIVH2`*.
7. Click **Save**.
8. Click **Activate Changes**.

   The changes will not take effect until the Managed Server is restarted.
9. Do the following:
   a. Ensure that Node Manager is up and running.
   b. On the Summary of Servers page, select the **Control** tab.
   c. Select **bi_server2** in the table and then click **Shutdown**.
   d. After the server has shut down, select **bi_server2** in the table and then click **Start**.

Configuring Custom Identity and Custom Trust for the bi_server2 Managed Server

To configure custom identity and custom trust:

1. Log in to the Oracle WebLogic Server Administration Console (`http://biinternal.mycompany.com/console`).
2. In the Change Center, click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**.

   The Summary of Servers page displays.
5. Select **bi_server2** in the table. The Settings page for `bi_server2` displays.
6. Click **Keystores**, and then do the following:
   a. Click **Change** next to **Demo Identity and Demo Trust**.
   b. Select **Custom Identity and Custom Trust** from the **Keystores** dropdown list and click **Save**.
   c. Under **Identity**, do the following:

      – Change the Custom Identity Keystore entry to point to the *APPLICATIONS_CONFIG*`/keystores/`*BIHOST2*`_fusion_identity.jks` file.

      – Enter and confirm the Custom Identity Keystore Passphrase.
   d. Under **Trust**, do the following:

      – Change the Custom Identity Keystore entry to point to the *APPLICATIONS_CONFIG*`/keystores/fusion_trust.jks` file.

      – Enter and confirm the Custom Trust Keystore Passphrase.

      – Click **Save**.
7. Click **SSL**, and then do the following:
   a. Ensure that Identity and Trust Locations is set to **Keystores**.
   b. Under **Identity**, do the following:

      – Change the Private Key Alias to *BIHOST2*`_fusion`.

      – Enter and confirm the Private Key Passphrase to the *keypassword*.

      – Click **Save**.
8. Click **Activate Changes**.
9. Set the following property in *APPLICATIONS_BASE*`/fusionapps/wlserver_10.3/common/bin/wlst.sh`:

```
WLST_PROPERTIES=" -Dweblogic.wlstHome='${WLST_HOME}'
-Dweblogic.security.SSL.trustedCAKeyStore=APPLICATIONS_CONFIG/keystores/
fusion_trust.jks ${WLST_PROPERTIES}"
```

Disabling Host Name Verification for the bi_server2 Managed Server

This step is required if you have not set up the appropriate certificates to authenticate the different nodes with the Administration Server. If you have not configured the server certificates, you will receive errors when managing the different WebLogic servers. To avoid these errors, disable host name verification while setting up and validating the topology, and enable it again after the topology configuration is complete.

To disable host name verification:

1. Log in to Oracle WebLogic Server Administration Console (`http://biinternal.mycompany.com/console`).
2. Click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Select **bi_server2** in the table. The settings page for the server is displayed.
6. Click the **SSL** tab.
7. Expand the **Advanced** section of the page.
8. Set **Host Name Verification** to **None**.
9. Click **Save**.
10. Click **Activate Changes**.
11. The change will not take effect until the `bi_server2` Managed Server is restarted (make sure that Node Manager is up and running):
    a. In the Summary of Servers screen, select the **Control** tab.
    b. Select **bi_server2** in the table and then click **Shutdown**.
    c. Select **bi_server2** in the table and then click **Start**.
12. Restart the Oracle Business Intelligence system components on *`BIHOST2`*:

```
$ cd APPLICATIONS_CONFIG/BIInstance1/bin
$ ./opmnctl stopall
$ ./opmnctl startall
```

Adding bi_server2 System Properties to the Server Start Tab

After scaling out the `bi_server2` Managed Server, you must add a new system property to the **Server Start** tab of this Managed Server.

1. Log in to the Oracle WebLogic Server Administration Console (`http://biinternal.mycompany.com/console`).
2. Click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**.

   The Summary of Servers page displays.
5. Select **bi_server2** in the table.

   The settings page for the server displays.
6. Click **Server Start**.
7. Add the following property to the arguments:

```
-DJDBCProgramName=DS/BIDomain/bi_server2
```

8. Click **Save** and then **Activate Changes**.
9. Restart the `bi_server2` Managed Server (ensure sure that Node Manager is up and running):
    a. In the Summary of Servers screen, select the **Control** tab.

b. Select **bi_server2** in the table and then click **Shutdown**.

c. Select **bi_server2** in the table and then click **Start**.

10. Restart the BI System Components on *BIHOST2*:

```
$ cd APPLICATIONS_CONFIG/BIInstance1/bin
$ ./opmnctl stopall
$ ./opmnctl startall
```

18.2.7.5.6 Performing Additional Configuration for Oracle Business Intelligence High Availability

This section describes additional high availability configuration tasks for Oracle BI Enterprise Edition, Oracle Real-Time Decisions, Oracle BI Publisher, and Oracle Financial Reports.

Additional Configuration Tasks for Oracle BI Scheduler

If you use server-side scripts with Oracle BI Scheduler, it is recommended that you configure a shared directory for the scripts so that they can be shared by all Oracle BI Scheduler components in a cluster.

Perform these steps only if you are using server-side scripts.

To share Oracle BI Scheduler scripts:

1. Create an *APPLICATIONS_CONFIG*/BIShared/OracleBISchedulerComponent/coreapplication_obisch1 directory.

2. From *BIHOST1*, copy the default Oracle BI Scheduler scripts (for example, *APPLICATIONS_CONFIG*/BIInstance/bifoundation/OracleBISchedulerComponent/coreapplication_obisch1/scripts/common) and custom Oracle BI Scheduler scripts (for example, *APPLICATIONS_CONFIG*/BIInstance/bifoundation/OracleBISchedulerComponent/coreapplication_obisch1/scripts/scheduler) to the following location:

APPLICATIONS_CONFIG/BIShared/OracleBISchedulerComponent/coreapplication_obisch1

3. Update the SchedulerScriptPath and DefaultScriptPath elements of the Oracle BI Scheduler instanceconfig.xml file, as follows:

- SchedulerScriptPath: Refers to the path where Oracle BI Scheduler-created job scripts are stored. Change this to the path of the shared BI Scheduler scripts location.
- DefaultScriptPath: Specifies the path where user-created job scripts (not agents) are stored. Change this to the path of the shared BI Scheduler scripts location.

The instanceconfig.xml files for Oracle BI Scheduler are in the following locations:

On *BIHOST1:*: *APPLICATIONS_CONFIG*/BIInstance/config/OracleBISchedulerComponent/coreapplication_obisch1

On *BIHOST2:* *APPLICATIONS_CONFIG*/BIInstance1/config/OracleBISchedulerComponent/coreapplication_obisch1

You must update these files for each Oracle BI Scheduler component in the deployment.

4. Restart the Oracle BI Scheduler component.

   On *BIHOST1*:

```
$ cd APPLICATIONS_CONFIG/BIInstance/bin
$ ./opmnctl stopproc
ias-component=coreapplication_obisch1
$ ./opmnctl startproc
ias-component=coreapplication_obisch1
```

   On *BIHOST2*:

```
$ cd APPLICATIONS_CONFIG/BIInstance1/bin
$ ./opmnctl stopproc
ias-component=coreapplication_obisch1
$ ./opmnctl startproc
ias-component=coreapplication_obisch1
```

Additional Configuration Tasks for Oracle Real-Time Decisions

This sections contains information about the following:

- Configuring Oracle Real-Time Decisions clustering
- Adding Oracle RTD system properties to the server start tab

Configuring Oracle Real-Time Decisions Clustering Properties

Perform these steps in Fusion Middleware Control to set up cluster-specific configuration properties for Oracle Real-Time Decisions (Oracle RTD). You only need to perform the steps on one of the nodes in your deployment. You do not need to set cluster-specific configuration properties for Oracle RTD for subsequent nodes.

1. Log in to Fusion Middleware Control (`http://biinternal.mycompany.com/em`).
2. Expand the **Application Deployments** node in the Farm_BIDomain window.
3. Expand **Oracle RTD(11.1.1)(bi_cluster)**.
4. Click any node under it. For example, **Oracle RTD(11.1.1)(bi_server1)**.
5. In the right pane, click **Application Deployment**, and then select **System MBean Browser**.
6. In the System MBean Browser pane, expand **Application Defined MBeans**.
7. For any one of the servers under Oracle RTD, navigate to the MBean and set the attribute, as shown in the following table. Other servers automatically get updated with the value you set.

Table 18–2 Oracle RTD MBean Attributes and Values for Clustering

MBean	Attribute	Value
SDClusterPropertyManager -> Misc	DecisionServiceAddress	`http://biinternal.mycompany.com`

8. Click **Apply**.

Adding Oracle RTD System Properties to the Server Start Tab

After scaling out Oracle RTD, use the Administration Console to add three system properties to the **Server Start** tab of each Managed Server.

1. Log in to the Oracle WebLogic Server Administration Console (`http://biinternal.mycompany.com/console`).

2. Click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**.

   The Summary of Servers page displays.
5. Select **bi_server<1,2>** in the table.

   The settings page for the server displays.
6. Click **Server Start**.
7. Add the following property to the arguments:

```
-Drtd.clusterRegistryJobIntervalMs=12000
-Drtd.clusterDepartureThresholdMs=50000
-Drtd.clusterDepartureThreshold2Ms=50000
```

8. Click **Save** and then **Activate Changes**.
9. Restart the `bi_server<1,2>` Managed Server (ensure sure that Node Manager is up and running):
   a. In the Summary of Servers screen, select the **Control** tab.
   b. Select **bi_server<1,2>** in the table and then click **Shutdown**.
   c. Select **bi_server<1,2>** in the table and then click **Start**.
10. Restart the BI System Components on *BIHOST1* and *BIHOST2*:

```
$ cd APPLICATIONS_CONFIG/BIInstancen/bin
$ ./opmnctl stopall
$ ./opmnctl startall
```

Performing this task enables an instance of Oracle RTD to be migrated successfully from one host to another in the event of a failure of a Managed Server.

Even after these changes, if the server migration finishes in less than 50 seconds, the Oracle RTD batch framework will be in an inconsistent state.

If the enterprise has deployed any RTD Inline Services that host Batch Job implementations, and if after a server migration the batch console command, "batch-names", or its brief name, "bn", shows no registered batch jobs, then the Oracle RTD Batch Manager service must be stopped and restarted. To do this, perform these steps:

1. In Fusion Middleware Control, expand the **WebLogic Domain** node in the left pane. Then, right-click **BIDomain** and select **System MBean Browser**.
2. Locate **SDPropertyManager > Misc MBean** under **Application Defined MBeans > OracleRTD > Server:bi_server*n***.

   Be sure to select the **Misc MBean** that corresponds to the local node where you are making the change. For example, if you are connecting to *APPHOST1*, then make sure to update the attribute associated with `bi_server1`.
3. Set the **BatchManagerEnabled** attribute to **false** and click **Apply**.
4. Set the **BatchManagerEnabled** attribute back to **true** and click **Apply**. Performing this task causes the Batch Manager to stop and be restarted.

   When it restarts, it will be running on either the same server as before, or on a different server.

5. After restarting Batch Manager, note that the corresponding MBean does not always immediately get refreshed on the server where Batch Manager comes back up, so this is not a concern. Instead, verify that Batch Manager is now operational by using the Batch Console tool:

   a. Locate the zip file for the Oracle RTD client tools in the following location:

      APPLICATIONS_BASE/fusionapps/bi/clients/rtd/rtd_client_11.1.1.zip

   b. Because most Oracle RTD client tools do not run on UNIX, unzip this file in a location on a Windows machine (referred to here as *RTD_HOME*). Then, locate the batch console jar file in:

      RTD_HOME/client/Batch/batch-console.jar

   c. Change to this directory and execute the jar, passing to it the URL and port of either the Managed Server, or of the cluster proxy:

      ```
      java -jar batch-console.jar -url http://SERVER:PORT
      ```

   d. When prompted, enter the user name and password of a user who is a member of the Administrator role, BI_Adminstrator role, or some other role authorized to administer Oracle RTD batch jobs.

   e. When prompted for a command, enter `bn`:

      ```
      Checking server connection...
      command: bn
          CrossSellSelectOffers
      command:quit
      ```

      If Batch Manager has successfully restarted, then the `bn` command lists the names of all batch implementations hosted by all deployed RTD Inline Services.

      The commonly deployed example, CrossSell, hosts a batch implementation named CrossSellSelectOffers, shown in the preceding example.

Additional Configuration Tasks for Oracle BI Publisher

Perform the steps in this section on each machine where Oracle BI Publisher is configured.

Configuring Integration with Oracle BI Presentation Services

To configure Oracle BI Publisher integration with Oracle BI Presentation Services:

1. Log in to Oracle BI Publisher (`http://biinternal.mycompany.com/xmlpserver`) with Administrator credentials and select the **Administration** tab.
2. Under **Integration**, select **Oracle BI Presentation Services**.
3. Verify and update the following:
   - **Server Protocol:** http
   - **Server:** biinternal.mycompany.com
   - **Port:** 80
   - **URL Suffix:** analytics-ws/saw.dll
4. Click **Apply**.
5. Under System Maintenance, select **Server Configuration**.

In the Catalog section, change the BI Publisher Repository value to the shared location for the Configuration Folder. For example:

APPLICATIONS_CONFIG/BIShared/BIPublisher/repository

6. Click **Apply**.
7. Restart your Oracle BI Publisher application:
   a. Log in to the Administration Console (http://biinternal.mycompany.com/console).
   b. Click **Deployments** in the Domain Structure window.
   c. Select **bipublisher(11.1.1)**.
   d. Click **Stop**, and then select **When Work Completes** or **Force Stop Now**.
   e. After the application has stopped, click **Start** and then **Start Servicing All requests**.

Setting the Oracle BI Enterprise Edition Data Source

The Oracle BI EE Data Source must point to the clustered Oracle BI Servers through the Cluster Controllers. Perform this task in Oracle BI Publisher.

To set the Oracle BI EE data source in Oracle BI Publisher:

1. Log in to Oracle BI Publisher (http://biinternal.mycompany.com/xmlpserver) with Administrator credentials and select the **Administration** tab.
2. Under **Data Sources**, select **JDBC Connection**.
3. Update the Oracle BI EE data source setting by changing the **Connection String** parameter to the following:

   jdbc:oraclebi://*primary_cluster_controller_host*:*primary_cluster_controller_port*/PrimaryCCS=*primary_cluster_controller_host*;PrimaryCCSPort=*primary_cluster_controller_port*;SecondaryCCS=*secondary_cluster_controller_host*;SecondaryCCSPort=*secondary_cluster_controller_port*;

   For example:

   jdbc:oraclebi://*BIHOST1*:10212/PrimaryCCS=*BIHOST1*;PrimaryCCSPort=10212;SecondaryCCS=*BIHOST2*;SecondaryCCSPort=10212;

   Note: Since the Cluster Controller Port may be different between *BIHOST1* and *BIHOST2*, you can use the following procedure to check the port being used:

   1. Log in to the Oracle Enterprise Manager Console: http://biinternal.mycompany.com/em.
   2. Expand **Farm_Domain > Business Intelligence > coreapplication**.
   3. Navigate to **Availability**.
   4. Check the port number used by the Cluster Controller on *BIHOST1* and *BIHOST2*.

4. Do one of the following:
   - Select **Use System User**.
   - Deselect **Use System User** and specify BIImpersonateUser credentials.

For more information, see "Credentials for Connecting to the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware Developer's Guide for Oracle Business Intelligence Enterprise Edition*.

5. Click **Test Connection**. You should receive a "Connection established successfully" message.
6. Click **Apply**.

Configuring Java Message Service for Oracle BI Publisher

You must configure the location for the persistence store to the Oracle Fusion Applications database.

On *BIHOST2*:

1. Log in to the Oracle WebLogic Server Administration Console (`http://biinternal.mycompany.com/console`).
2. In the Domain Structure window, expand the **Services** node and then click the **Persistence Stores** node. The Summary of Persistence Stores page is displayed.
3. Click **Lock & Edit**.
4. Click **New**, and then **Create JDBCStore**.
5. Enter a name (for example, `BipJDBCStore-bi_server2`) and target (for example, `bi_server2`). Select **bip_datasource** as the data source, and enter `Bip_bi_server2_` as the prefix name.
6. Click **OK** and then **Activate Changes**.
7. In the Domain Structure window, expand the **Services** node and then click the **Messaging > JMS Servers** node. The Summary of JMS Servers page is displayed.
8. Click **Lock & Edit**.
9. Click **New**.
10. Enter a name (for example, `BipJmsServer-bi_server2`) and in the **Persistence Store** drop-down list, select **BipJDBCStore-bi_server2** and click **Next**.
11. Select **bi_server2** as the target.
12. Click **Finish** and **Activate Changes**.
13. In the Domain Structure window, expand the **Services** node and then click the **Messaging > JMS Modules** node. The JMS Modules page is displayed.
14. In the Change Center, click **Lock & Edit**.
15. Click **BipJmsResource** and then click the **Subdeployments** tab.
16. Select **BipJmsSubDeployment** under **Subdeployments**.
17. Add the new Oracle BI Publisher JMS Server (**BipJmsServer-bi_server2**) as an additional target for the subdeployment.
18. Click **Save** and then **Activate Changes**.

To validate, do the following:

1. Log in to each Oracle BI Publisher URL.
2. Navigate to **Administration > System Maintenance > Scheduler Diagnostics**.

   All statuses should be in a Passed state and both instances should be visible.

Additional Configuration Tasks for Oracle Business Intelligence for Microsoft Office

The information in this section tells you how to do the following:

- Configure Oracle Business Intelligence for Microsoft Office properties
- Validate Oracle Business Intelligence for Microsoft Office

Configuring Oracle Business Intelligence for Microsoft Office Properties

To perform additional configuration tasks for Oracle Business Intelligence for Microsoft Office:

1. Validate the Oracle BI Enterprise Edition Office Server setup by accessing `http://biinternal.mycompany.com/bioffice/about.jsp`.

   The About Oracle BI EE Office Server page displays.

2. Go to the Oracle BI Enterprise Edition Office Server directory. For example:

   APPLICATIONS_CONFIG`/domains/`*BIHOST1*`/BIDomain/servers/bi_server1/tmp/_WL_user/bioffice_11.1.1/cvsibb/war/WEB-INF`

   If you are not sure how to locate the Oracle BI Enterprise Edition Office Server directory, check the **LogDir** parameter on the About Oracle BI EE Office Server page. The Oracle BI Enterprise Edition Office Server directory is the parent directory of the log directory.

   Note: You can determine the exact location for *BIHOSTn* by using the following URL: `http://BIVHn:10217/bioffice/about.jsp`.

3. On both*BIHOST1* and *BIHOST2*, open bioffice.xml for editing and modify the BI Office properties shown in the following table.

Table 18–3 BI Office Properties in bioffice.xml

Property Name	Valid Value	Description
SawBaseURL	http://biinternal.mycompany.com/analytics/saw.dll or http://biinternal.mycompany.com/analytics-ws/saw.dll	Load Balancer Virtual Server Name URL for Oracle BI Presentation Services. **Important:** If SSO is enabled, then enter the URL for the protected analytics servlet that you deployed when configuring BI Office to integrate with the SSO-enabled Oracle BI Server. The URL that is specified for this property is used for Web services requests between the BI Office Server and Presentation Services.
SawUseSSO	0 = No (Default) 1 = Yes	Set this property to `1` if the Oracle Business Intelligence implementation is enabled for SSO.
SawWebURLforSSO	http://biinternal.mycompany.com/analytics/saw.dll	When SSO is enabled, use this property to enter the public URL that allows external users to access Oracle Business Intelligence using SSO from the Oracle BI Add-in for Microsoft Office.

4. Restart the BI Office application:
   a. Log in to the Administration Console (`http://biinternal.mycompany.com/console`).
   b. Click **Deployments** in the Domain Structure window.
   c. Select **bioffice(11.1.1)**.
   d. Click **Stop**.
   e. After the application has stopped, click **Start**.
5. Validate that the **SawBaseURL** parameter has been updated on the About Oracle BI EE Office Server page.

Validating Oracle Business Intelligence for Microsoft Office

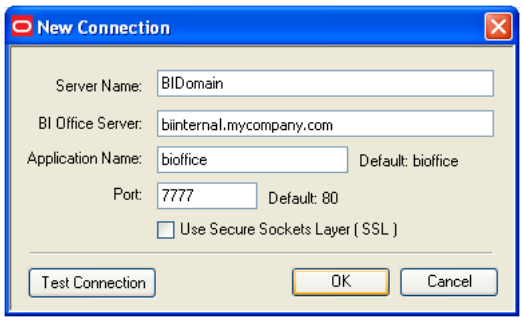
To validate configuration for Oracle Business Intelligence for Microsoft Office:

1. Log in to Oracle BI Presentation Services at:

   `http://biinternal.mycompany.com/analytics`
2. In the lower left pane, under the Get Started heading, select **Download BI Desktop Tools** and then select **Oracle BI for MS Office**.
3. Install Oracle BI for Microsoft by running the Oracle BI Office InstallShield Wizard.
4. Open Microsoft Excel or Microsoft PowerPoint.
5. From the **Oracle BI** menu, select **Preferences**.
6. In the **Connections** tab, select **New**.
7. Enter values for the following fields:
   - **Server Name:** Provide a name for the connection.
   - **BI Office Server:** Provide the URL for the Oracle BI Office Server.
   - **Application Name:** Enter the Application Name that you defined for the Oracle BI Office Server when you deployed the Oracle BI Office Server application to Oracle WebLogic Server. The default name is **bioffice**.
   - **Port:** Enter the Oracle BI Office Server port number.

   The following figure shows the New Connection dialog.

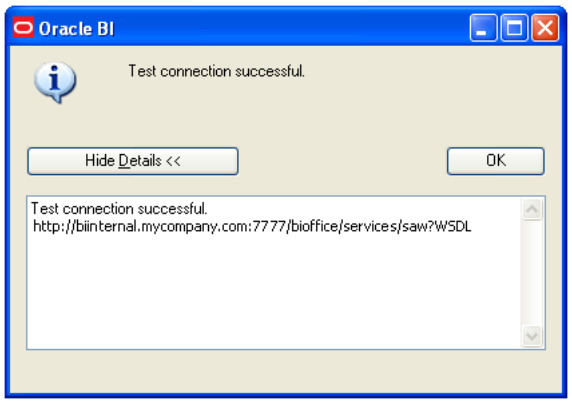
Figure 18–1 New Connection Dialog for Oracle BI Office



8. Click **Test Connection** to test the connection between the add-in and the Oracle BI Office Server.

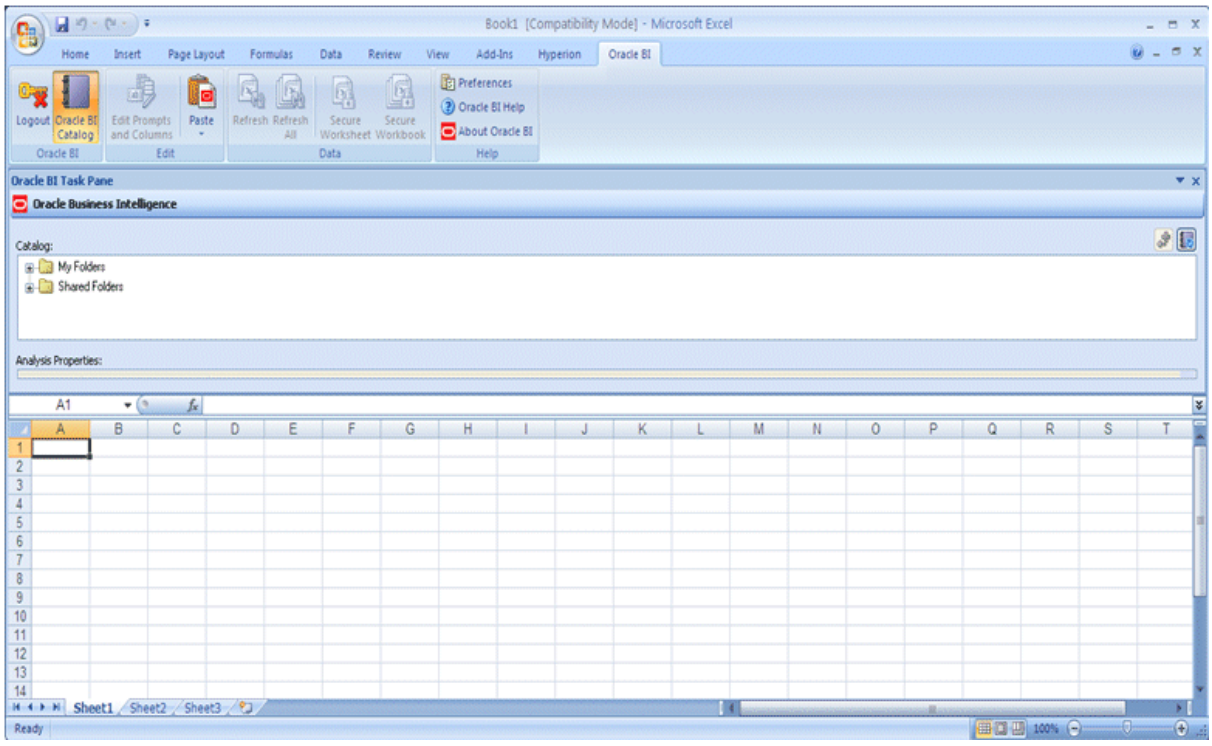
Successful connections receive a "Test connection successful" message, as shown in the following figure.

Figure 18–2 Test Connection Successful Message



9. Log in as an Administrator (for example, `weblogic`) and validate that you can access the Oracle BI Task Pane, as shown in the following figure.

Figure 18–3 Oracle BI Task Pane in Microsoft Excel



Additional Configuration Tasks for Oracle Financial Reporting

There are additional configuration tasks to perform for Oracle Financial Reporting. Do the following on *`BIHOST1`* and *`BIHOST2`*:

1. Update the `VARIABLE_VALUE_LIMIT` from 4096 to 3072000 in the `NQSConfig.INI` file. For example,

```
VARIABLE_VALUE_LIMIT = 3072000;
```

On *BIHOST1*, this file is located in *APPLICATIONS_CONFIG*/BIInstance/config/OracleBIServerComponent/coreapplication_obis1.

On *BIHOST2*, this file is located in *APPLICATIONS_CONFIG*/BIInstance1/config/OracleBIServerComponent/coreapplication_obis1.

2. Run the following commands to restart the Oracle Business Intelligence system components on *BIHOST1* and *BIHOST2*:

```
$ cd APPLICATIONS_CONFIG/BIInstancen/bin
$ ./opmnctl stopall
$ ./opmnctl startall
```

18.2.7.5.7 Configuring a Default Persistence Store for Transaction Recovery Each server has a transaction log that stores information about committed transactions that are coordinated by the server that may not have been completed. The Oracle WebLogic Server uses this transaction log for recovery from system crashes or network failures. To leverage the migration capability of the Transaction Recovery Service for the servers within a cluster, store the transaction logs in the Oracle Fusion Applications database.

To set the location for the default persistence store:

1. Log in to the Oracle WebLogic Server Administration Console (http://biinternal.mycompany.com/console).
2. In the Change Center, click **Lock & Edit**.
3. In the Domain Structure window, expand the **Environment** node and then click the **Servers** node. The Summary of Servers page is displayed.
4. Click **bi_server2** in the table. The Settings page for the selected server is displayed, and defaults to the Configuration tab.
5. Navigate to **Configuration > Services**.
6. In the Transaction Log Store section of the page, do the following:
   - For the type, select **JDBC** from the dropdown list. list.
   - For the data store, select **bip_datasource** from dropdown list.
   - For the prefix name, enter TLOG_bi_server2_.
7. Click **Save**.
8. Click **Activate Changes**.
9. Restart bi_server2 to activate the changes:
   a. Log in to the Oracle WebLogic Server Administration Console (http://biinternal.mycompany.com/console).
   b. In the Summary of Servers screen, select the **Control** tab.
   c. Select **bi_server2** in the table and then click **Shutdown**.
   d. Start the bi_server2 server.
   e. Restart the Oracle Business Intelligence system components on *BIHOST2*:

```
$ cd APPLICATIONS_CONFIG/BIInstance1/bin
$ ./opmnctl stopall
$ ./opmnctl startall
```

18.2.7.5.8 Starting and Validating Oracle Business Intelligence on BIHOST2 This information in this section tells you how to do the following:

- Start the `bi_server2` Managed Server
- Start the Oracle Business Intelligence system components
- Validate Oracle Business Intelligence URLs

Starting the bi_server2 Managed Server

To start the `bi_server2` Managed Server:

1. Start the `bi_server2` Managed Server using the Oracle WebLogic Server Administration Console, as follows:
   a. Log in to the Oracle WebLogic Server Administration Console (`http://biinternal.mycompany.com/console`).
   b. Expand the **Environment** node in the **Domain Structure** window.
   c. Select **Servers**. The Summary of Servers page is displayed.
   d. Click the **Control** tab.
   e. Select **bi_server2** and then click **Start**.
2. Verify that the server status is reported as "Running" in the Administration Console. If the server is shown as "Starting" or "Resuming," wait for the server status to change to "Started." If another status is reported (such as "Admin" or "Failed"), check the server output log files for errors.

Starting the Oracle Business Intelligence System Components

You can control Oracle Business Intelligence system components using `opmnctl` commands.

To start the Oracle Business Intelligence system components using the `opmnctl` command-line tool:

1. Go to the directory that contains the Oracle Process Manager and Notification Server command-line tool, located in *`APPLICATIONS_CONFIG`*`/BIInstance1/bin`.
2. Run the `opmnctl` command to start the Oracle Business Intelligence system components:
   - `./opmnctl startall`: Starts Oracle Process Manager and Notification Server and all Oracle Business Intelligence system components
   - `./opmnctl start`: Starts Oracle Process Manager and Notification Server only
   - `./opmnctl startproc ias-component=`*`component_name`*: Starts a particular system component. For example, where `coreapplication_obips1` is the Presentation Services component:

     ```
     ./opmnctl startproc ias-component=coreapplication_obips1
     ```

3. Check the status of the Oracle Business Intelligence system components:

   ```
   ./opmnctl status
   ```

Validating Oracle Business Intelligence URLs

Access the following URLs:

- Access `http://BIVH2:10217/analytics` to verify the status of `bi_server2`.

- Access `http://BIVH2:10217/wsm-pm` to verify the status of Web Services Manager. Click **Validate Policy Manager**. A list of policies and assertion templates available in the data is displayed.

  Note: The configuration is incorrect if no policies or assertion templates appear.
- Access `http://BIVH2:10217/xmlpserver` to verify the status of the Oracle BI Publisher application.
- Access `http://BIVH2:10217/ui` to verify the status of the Oracle Real-Time Decisions application.
- Access `http://BIVH2:10217/mapviewer` to verify the status of the map view functionality in Oracle BI EE.
- Access `http://BIVH2:10217/hr` to verify Financial Reporting.
- Access `http://BIVH2:10217/calcmgr/index.htm` to verify Calculation Manager.
- Access `http://BIVH2:10217/aps/Test` to verify APS.
- Access `http://BIVH2:10217/workspace` to verify workspace.

18.2.7.5.9 Validating Access Through Oracle HTTP Server You should verify URLs to ensure that the appropriate routing and failover is working from Oracle HTTP Server to bi_cluster. Perform these steps to verify the URLs:

1. While `bi_server2` is running, stop `bi_server1` using the Oracle WebLogic Server Administration Console.
2. Access the following URLs to verify that routing and failover is functioning properly:
   - `http://WEBHOST1:10621/analytics`
   - `http://WEBHOST1:10621/xmlpserver`
   - `http://WEBHOST1:10621/ui` (access only available on Microsoft Internet Explorer 7 or 8)
   - `http://WEBHOST1:10621/hr`
   - `http://WEBHOST1:10621/calcmgr/index.htm`
   - `http://WEBHOST1:10621/aps/Test`
   - `http://WEBHOST1:10621/workspace`
3. Start `bi_server1` from the Oracle WebLogic Server Administration Console.
4. Stop `bi_server2` from the Oracle WebLogic ServerAdministration Console.
5. Access the following URLs to verify that routing and failover is functioning properly:
   - `http://WEBHOST1:10621/analytics`
   - `http://WEBHOST1:10621/xmlpserver`
   - `http://WEBHOST1:10621/ui` (access only available on Microsoft Internet Explorer 7 or 8)
   - `http://WEBHOST1:10621/hr`
   - `http://WEBHOST1:10621/calcmgr/index.htm`
   - `http://WEBHOST1:10621/aps/Test`
   - `http://WEBHOST1:10621/workspace`

6. Start `bi_server2` from the Oracle WebLogic ServerAdministration Console.

18.2.7.5.10 Configuring Node Manager for the Managed Servers Oracle recommends using host name verification for the communication between Node Manager and the servers in the domain. This requires the use of certificates for the different addresses communicating with the Administration Server and other servers. See Section 18.2.2, "Scaling Out Node Manager." for further details. The procedures in that chapter must be performed twice using the information provided in the following table.

Table 18–4 Details for Host Name Verification for Node Manager and Servers

Run	Host Name (Host)	Server Name (WLS_SERVER)
Run1:	*BIHOST1*	bi_server1
Run2:	*BIHOST2*	bi_server2

> **Note:** If you configured Node Manager for the Managed Servers earlier, you do not need to configure it again.

18.2.7.5.11 Configuring Server Migration for the Managed Servers Server migration is required for proper failover of the Oracle BI Publisher components in the event of failure in any of the *BIHOST1* and *BIHOST2* nodes. For more information, see Section 18.3, "Setting Up Server Migration for Oracle Fusion Applications."

18.2.7.6 Configuring and Validating Oracle Essbase Clustering

This section describes how to configure and validate secondary instances of Oracle Essbase Agent so that they are distributed for high availability.

> **Note:** In Oracle Fusion Applications, Oracle Essbase can only connect to and work with the primary server instance of an Oracle Real Application Clusters (Oracle RAC) database. If, for any reason, there is an Oracle RAC database failover to a secondary server instance, Oracle Essbase will not work.

Perform the following steps in Fusion Middleware Control to scale out the secondary Oracle Essbase Agent:

1. Log in to Fusion Middleware Control (`http://biinternal.mycompany.com/em`).
2. Expand the **Business Intelligence** node in the Farm_BIDomain window.
3. Click **coreapplication**.
4. Click **Availability**, then click **Failover**.
5. Click **Lock and Edit Configuration** to activate the Primary/Secondary Configuration section of the **Availability** tab.
6. Specify the Secondary Host/Instance for Essbase Agent.
7. Ensure the **Shared Folder Path** is set to *APPLICATIONS_CONFIG*`/BIShared/Essbase/essbaseserver1` and click **Apply**.
8. Click **Activate Changes**.
9. Under Manage System, click **Restart**.

10. Click **Yes** in the confirmation dialog.

> **Note:** Under Potential Single Points of Failure, no problems should be reported for Essbase Agent.

Do the following to validate Essbase clustering:

1. Check the APS (Hyperion Provider Services) test URL:

   ```
   http://biinternal.mycompany.com/aps/Essbase?Clustername=Essbase_FA_Cluster
   ```

   The message "Hyperion Provider Services: Hello!" should display.

2. Run the following command on *BIHOST1*:

   ```
   APPLICATIONS_CONFIG/BIInstance/bin/opmnctl stopproc
   ias-component=essbaseserver1
   ```

3. Ensure that Essbase starts on *BIHOST2*:

   ```
   APPLICATIONS_CONFIG/BIInstance1/bin/opmnctl status
   ```

   The status should be `init` then `Alive`.

4. Check the APS test URL again:

   ```
   http://biinternal.mycompany.com/aps/Essbase?Clustername=Essbase_FA_Cluster
   ```

18.2.7.7 Validating the System

You should verify URLs to ensure that the appropriate routing and failover is working from Oracle HTTP Server to `bi_cluster`. Perform these steps to verify the URLs:

1. While `bi_server2` is running, stop `bi_server1` using the Oracle WebLogic Server Administration Console.
2. Access the following URLs to verify that routing and failover is functioning properly:
   - `http://WEBHOST1:10621/analytics`
   - `http://WEBHOST1:10621/xmlpserver`
   - `http://WEBHOST1:10621/ui` (access only available on Microsoft Internet Explorer 7 or 8)
   - `http://WEBHOST1:10621/hr`
   - `http://WEBHOST1:10621/workspace`
   - `http://WEBHOST1:10621/calcmgr/index.htm`
   - `http://WEBHOST1:10621/aps/Test`
3. Start `bi_server1` from the Oracle WebLogic Server Administration Console.
4. Stop `bi_server2` from the Oracle WebLogic Server Administration Console.
5. Access the following URLs to verify that routing and failover is functioning properly:
   - `http://WEBHOST1:10621/analytics`
   - `http://WEBHOST1:10621/xmlpserver`

- http://WEBHOST1:10621/ui (access only available on Microsoft Internet Explorer 7 or 8)
- http://WEBHOST1:10621/hr
- http://WEBHOST1:10621/workspace
- http://WEBHOST1:10621/calcmgr/index.htm
- http://WEBHOST1:10621/aps/Test

6. Start bi_server2 from the Oracle WebLogic Server Administration Console.

18.2.8 Scaling Up: Adding Managed Servers to Existing Hosts

You can scale out and or scale up an Oracle Fusion Applications environment. When you scale out, you add a new instance of a Managed Server to a new host (called *SCALED_OUT_HOST* in previous sections) that does not already have the Managed Server running in it. When you scale up, you are adding a new instance of a Managed Server in an existing host (either a *PROVISIONED_HOST* or *SCALED_OUT_HOST*) that already has one or more instances of the Managed Server running in it.

This section describes how to scale up an environment by adding a new instance of a Managed Server to an existing host, called *SCALED_UP_HOST*. Note that a *SCALED_UP_HOST* is one of the *PROVISIONED_HOST* or *SCALED_UP_HOST* that are already part of the Oracle Fusion Applications environment. For clarity in this section, we use *SCALED_UP_MGD_SERVER* to denote the Managed Server to be scaled up.

This section tells you how to do the following:

- Scale up the topology (add Managed Servers to an existing node) for Oracle ADF server
- Scale out the topology (add Managed Servers to a new node) for Oracle SOA Suite server
- Scale up the topology (add Managed Servers to an existing node) for Oracle SOA Suite server
- Scale up the topology (add Managed Servers to an existing node) for Oracle Business Intelligence

18.2.8.1 Scaling Up Oracle Fusion Applications Managed Servers to an Existing Host

Before performing the tasks in this section, ensure that the Managed Server (*SCALED_UP_MGD_SERVER*) to be scaled up and its domain (referred to as *domain*) is running.

18.2.8.1.1 Cloning Managed Servers and Assigning Them to SCALED_UP_HOST To add a Managed Server (*SCALED_UP_MGD_SERVER*) and assign it to *SCALED_UP_HOST*:

1. Log in to the Administration Server: http://*domain_name*internal.mycompany.com/console.
2. Navigate to ***Domain_Name*** **> Environment > Servers**.
3. Switch to **Lock & Edit** mode.
4. Select the ***SCALED_UP_MGD_SERVER*** checkbox and then click **Clone**.
5. Specify the following Server Identity attributes:
   - Server Name - *SCALED_UP_MGD_SERVER_n*

Note: To ensure consistency in naming, copy the name of the server shown in **Server Identity** and paste it into the **Server Name** field. Increase the number of instances of *SCALED_UP_MGD_SERVER* by one and use that number to replace "*n*" at the end of the server name. Oracle recommends following the managed server naming convention *NamedManagedServer_n*.

- Server Listen Address - <*SCALED_UP_HOST*> (This is the existing host where the new instance of *SCALED_UP_MGD_SERVER* will be added.)
- Server Listen Port - Give an unused port on the machine *SCALED_UP_HOST*

6. Click **OK**.
7. Navigate back to ***Domain_Name*** **> Environment > Servers**. You now should see the newly cloned server, *SCALED_UP_MGD_SERVER_n*.
8. From **SCALED_UP_MGD_SERVER_*n***, click **Advanced** and then select the **WebLogic Plug-In Enabled** checkbox.
9. Click **Save** and then click **Activate Changes**.
10. Run the newly created Managed Server:
    a. Navigate to ***Domain_Name*** **> Environment**.
    b. From the **Navigation** pane on the Oracle WebLogic Server console, select **Activate Changes**.
    c. Navigate to ***Domain_Name*** **> Environment > Servers > Control**.
    d. Check the newly created Managed Server and click **Start**.
    e. Navigate to ***Domain_Name*** **> Environment > Servers** and check the **State** to verify that the newly created Managed Server is running.
11. Log in to the Administration Server once again (`http://`*`domain_name`*`internal.mycompany.com/console`) and verify that all the Managed Servers, including the new instance of the scaled-up Managed Server, are running.
12. Do the following:
    a. Switch to **Lock & Edit** mode.
    b. Select the ***SCALED_UP_MGD_SERVER*** checkbox.
    c. Select the **Server Start** tab.
    d. Change the Arguments to reflect the name of your cloned Managed Server and make sure the server group is the correct cluster name. For example, you should see the following:

```
-DJDBCProgramName\=DS/domain_name/SCALED_UP_MGD_SERVER_n
-Dserver.group\=SCALED_UP_MGD_SERVERCluster
```

Note: The naming convention of a *SCALED_UP_MGT_SERVER_CLUSTER* is the name of the managed server appended with "Cluster" after dropping "Server_n". For example, if *SCALED_UP_MGD_SERVER_n* is HomePageServer_4, its cluster (that is, server group) is HomePageCluster.

e. Click **Save**.

13. Select the **Logging** tab, and then select the **HTTP** tab.
14. Do the following:
    a. Change the Log file name to `logs/access.log.%yyyyMMdd%`.
    b. Change the rotation type to **By Time**.
    c. Leave the **Limit number of retained files** option unchecked.
    d. Leave the **Rotate log file on startup** option unchecked.
    e. Click **Save**.
    f. Expand **Advanced**.
    g. Change the format to **Extended**.
    h. Change the extended logging format fields to the following:

```
date time time-taken cs-method cs-uri
sc-status sc(X-ORACLE-DMS-ECID)
cs(ECID-Context) cs(Proxy-Remote-User)
cs(Proxy-Client-IP)
```

    i. Click **Save**.
15. Click **Activate Changes**.
16. Restart the *SCALED_UP_MGD_SERVER_n* for the changes to take affect.

18.2.8.1.2 Validating the System You should verify URLs to ensure that the appropriate routing and failover are working.

To verify the URLs:

1. Log in to the domain's Oracle WebLogic Server Administration Console and stop all the instances of *SCALED_UP_MGD_SERVER* currently running in *SCALED_UP_HOST*, *PROVISIONED_HOST*, and *SCALED_OUT_HOST*, where applicable. (Also stop *SCALED_UP_MGD_SERVER_n* that you just added.)
2. Do the following:
    a. Edit the `FusionVirtualHost_`*domain*`.conf` file where *domain* takes the value of `fs` (Common domain), `crm`, `fin`, `hcm`, `ic`, `scm`, and so on, depending on the domain that you are working with.

> **Note:** If the *SCALED_UP_HOST*'s host and port do not already exist in the *SCALED_UP_MGT_SERVER* entry, complete Steps b and c. Otherwise, skip to Step 3.

    b. Locate the name (in lower case) of the scaled-up Managed Server in the file. Add the value *SCALED_UP_HOST*`:port` to the WebLogicCluster property. Note that there are two parts, internal and external, in the `FusionVirtualHost_`*domain*`.conf` file on *WEBHOST*. The *SCALED_UP_HOST*`:port` must be added to both the internal and external parts. If you scale out web tier to *WEBHOST2* and others, do the same on these hosts as well.

       The following is an example of scaling up the `HomePage` Managed Server, and what the *SCALED_UP_HOST*`:port` looks like in the `<Location> xml` element in the `FusionVirtualHost_fs.conf` file

```
<Location /homepage>
   SetHandler weblogic-handler
   WebLogicCluster <PROVISIONED_HOST:port>,<SCALED_UP_HOST:port>,
   <SCALED_OUT_HOST:port>
   WLProxySSL ON
   WLProxySSLPassThrough ON
   RewriteEngine On
   RewriteOptions inherit
</Location>
```

c. Restart Oracle HTTP Server on both *WEBHOST1* and all other web-tier hosts, where applicable.

3. Log in to the domain's Oracle WebLogic Server Administration Console and start the *SCALED_UP_MGD_SERVER_n* Managed Server. Begin with n=1.
4. Access the URL of the application deployed to the *SCALED_UP_MGD_SERVER* from a different machine to verify that routing and failover are functioning properly.

   Close all browser windows then open a new one to ensure that the Oracle Fusion Applications login window displays correctly. The URL for the HomePage Managed Server for example, is:

   https://*domain*external.mycompany.com/homePage/faces/AtkHomePageWelcome
5. Log in to the domain's Oracle WebLogic Server Administration Console and stop the *SCALED_UP_MGD_SERVER_n* Managed Server that you started in Step 3.
6. Repeat Steps 3 through 5 for the other instances of the *SCALED_UP_MGD_SERVER* that you have.
7. After completing validation, start all instances of *SCALED_UP_MGD_SERVER*.

18.2.8.2 Scaling Up Oracle SOA Suite Server to an Existing Host

Before performing the procedures in this section, ensure that CommonDomain and its Managed Servers are running.

18.2.8.2.1 Cloning Managed Servers and Assigning Them to SCALED_UP_HOST To add a Managed Server and assign it to *SCALED_UP_HOST*:

1. Log in to the Administration Server: http://*domain_name*internal.mycompany.com/console.
2. Navigate to ***Domain_Name*** **> Environment > Servers**.
3. Switch to **Lock & Edit** mode.
4. Select the ***Managed_Servers*** checkbox (for example, **soa_server1**) and then click **Clone**.
5. Specify the following Server Identity attributes:
   - Server Name - soa_server*n*

Note: To ensure consistency in naming, copy the name of the server shown in **Server Identity** and paste it into the **Server Name** field. Increase the total number of instances of soa_server in this domain by one and use that number to replace *n* at the end of the server name. Oracle recommends following the Oracle SOA Suite server naming convention soa_server*n*.

- Server Listen Address - <*SCALED_UP_HOST*>
- Server Listen Port - Give an unused port on the machine *SCALED_UP_HOST*

6. Click **OK**.
7. Navigate back to ***Domain_Name***. You now should see the newly cloned SOA server, `soa_server`*n*.
8. Do the following:
   a. Click **soa_server*n***.
   b. From the **General** tab, select **Advanced** and then select the **WebLogic Plug-In Enabled** checkbox.
9. Click **Save** and then **Activate Changes**.
10. Run the newly created Managed Servers:
    a. Navigate to ***Domain_Name***.
    b. From the **Navigation** pane on the Oracle WebLogic Server console, select **Activate Changes**.
    c. Navigate to ***Domain_Name***.
    d. Check the newly created Managed Servers and click **Start**.
    e. Navigate to ***Domain_Name*** and check the **State** to verify that the newly created Managed Servers are running.
11. Log in to the Administration Server once again (`http://`*domain_name*`internal.mycompany.com/console`) and verify that all the Managed Servers, including scaled-up servers, are running.
12. Do the following:
    a. Switch to **Lock & Edit** mode.
    b. Select the ***Managed_Server*** checkbox (for example, **soa_server*n***).
    c. Select the **Server Start** tab.
    d. Change the Arguments to reflect the name of your cloned Managed Server and make sure the server group is the correct cluster name. For example, you should see the following:

       ```
       -DJDBCProgramName\=DS/CommonDomain/soa_servern
       -Dserver.group\=SOACluster
       ```

    e. Click **Save**.
13. Select the **Logging** tab, and then select the **HTTP** tab.
14. Do the following:
    a. Change the Log file name to `logs/access.log.%yyyyMMdd%`.
    b. Change the rotation type to **By Time**.
    c. Leave the **Limit number of retained files** option unchecked.
    d. Leave the **Rotate log file on startup** option unchecked.
    e. Click **Save**.
    f. Expand **Advanced**.
    g. Change the format to **Extended**.

h. Change the extended logging format fields to the following:

```
date time time-taken cs-method cs-uri
sc-status sc(X-ORACLE-DMS-ECID)
cs(ECID-Context) cs(Proxy-Remote-User)
cs(Proxy-Client-IP)
```

i. Click **Save**.

15. Click **Activate Changes**.

16. Restart the Managed Server for the changes to take affect.

18.2.8.2.2 Validating the System You should verify URLs to ensure that the appropriate routing and failover is working from Oracle HTTP Server to the domain's SOACluster.

To verify the URLs:

1. Log in to the domain's Oracle WebLogic Server Administration Console and stop all the instances of `soa_server` currently running in *`SCALED_UP_HOST`*, *`PROVISIONED_HOST`*, and *`SCALED_OUT_HOST`*, where applicable. (Also stop `soa_server`*`n`* that you just added.)

2. Do the following:

   a. Edit the `FusionVirtualHost_`*`domain`*`.conf` file where *`domain`* takes the value of `fs` (Common domain), `crm`, `fin`, `hcm`, `ic`, `scm`, and so on, depending on the domain that you are working with.

   Note: If the *`SCALED_UP_HOST`*'s host and port do not already exist in the `/soa/composer` entry, complete Steps b and c. Otherwise, skip to Step 3.

   b. Locate `/soa/composer` in the file. Add the value *`SCALED_UP_HOST`*`:port` to the WebLogicCluster property. Note that there are two parts, internal and external, in the `FusionVirtualHost_`*`domain`*`.conf` file on *`WEBHOST`*. The *`SCALED_UP_HOST`*`:port` must be added to both the internal and external parts. If you scale out web tier to *`WEBHOST2`* and others, do the same on these hosts as well.

   The following is an example of scaling up the `HomePage` Managed Server, and what the *`SCALED_UP_HOST`*`:port` looks like in the `<Location> xml` element in the `FusionVirtualHost_fs.conf` file

```
<Location /homepage>
   SetHandler weblogic-handler
   WebLogicCluster <DOMAINHOSTSOAVH1:port>, <DOMAINHOSTSOAVH2:port>
   WLProxySSL ON
   WLProxySSLPassThrough ON
   RewriteEngine On
   RewriteOptions inherit
</Location>
```

   c. Restart Oracle HTTP Server on both *`WEBHOST1`* and all other web-tier hosts, where applicable.

3. Log in to the domain's Oracle WebLogic Server Administration Console and start the `soa_server`*`n`* Managed Server. Begin with `n`=1.

4. Access the URL `http://`*`domain_name`*`internal.mycompany.com/soa-infra` to verify that routing and failover are functioning properly.

Close all browser windows then open a new one to ensure that the Oracle Fusion Applications login window displays correctly.

5. Log in to the domain's Oracle WebLogic Server Administration Console and stop the `soa_servern` Managed Server that you started in Step 3.
6. Repeat Steps 3 through 5 for the other instances of the `soa_servern` that you have.
7. After completing validation, start all instances of `soa_servern`.

18.2.8.3 Scaling Up Oracle Business Intelligence to an Existing Host

The procedure in this section allows you to increase the number of instances of system components, such as Oracle Business Intelligence server, Oracle Business Intelligence Presentation Services server, and Oracle Business Intelligence Java host, on *SCALED_UP_HOST*. (Note that it is not necessary to run multiple Oracle Business Intelligence servers on *SCALED_UP_HOST*.)

Before performing the procedure, ensure that BIDomain and its Managed Server and system components are running in an existing host (referred to as *SCALED_UP_HOST*), where it is either a *PROVISIONED_HOST* or *SCALED_OUT_HOST*.

18.2.8.3.1 Scale-Up Procedure for Oracle Business Intelligence To scale up Oracle Business Intelligence on *SCALED_UP_HOST*:

1. Log in to Fusion Middleware Control: `http://biinternal.mycompany.com/em`.
2. Expand the **Business Intelligence** node in the Farm_BIDomain window.
3. Click **coreapplication**.
4. Click **Capacity Management**, then click **Scalability**.
5. Click **Lock & Edit** and then change the number of BI Servers, Presentation Servers, or Java Hosts using the arrow keys.

> **Note:** To avoid port conflicts for the system components being scaled within the given Oracle WebLogic Server instance, enter a different range of available ports in the **Port Range From** and **Port Range To** fields. For example, change **Port Range From** to `10221` and **Port Range To** to `10300`.

6. Click **Apply**, then click **Activate Changes**.
7. Click **Restart** to apply recent changes.
8. Click **Restart** under **Manage System**.
9. Click **Yes** in the confirmation dialog.

18.2.9 Procedures for Scaling Out Oracle SOA Suite Server

This section describes the additional scale-out steps required for the `soa_server1` and `soa_server2` servers on *PROVISIONED_HOST* and *SCALED_OUT_HOST*.

Notes:

- The Oracle SOA Suite server uses the Java Message Service (JMS) server. JMS requires a shared file system for its file store and transactional log. Each Oracle SOA Suite Managed Server in a cluster uses a separate file on the shared folder. During a node failure, the Oracle SOA Suite server must be moved to a targeted node to run the same server using the exact JMS file store and transaction log. To enable this server migration, each Oracle SOA Suite server must be configured with its own virtual IP, which can be floated on any server where the Oracle SOA Suite server is migrated.
- For Java Database Connectivity (JDBC), each Oracle SOA Suite Managed Server in a cluster uses a dedicated table per server on a database using the shared data source connection. During a node failure, the Oracle SOA Suite server must be moved to a targeted node to run the same server using the exact JDBC store and transaction log.

Perform the procedures in this section for the Oracle SOA Suite servers in all domains except the BIDomain, which has no Oracle SOA Suite servers.

Note: For Oracle Fusion Applications, the Oracle SOA Suite virtual IPs *PROVISIONED_HOST* and *SCALED_OUT_HOST* are called *DOMAINHOSTSOAVH1* and *DOMAINHOSTSOAVH2*.

where

DOMAIN is replaced with the domain-specific syntax. For example, *CRMSOAVH1*, *CRMSOAVH2*, *FINSOAVH1*, *HCMSOAVH1*, *ICSOAVH1*, *PROJSOAVH1*, and so on.

18.2.9.1 Scaling Out the Oracle SOA Suite Server

When scaling out the Oracle SOA Suite server, you add new Managed Servers configured to new nodes.

18.2.9.1.1 Prerequisites for Scaling Out the Topology for Oracle SOA Suite Server Before you begin, ensure the following:

- *SCALED_OUT_HOST* Node Manager has been started in the Secure Sockets Layer (SSL) mode
- You are starting with a clean machine if it is the first time it is being used for a scale out
- The `/etc/hosts` file has proper entries. To verify this from the clean machine, ping the hosts listed in `/etc/hosts` files with the fully qualified name of the hosts.
- The user created on *SCALED_OUT_HOST* should the same as the user on *PROVISIONED_HOST*
- The directory structure *APPLICATIONS_BASE* is mounted on*SCALED_OUT_HOST*, and is the same shared file system as used by *PROVISIONED_HOST*
- The directory structure *APPLICATIONS_CONFIG* on *SCALED_OUT_HOST* has been created

- The initial deployment on *PROVISIONED_HOST* has already been done and verified by provisioning

18.2.9.1.2 Adding a New Machine in the Oracle WebLogic Server Console To add a new machine:

1. Stop the domain's Administration Server:

   ```
   PROVISIONED_HOST> APPLICATIONS_CONFIG/domains/PROVISIONED_
   HOST/CommonDomain/bin/stopWebLogic.sh
   ```

2. Set the following variable on *SCALED_OUT_HOST*:

   ```
   WLST_PROPERTIES="-Dweblogic.security.SSL.trustedCAKeyStore=
   APPLICATIONS_BASE/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks"
   ```

3. Start the domain's Administration Server on *SCALED_OUT_HOST*:

   ```
   SCALED_OUT_HOST> APPLICATIONS_BASE/fusionapps/wlserver_10.3/common/bin/wlst.sh

   SCALED_OUT_HOST> nmConnect(username='username', password='password',
   domainName='domain_nameDomain', host='PROVISIONED_HOST',port='5556',
   nmType='ssl', domainDir='APPLICATIONS_CONFIG/domains/PROVISIONED_HOST/''domain_
   nameDomain')

   SCALED_OUT_HOST> nmStart('AdminServer')
   ```

   Note: The *username* and *password* used in the `nmConnect` are the Node Manager credentials (username and password) specified when creating the provisioning response file.

4. Log in to the Administration Server: `http://domain_nameinternal.mycompany.com/console`.
5. Navigate to ***Domain_Name*** **> Environment > Machines**.

   LocalMachine is located in the right-hand pane.
6. In the left-hand pane, click **Lock & Edit**.
7. In the right-hand pane, first click **New** to add the remote machine, and then specify the following:
   - Name - enter *SCALED_OUT_HOST*
   - Machine operating system - Unix
8. Click **Next**.
9. In the window that opens, set the following attributes:
   - Type - SSL
   - Listen Address - <*SCALED_OUT_HOST*>

     Note: The "localhost" default value here is wrong.

   - Listen port - 5556
10. Click **Finish** and activate the changes.

18.2.9.1.3 Packing and Unpacking the Managed Server Domain Home

Since the *PROVISIONED_HOST* domain directory file system is also available from *SCALED_OUT_HOST*, both the `pack` and `unpack` commands can be executed from the *SCALED_OUT_HOST*.

To pack and unpack the Managed Server domain home:

1. Change directory to *APPLICATIONS_BASE*`/fusionapps/oracle_common/common/bin`.
2. Run the `pack` command:

   ```
   SCALED_OUT_HOST> ./pack.sh -managed=true -domain=APPLICATIONS_CONFIG/domains/
   SCALED_OUT_HOST/domain_nameDomain -template=APPLICATIONS_BASE/user_templates/
   domain_nameDomain_managed.jar -template_name="domain_name_Managed_Server_
   Domain"
   ```

3. Run the `unpack` command:

   ```
   SCALED_OUT_HOST> ./unpack.sh -domain=APPLICATIONS_CONFIG/domains/
   SCALED_OUT_HOST/domain_nameDomain -template=APPLICATIONS_BASE/user_templates/
   Managed_Server_Domain.jar
   ```

   Here, *APPLICATIONS_BASE* is shared. If you enable local applications config, replace *APPLICATIONS_CONFIG* with *APPLICATIONS_LOCAL_CONFIG*, which is local to *SCALED_OUT_HOST*.

18.2.9.1.4 Cloning Managed Servers and Assigning Them to SCALED_OUT_HOST

To add a Managed Server and assign it to *SCALED_OUT_HOST*:

1. Log in to the Administration Server: `http://domain_name`internal.mycompany.com/console.
2. Navigate to ***Domain_Name*** **> Environment > Servers**.
3. Switch to **Lock & Edit** mode.
4. Select the ***Managed_Server*** checkbox (for example, **soa_server1**) and then click **Clone**.
5. Specify the following Server Identity attributes:
   - Server Name - `soa_server3`

     Note: To ensure consistency in naming, copy the name of the server shown in **Server Identity** and paste it into the **Server Name** field. Then change the number to "3".

   - Server Listen Address - <*SCALED_OUT_HOST*>
   - Server Listen Port - leave "as is"
6. Click **OK**.
7. Navigate back to ***Domain_Name*** **> Environment > Servers**. You now should see the newly cloned server, `soa_server3`.
8. Click **soa_server3** and change the following attributes:
   - Machine - <*SCALED_OUT_HOST*>
   - Cluster Name - accept the default, SOACluster

Note: Ensure that this cluster name is the same as the cluster name of the original Managed Server.

9. From **soa_server3**, click **Advanced** and then select the **WebLogic Plug-In Enabled** checkbox.
10. Click **Save**.
11. Select the **Keystores** tab, and then ensure that the keystores value is **Custom Identity and Custom Trust**.
12. Do the following:
    a. Change the Custom Identity Keystore path to point to the *APPLICATIONS_BASE*/fusionapps/wlserver_10.3/server/lib/*SCALED_OUT_HOST*_fusion_identity.jks file.
    b. Leave the Custom Identity Keystore type blank.
    c. Change the Custom Identity Keystore Passphrase entry. This should be the same as the *keystorepassword* field described in the first bullet in Step 4 in Section 18.2.2.3, "Creating the Identity Keystore on SCALED_OUT_HOST."
    d. Re-enter the Confirm Custom Identity Keystore Passphrase.
    e. Ensure that the Confirm Custom Trust Keystore path is pointing to the *APPLICATIONS_BASE*/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks file.
    f. Leave the Custom Trust Keystore type blank.
    g. Change the Custom Trust Keystore Passphrase entry. This should be the same as the *keystorepassword* field described in the first bullet in Step 4 in Section 18.2.2.3, "Creating the Identity Keystore on SCALED_OUT_HOST."
    h. Re-enter the Custom Trust Keystore Passphrase.
    i. Click **Save**.
13. Select the **SSL** tab.
    a. Make sure that Identity and Trust Locations is set to **Keystores**.
    b. Change the Private Key Alias to *SCALED_OUT_HOST*_fusion.
    c. Change the Private Key Passphrase to the *keypassword*, as described in the second bullet in Step 4 in Section 18.2.2.3, "Creating the Identity Keystore on SCALED_OUT_HOST."
    d. Re-enter the *keypassword* from Step c for the Confirm Private Key Passphrase.
    e. Click **Save**.
14. Select the **Server Start** tab.

    Change the Arguments to reflect the name of your cloned Managed Server and make sure the server group is the correct cluster name. For example, you should see the following:

    ```
    -DJDBCProgramName\=DS/domain_nameDomain/soa_server3
    -Dserver.group\=SOACluster
    ```

    Click **Save**.
15. Select the **Logging** tab, and then select the **HTTP** tab.

16. Do the following:
    a. Change the Log file name to `logs/access.log.%yyyyMMdd%`.
    b. Change the rotation type to **By Time**.
    c. Leave the **Limit number of retained files** option unchecked.
    d. Leave the **Rotate log file on startup** option unchecked.
    e. Click **Save**.
    f. Expand **Advanced**.
    g. Change the format to **Extended**.
    h. Change the extended logging format fields to the following:

```
date time time-taken cs-method cs-uri
sc-status sc(X-ORACLE-DMS-ECID)
cs(ECID-Context) cs(Proxy-Remote-User)
cs(Proxy-Client-IP)
```

    i. Click **Save**.
17. Click **Activate Changes**.
18. Run the newly created Managed Server:
    a. Navigate to ***Domain_Name*** **> Environment**.
    b. From the **Navigation** pane on the Oracle WebLogic Server console, select **Activate Changes**.
    c. Navigate to ***Domain_Name*** **> Environment > Servers > Control**.
    d. Check the newly created Managed Server and click **Start**.
    e. Navigate to ***Domain_Name*** **> Environment > Servers** and check the **State** to verify that the newly created Managed Servers are running.

18.2.9.1.5 Validating the System You should verify URLs to ensure that the appropriate routing and failover is working from Oracle HTTP Server to the domain's SOACluster.

To verify the URLs:

1. Log in to the domain's Oracle WebLogic Server Administration Console and stop the `soa_server1` Managed Server on *`PROVISIONED_HOST`* while the Managed Servers on *`SCALED_OUT_HOST`* are running.
2. Do the following:
    a. Edit the `FusionVirtualHost` file, adding the scaled-out `soa_server3` Managed Server's host and port.
    b. Add the code shown in the following example to both the Internal and External part of the `FusionVirtualHost` file on *`WEBHOST1`* and *`WEBHOST2`*.

```
<Location /soa/composer>
   SetHandler weblogic-handler
   WebLogicCluster <DOMAINHOSTSOAVH1:port>,<DOMAINHOSTSOAVH2:port>,
   WLProxySSL ON
   WLProxySSLPassThrough ON
   RewriteEngine On
   RewriteOptions inherit
</Location>
```

c. Restart Oracle HTTP Server on both *WEBHOST1* and *WEBHOST2*.

3. Access `http://domain_nameinternal.mycompany.com/soa-infra` to verify that routing and failover are functioning properly. (Ensure the log in prompt is visible.)
4. Log in to the domain's Oracle WebLogic Server Administration Console and stop the `soa_server3` Managed Server on *SCALED_OUT_HOST*.
5. Start the `soa_server1` Managed Server on *PROVISIONED_HOST*.
6. Repeat Step 3. (Ensure the log in prompt is visible.)
7. Start the `soa_server3` Managed Server on *SCALED_OUT_HOST* and verify that `soa_server1` and `soa_server3` are running.

18.2.9.2 Enabling Virtual IPs on PROVISIONED_HOST and SCALED_OUT_HOST

To enable the virtual IP on Linux:

> **Note:** In this example, `ethX` is the ethernet interface (`eth0` or `eth1`) and `Y` is the index (0, 1, 2, and so on). In addition, the *DOMAINHOSTSOAVH1* and *DOMAINHOSTSOAVH2* VIPs will be used.

1. On *PROVISIONED_HOST*:
   a. Run the `ifconfig` command as root:

      ```
      /sbin/ifconfig interface:index IPAddress netmask netmask
      ```

      For example:

      ```
      /sbin/ifconfig ethX:Y 100.200.140.206 netmask 255.255.255.0
      ```

   b. Enable your network to register the new location of the virtual IP:

      ```
      /sbin/arping -q -U -c 3 -I interface IPAddress
      ```

      For example:

      ```
      /sbin/arping -q -U -c 3 -I ethX 100.200.140.206
      ```

   c. Validate that the address is available by pinging it from another node.

      For example:

      ```
      /bin/ping 100.200.140.206
      ```

2. Repeat Steps a through c on *SCALED_OUT_HOST*.

18.2.9.3 Setting the Listen Address for soa_server*n*

Ensure that you have performed the steps described in Section 18.2.9.2, and the scale-out steps described in Section 18.2.3.2, "Adding a New Machine In the Oracle WebLogic Server Console," Section 18.2.3.3, "Packing and Unpacking the Managed Server Domain Home to SCALED_OUT_HOST," and Section 18.2.3.4, "Cloning Managed Servers and Assigning Them to SCALED_OUT_HOST" before setting the `soa_server`*n* listen address.

To set the listen address for the Managed Server:

1. Log in to the Administration Console.
2. In the Change Center, click **Lock & Edit**.

3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Select **soa_server*n*** in the table. The Setting page for `soa_servern` is displayed.
6. Set the **Listen Address** to *DOMAINHOSTSOAVH1*.
7. Click **Save**.
8. Click **Activate Changes**.
9. The changes will not take effect until the `soa_servern` Managed Server is restarted (ensure that Node Manager is up and running):
   a. On the Summary of Servers page, select the **Control** tab.
   b. Select **soa_server*n*** in the table and then click **Shutdown**.
   c. After the server has shut down, select **soa_server*n*** in the table and then click **Start**.

18.2.9.4 Updating the FusionVirtualHost Configuration File

To enable Oracle HTTP Server to route to `soa_cluster`, which contains the `soa_servern` Managed Servers, you must set the WebLogicCluster parameter to the list of nodes in the cluster.

> **Note:** The `FusionVirtualHost` configuration file uses specific file-naming conventions. For information about these conventions, see Table 18–1 in Section 18.2.3.5, "Configuring Oracle HTTP Server."

To set the parameter:

1. Update the WebLogicCluster parameter in the `FusionVirtualHost` configuration file to contain a cluster list of virtual *host*:*port* entries. (On *WEBHOST1*: *APPLICATIONS_CONFIG*/CommonDomain_webtier/config/OHS/ohs1/moduleconf/FusionVirtualHost_*domain*.conf. On *WEBHOST2*: *APPLICATIONS_CONFIG*/CommonDomain_webtier1/config/OHS/ohs2/moduleconf/FusionVirtualHost_*domain*.conf.) For example:

```
<Location /soa-infra>
 SetHandler weblogic-handler
 WebLogicCluster DOMAINHOSTSOAVH1:7416,DOMAINHOSTSOAVH2:7416
</Location>
```

2. Restart Oracle HTTP Server on both *WEBHOST1* and *WEBHOST2*:

```
WEBHOST1> APPLICATIONS_CONFIG/CommonDomain_webtier/bin/opmnctl restartproc
ias-component=ohs1

WEBHOST2> APPLICATIONS_CONFIG/CommonDomain_webtier1/bin/opmnctl restartproc
ias-component=ohs2
```

The servers specified in the WebLogicCluster parameters are only important at startup time for the plug-in. The list must provide at least one running cluster member for the plug-in to discover other members in the cluster. The listed cluster member must be running when Oracle HTTP Server is started. Oracle WebLogic Server and the plug-in work together to update the server list automatically with new, failed, and recovered cluster members.

Sample scenarios include the following:

- **Example 1:** If you have a two-node cluster and then add a third member, you do not need to update the configuration to add the third member. The third member will be discovered dynamically at runtime.
- **Example 2:** You have a three-node cluster, but only two nodes are listed in the configuration. However, if both listed nodes are down when you start Oracle HTTP Server, then the plug-in would fail to route to the cluster. You must ensure that at least one of the listed nodes is running when you start Oracle HTTP Server.

If you list all the members of the cluster, then you guarantee you can route to the cluster, assuming at least one member is running when Oracle HTTP Server is started. For more information on configuring the Oracle WebLogic Server plug-in, see *Oracle Fusion Middleware Using Web Server 1.1 Plug-Ins with Oracle WebLogic Server*.

18.2.9.5 Switching Oracle User Messaging Service to Use Oracle Advanced Queuing

After *PROVISIONED_HOST* has been provisioned, Oracle User Messaging Service is fully configured with `UMSAQJMSForeignServer` in the `UMSAQJMSSystemResource` JMS Module, and the Oracle Advanced Queuing (AQ-JMS) Foreign Server is deployed over the Oracle SOA Suite Cluster.

No additional JMS configuration is required for the scaled-out server host.

Although you will see `UMSJMSServer_auto_1` configured with the `UMSJMSFileStore_auto_1` file persistence deployed over the `soa_server1` Managed Server, they are not being used by Oracle Fusion Applications.

18.2.9.6 Configuring JMS Servers with JDBC Store Persistence

After *PROVISIONED_HOST* has been provisioned, the Java Message Service (JMS) servers are set up and configured and Java Database Connectivity (JDBC) stores are created and fully configured for *PROVISIONED_HOST*. You now must create and configure the JMS servers and JDBC stores for *SCALED_OUT_HOST_HOST*.

Do the following to create and configure the JMS servers and JDBC stores for *SCALED_OUT_HOST*:

1. Log in to the Oracle WebLogic Server Administration Console.
2. Click **Lock & Edit**.
3. In the Domain Structure window, expand the **Services** node and then click the **Persistence Stores** node.

   The Summary of Persistence Stores page appears.
4. Click **New**, and then **Create JDBC Store**.
5. In the file store fields, enter the following:
   - Name: for example, `SOAJMSJDBCStore_2`
   - Target: `soa_server2`
   - Data Source: `SOALocalTxDataSource`
   - Prefix Name: *DOMAIN*`_FUSION_SOAINFRA.SOAJMS_2_`. (Do not forget to include the ending "_".)
6. Click **OK**.

7. Repeat Steps 3 through 6 for the remaining the three remaining JDBC stores, using the same target and data-source field values:
   - `AGJMSJDBCStore_2`
   - `BPMJMSJDBCStore_2`
   - `PS6SOAJMSJDBCStore_2`
8. Click **Activate Changes**.
9. Click **Lock & Edit**.
10. In the Domain Structure window, expand the **Services** node and then click the **Messaging > JMS Servers** node.

    The Summary of Summary of JMS Servers page appears.
11. Click **New**.
12. Enter a name (for example, `SOAJMSServer_2`), then select **SSOAJMSJDBCStore_2** in the Persistence Store dropdown list.
13. Click **Next**.
14. Select **soa_server2** as the target.
15. Click **Finish**.
16. Repeat Steps 10 through 15 for the remaining JMS servers:
    - `AGJMSServer_2`
    - `BPMJMSServer_2`
    - `PS6SOAJMSServer_2`
17. Click **Activate Changes**.
18. Click **Lock & Edit**.
19. In the Domain Structure window, expand the **Services** node and then click the **Messaging > JMS Modules** node.

    The JMS Modules page appears.
20. Click **SOAJMSModule** and then click the **Subdeployments** tab.
21. Click **SOAJMSServer*xxxxx*** under **Subdeployments**.
22. Add the new `SOAJMSServer_2` server as an additional target for the subdeployment.
23. Click **Save**.
24. Repeat Steps 19 through 23 for the `BPMJMSModule` JMS module.

    Note: Do not make any changes to these JMS modules:
    - `ADSJMSAQModule`
    - `JRFWSAsyncJmsModuleAQ`
    - `AGJMSModule`
    - `PS6SOAJMSModule`
25. Click **Activate Changes**.

18.2.9.7 Configuring Oracle Coherence for Deploying Composites

Although deploying composites uses multicast communication by default, Oracle recommends using unicast communication instead in SOA enterprise deployments. Use unicast if you disable multicast communication for security reasons.

> **Note:** An incorrect configuration of the Oracle Coherence framework that is used for deployment may prevent the SOA system from starting. The deployment framework must be properly customized for the network environment on which the SOA system runs. Oracle recommends the configuration described in this section.

Multicast communication enables Oracle Fusion Middleware SOA to discover all of the members of a cluster to which it deploys composites dynamically. However, unicast communication does not enable nodes to discover other cluster members in this way. Consequently, you must specify the nodes that belong to the cluster. You do not need to specify all of the nodes of a cluster, however. You need only specify enough nodes so that a new node added to the cluster can discover one of the existing nodes. Consequently, when a new node has joined the cluster, it is able to discover all of the other nodes in the cluster. Additionally, in configurations such as SOA enterprise deployments, where multiple IPs are available in the same box, you must configure Oracle Coherence to use a specific host name to create the Oracle Coherence cluster.

> **Tip:** To guarantee high availability during deployments of SOA composites, specify enough nodes so that at least one of them is running at any given time.

Specify the nodes using the `tangosol.coherence.wka` *n* system property, where *n* is the number for each Oracle HTTP Server. The numbering starts at 1. This numbering must be sequential and must not contain gaps. In addition, specify the host name used by Oracle Coherence to create a cluster through the `tangosol.coherence.localhost` system property. This local host name should be the virtual host name used by the SOA server as the listener addresses (*DOMAINHOSTSOAVH1* and *DOMAINHOSTSOAVH2*). Set this property by adding the `-Dtangosol.coherence.localhost` parameters to the Arguments field of the Oracle WebLogic Server Administration Console's Server Start tab.

> **Note:** *DOMAINHOSTSOAVH1* is the virtual host name that maps to the virtual IP where `soa_server1` is listening (in *PROVISIONED_HOST*). *DOMAINHOSTSOAVH2* is the virtual host name that maps to the virtual IP where `soa_server2` is listening (in *SCALED_OUT_HOST*).

To add the host name used by Oracle Coherence:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the Domain Structure window, expand the **Environment** node.
3. Click **Servers**.

   The Summary of Servers page appears.
4. Select **soa_server1** (represented as a hyperlink) from the column of the table.

   The Settings page appears.

5. Click **Lock & Edit**.
6. Click the **Server Start** tab.
7. Append the following for `soa_server1` and `soa_server2` to the **Arguments** field.

   For `soa_server1`:

   ```
   -Dtangosol.coherence.wka1=DOMAINHOSTSOAVH1
   -Dtangosol.coherence.wka2=DOMAINHOSTSOAVH2
   -Dtangosol.coherence.localhost=DOMAINHOSTSOAVH1
   -Dtangosol.coherence.localport=8089
   -Dtangosol.coherence.wka1.port=8089
   -Dtangosol.coherence.wka2.port=8089
   ```

   For `soa_server2`:

   ```
   -Dtangosol.coherence.wka1=DOMAINHOSTSOAVH2
   -Dtangosol.coherence.wka2=DOMAINHOSTSOAVH1
   -Dtangosol.coherence.localhost=DOMAINHOSTSOAVH2
   -Dtangosol.coherence.localport=8089
   -Dtangosol.coherence.wka1.port=8089
   -Dtangosol.coherence.wka2.port=8089
   ```

   Note: There should be no breaks in lines between the different `-D` parameters. Do not copy or paste the code from above to your Administration Console's Arguments text field. This may result in HTML tags being inserted in the Java arguments. The code should not contain other characters than those included in the example above.

8. Click **Save** and **Activate Changes**.

   Notes:

   - You must ensure that these variables are passed to the Managed Server correctly. (They should be reflected in the server's output log.) Failure of the Oracle Coherence framework can prevent the soa-infra application from starting.
   - By default, the Oracle Coherence cluster uses port 8088 for deployment. This port can be changed by specifying the `-Dtangosol.coherence.wkaX.port` startup parameter. To avoid a port number conflict when configuring coherence parameters in different domains, ensure that you increment port 8089 by 1, or choose the next free port in this sequence.
   - The multicast and unicast addresses are different from the ones used by the Oracle WebLogic Server cluster for cluster communication. Oracle SOA Suite guarantees that composites are deployed to members of a single Oracle WebLogic Server cluster even though the communication protocol for the two entities (the Oracle WebLogic Server cluster and the groups to which composites are deployed) are different.

18.2.9.8 Configuring a JDBC Transaction Log Store for Transaction Recovery

Each server has a transaction log that stores information about committed transactions that are coordinated by the server that may not have been completed. Oracle

WebLogic Server uses this transaction log for recovery from system crashes or network failures. To leverage the migration capability of the Transaction Recovery Service for the servers within a cluster, store the transaction log in a location accessible to a server and its backup servers.

To set the location for the transaction log store:

1. Log in to the Oracle WebLogic Server Administration Console (`http://domain_nameinternal.mycompany.com/console`).
2. In the Change Center, click **Lock & Edit**.
3. In the Domain Structure window, expand the **Environment** node and then click the **Servers** node.

   The Summary of Servers page appears.
4. Click the server name **soa_server2** (represented as a hyperlink) in the table. The Settings page for the selected server appears, and defaults to the **Configuration** tab.
5. In the **Configuration** tab, click the **Services** tab.
6. In the **Transaction Log Store** section of the page, do the following:
   a. For the type, change the dropdown list selection from **Default Store** to **JDBC**.
   b. For the data store, select **SOALocalTxDataSource** from dropdown list.
   c. For prefix name, enter *DOMAIN*`_FUSION_SOAINFRA.TLOG_soa_server2_`. (Do not forget to include the ending "_".)

Note: The prefix name is specific for each domain.

- Oracle Fusion Customer Relationship Management domain: `CRM_FUSION_SOAINFRA.TLOG_soa_server2_`
- Oracle Fusion Financials domain: `FIN_FUSION_SOAINFRA.TLOG_soa_server2_`
- Oracle Fusion Common domain: `SETUP_FUSION_SOAINFRA.TLOG_soa_server2_`
- Oracle Fusion Incentive Compensation domain: `OIC_FUSION_SOAINFRA.TLOG_soa_server2_`
- Oracle Fusion Human Capital Management domain: `HCM_FUSION_SOAINFRA.TLOG_soa_server2_`
- Oracle Fusion Supply Chain Management domain: `SCM_FUSION_SOAINFRA.TLOG_soa_server2_`
- Oracle Fusion Project Portfolio Management domain: `PRJ_FUSION_SOAINFRA.TLOG_soa_server2_`
- Oracle Fusion Procurement domain: `PRC_FUSION_SOAINFRA.TLOG_soa_server2_`

Note: When the JDBC transaction log store configuration is complete, and after bouncing the `soa_server2` server, do the following:

- Append the table name in the prefix name with `WLStore`. For example, `TLOG_soa_server2_WLStore`.
- Verify that the new table, `TLOG_soa_server2_WLStore`, has been created in *`DOMAIN`*`_FUSION_SOAINFRA`.

7. Click **Save** and then click **Activate Changes**.
8. Restart the Managed Server to activate the changes (ensure that Node Manager is up and running):
   a. Log in to the Oracle WebLogic Server Administration Console (`http://`*`domain_name`*`internal.mycompany.com/console`).
   b. In the Summary of Servers screen, select the **Control** tab.
   c. Select **soa_server2** in the table and then click **Shutdown**.
   d. Start the `soa_server2` server.

18.2.9.9 Disabling Host Name Verification for the soa_server*n* Managed Servers

This step is required if you have not set up the appropriate certificates to authenticate the different nodes with the Administration Server. By default, Host Name Verification should be set to *None*. If it is not, follow the steps below.

If you have not configured the server certificates, you will receive errors when managing the different Oracle WebLogic Servers. To avoid these errors, disable host name verification while setting up and validating the topology, and enable it again after the enterprise deployment topology configuration is complete.

To disable Host Name Verification:

1. Log in to Oracle WebLogic Server Administration Console. For example, `http://`*`domain_name`*`internal.mycompany.com/console`.
2. Click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**.

   The Summary of Servers page appears.
5. Select **soa_server*n*** (represented as a hyperlink) in the table.

   The Settings page appears.
6. Select the **SSL** tab.
7. Expand the **Advanced** section of the page.
8. Set **Hostname Verification** to **None**.
9. Click **Save**.
10. Repeat Steps 1 through 9 for the other instance of the `soa_server`*`n`* Managed Server.
11. Save and activate the changes.

18.2.9.10 Restarting Node Manager on PROVISIONED_HOST

To restart Node Manager on *PROVISIONED_HOST*:

1. Stop Node Manager by stopping the process associated with it:
   a. If it is running in the foreground in a shell, simply use CTRL+C.
   b. If it is running in the background in the shell, find the associated process and use the `kill` command to stop it. For example:

```
PROVISIONED_HOST> ps -ef | grep NodeManager
orcl 9139 9120 0 Mar03 pts/6 00:00:00/bin/sh ./startNodeManager.sh
```

   c. Run the following command:

```
PROVISIONED_HOST> kill -9 9139
```

2. Start Node Manager:

```
PROVISIONED_HOST> APPLICATIONS_CONFIG/nodemanager/PROVISIONED_
HOST/startNodeManagerWrapper.sh
```

18.2.9.11 Starting and Validating soa_server1 on PROVISIONED_HOST

To start the `soa_server1` Managed Server on *PROVISIONED_HOST*:

1. Access the Administration Console. For example, `http://`*domain_name*`internal.mycompany.com/console`.
2. Click **Servers**.
3. Open the **Control** tab.
4. Select **soa_server1**.
5. Click **Start**.

To validate the `soa_server1` Managed Server on *PROVISIONED_HOST*:

1. Verify that the server status is reported as "Running" in the Administration Console. If the server is shown as "Starting" or "Resuming," wait for the server status to change to "Started." If another status is reported (such as "Admin" or "Failed"), check the server output log files for errors.
2. Access `http://`*DOMAINHOSTSOAVH1*`:7416/soa-infra` and `http://`*domain_name*`internal.mycompany.com/soa-infra` to verify status of `soa_server1`.

> **Note:** Although the `soa_server1` server may be up, some applications may be in a failed state. Therefore, Oracle recommends verifying the above URLs and watching for errors pertaining each individual application in the server's output file.

18.2.9.12 Restarting Node Manager on SCALED_OUT_HOST

To restart Node Manager on *SCALED_OUT_HOST*, follow the steps in Section 18.2.9.10, "Restarting Node Manager on PROVISIONED_HOST."

18.2.9.13 Starting and Validating soa_server*n* on SCALED_OUT_HOST

To start the `soa_server`*n* Managed Server on *SCALED_OUT_HOST* and ensure that it is configured correctly:

1. From the Administration Console, start the `soa_server`*n* Managed Server.

2. Verify that the server status is reported as "Running" in the Administration Console. If the server is shown as "Starting" or "Resuming," wait for the server status to change to "Started." If another status is reported (such as "Admin" or "Failed"), check the server output log files for errors.
3. Access `http://DOMAINHOSTSOAVH2:7416/soa-infra` and `http://domain_nameinternal.mycompany.com/soa-infra`.

> **Note:** Although `soa_server2` server may be up, some applications may be in a failed state. Therefore, Oracle recommends verifying the above URLs and watching for errors pertaining each individual application in the server's output file.

18.2.10 Configuring Administration Server High Availability

This section describes how to configure and validate the Oracle WebLogic Server Administration Server for high availability.

18.2.10.1 Enabling Administration Server High Availability

The Administration Server is a singleton application, so it cannot be deployed in an active-active configuration. By default, the Administration Server is only available on the first installed node. If this node becomes unavailable, then the Administration Console and Fusion Middleware Control also become unavailable. To avoid this scenario, the Administration Server and the applications deployed to it must be enabled for failover. The enterprise deployment architecture in this guide calls for the deploying the Administration Server on a disk shared between the primary node and the secondary node.

The following domains are deployed as part of the Oracle Fusion Applications enterprise deployment implementation:

> **Note:** The list of domains may differ depending on the product offerings that are provisioned in your environment.

- Oracle Fusion Customer Relationship Management Domain
- Oracle Fusion Common Domain
- Oracle Fusion Financials Domain
- Oracle Fusion Human Capital Management Domain
- Oracle Fusion Supply Chain Management Domain
- Oracle Fusion Incentive Compensation Domain
- Oracle Fusion Project Portfolio Management Domain
- Oracle Fusion Procurement Domain
- Oracle Business Intelligence Domain

The process described in this guide initially deploys each domain-specific Administration Server in shared storage (*APPLICATIONS_BASE*) mounted on *PROVISIONED_HOST*, and Managed Servers in the local disk (*APPLICATIONS_CONFIG*).

This section tells you how to do the following:

- Enable an administrative virtual host on *PROVISIONED_HOST*

- Add a new machine in the Oracle WebLogic Server Console
- Enable the Administration Server to listen on the virtual IP address

18.2.10.1.1 Enabling an Administrative Virtual Host on PROVISIONED_HOST

> **Note:** *DOMAINADMINVH* is used as a generic name in this section.
>
> where
>
> *DOMAIN* is replaced with the domain-specific syntax. For example, *CRMADMINVH*, *FINADMINVH*, *HCMADMINCH*, and so on.

The Administration Server must be configured to listen on a virtual IP Address to enable it to seamlessly failover from one host to another. In a failure, the Administration Server, along with the virtual IP Address, can be migrated from one host to another.

However, before the Administration Server can be configured to listen on a virtual IP Address, one of the network interface cards on the host running the Administration Server must be configured to listen on this virtual IP Address. The steps to enable a virtual IP Address are completely dependent on the operating system.

To enable a virtual IP Address on *PROVISIONED_HOST*:

> **Note:** In a UNIX environment, the command must be run as the root user.

1. On *PROVISIONED_HOST*, run the `ifconfig` command to get the value of the netmask. In a UNIX environment, run this command as the root user. For example:

```
[root@PROVISIONED_HOST ~] # /sbin/ifconfig
eth0     Link encap:Ethernet  HWaddr 00:11:43:D7:5B:06
     inet addr:139.185.140.51  Bcast:139.185.140.255  Mask:255.255.255.0
     inet6 addr: fe80::211:43ff:fed7:5b06/64 Scope:Link
     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
     RX packets:10626133 errors:0 dropped:0 overruns:0 frame:0
     TX packets:10951629 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:1000
     RX bytes:4036851474 (3.7 GiB)  TX bytes:2770209798 (2.5 GiB)
     Base address:0xecc0 Memory:dfae0000-dfb00000
```

2. On *PROVISIONED_HOST*, bind the virtual IP Address to the network interface card using `ifconfig`. In a UNIX environment, run this command as the root user. Use a netmask value that was obtained in Step 1.

   The syntax and usage for the `ifconfig` command is as follows:

```
/sbin/ifconfig networkCardInterface Virtual_IP_Address netmask netMask
```

   For example:

```
/sbin/ifconfig eth0:1 100.200.140.206 netmask 255.255.255.0
```

3. Update the routing table using `arping`. In a UNIX environment, run this command as the root user.

```
/sbin/arping -q -U -c 3 -I networkCardInterface Virtual_IP_Address
```

For example:

```
/sbin/arping -q -U -c 3 -I eth0 100.200.140.206
```

4. Validate that the address is available by pinging it from another node. For example:

```
/bin/ping 100.200.140.206
```

18.2.10.1.2 Adding a New Machine in the Oracle WebLogic Server Console Create a new machine and assign the Administration Server to the new machine using the Administration Console:

1. Log in to the Administration Console.
2. In the Change Center, click **Lock & Edit**.
3. In the Environment section of the Home page, click **Machines**.
4. On the Summary of Machines page, select the machine that is associated with the Administration Server from under the **Machines** table and click **Clone**. For example: `PROVISIONED_HOST.MYCOMPANY.COM`.
5. On the Clone a Machine page, enter the name of the machine under the Machine Identity section and click **OK**. For example, enter `ADMINHOST` as the machine name.
6. On the Summary of Machines page, click the newly created machine link.
7. On the Settings page for the `ADMINHOST` machine, click **Servers**.
8. Click **Add** under the **Servers** table.
9. On the Add a Server to Machine page, select **Select an existing server, and associate it with this machine**.
10. Choose the AdminServer from the dropdown list.
11. Click **Finish** to associate the Administration Server with the machine.
12. On the Settings page for the `ADMINHOST` machine, click **Node Manager**.
13. Set the listen address to *`DOMAINADMINVH`*.

> **Note:** Ensure that you have performed the steps described in Section 18.2.10.1.1, "Enabling an Administrative Virtual Host on PROVISIONED_HOST" before setting the Node Manager listen address.

14. Click **Save**.
15. In the Change Center, click **Activate Changes**.

18.2.10.1.3 Enabling an Administration Server to Listen on the Virtual IP Address Ensure that you have performed the steps described in Section 18.2.10.1.1, "Enabling an Administrative Virtual Host on PROVISIONED_HOST" before setting the Administration Server listen address.

To set the Administration Server listen address:

1. Log in to the Administration Console.
2. In the Change Center, click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.

4. Click **Servers**. The Summary of Servers page is displayed.
5. Select **AdminServer(admin)** in the table. The Settings page for AdminServer(admin) is displayed.
6. Set the listen address to *DOMAINADMINVH* (domain-specific administrative virtual host).
7. Click **Save**.
8. Click **Activate Changes**.
9. The changes will not take effect until the Administration Server is restarted. Follow these steps to restart the Administration Server:
   a. In the Summary of Servers page, select the **Control** tab.
   b. Select **AdminServer(admin)** in the table and then click **Shutdown**.
10. Set the following environment variable:

```
WLST_PROPERTIES="-Dweblogic.security.SSL.trustedCAKeyStore=
APPLICATIONS_CONFIG/keystores/fusion_trust.jks"
```

11. Start the Administration Server again from the command line using the `nmconnect` user name and password.

```
PROVISIONED_HOST> APPLICATIONS_BASE/fusionapps/wlserver_10.3/common/bin/wlst.sh

PROVISIONED_HOST> nmConnect(username='username', password='password',
domainName='domain_name', host='DOMAINADMINVH',port='5556', nmType='ssl',
domainDir='APPLICATIONS_CONFIG/domains/PROVISIONED_HOST/domain_name')

PROVISIONED_HOST> nmStart('AdminServer')
PROVISIONED_HOST> exit ()
```

18.2.10.2 Configuring Oracle HTTP Server

To configure Oracle HTTP Server:

1. On *WEBHOST1*:
   a. `cd APPLICATIONS_CONFIG/CommonDomain_webtier/config/OHS/ohs1/moduleconf.`
   b. Edit the domain-specific virtual host `config` file. For example:

```
cp FusionVirtualHost_domain.conf FusionVirtualHost_domain.conf.org
```

> **Note:** The `FusionVirtualHost` configuration file uses specific file-naming conventions. For information about these conventions, see Table 18–1 in Section 18.2.3.5, "Configuring Oracle HTTP Server."

2. Edit the `FusionVirtualHost` configuration file, adding the Administrative virtual host and port. Example 18–2 shows sample code.

> **Note:** Replace *DOMAINADMINVH* and port with domain-specific Administrative virtual host and port number.

Example 18–2 Add AdministrativeVirtual Host and Port

```
## Context roots for application em
```

```
    <Location /em>
        SetHandler weblogic-handler
        WebLogicCluster DOMAINADMINVH:port
    </Location>

## Context roots for application console
    <Location /console >
        SetHandler weblogic-handler
        WebLogicCluster DOMAINADMINVH:port
    </Location>
```

3. Restart Oracle HTTP Server: `cd` to *APPLICATIONS_CONFIG*`/CommonDomain_webtier/bin` and enter the following:

```
WEBHOST1> ./opmnctl stopall
WEBHOST1> ./opmnctl startall
```

4. Repeat Steps 1 through 3 on *WEBHOST2*.

18.2.10.3 Validating the Administration Server

Perform these steps to ensure that the Administration Server and Oracle Enterprise Manager Fusion Middleware Control are properly configured:

1. Ensure that you can access the domain-specific Oracle WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control. For example:

   `http://`*domain_name*`internal.mycompany.com/console`

   `http://`*domain_name*`internal.mycompany.com/em`

2. After completing the steps in Section 18.2.10.1 and Section 18.2.10.2 for other domains, repeat Step 1 for other domains by replacing the domain-specific URL.

3. Do the following:

   a. Log into Oracle Fusion Functional Setup Manager as a super user. The user should have the Oracle WebLogic Server Administrator role, for example, "FAadmin". Functional Setup Manager is located here:

      `https://commonexternal.mycompany.com/setup/faces/TaskListManagerTop`

   b. Select **Register Domains** in the left-hand task pane.

   c. On the Register Domains page, select the domain to be updated and click **Edit**.

   d. Do the following:

      – Replace `ADMIN_HOST` (the default value) with *DOMAINADMINVH* wherever it appears.

      – Update the value of **Node Manager Protocol** to `ssl`.

      – Ensure the value of **Node Manager Port** is `5556`.

   e. Click **Save and Close**.

   f. Repeat Step a through Step e for all domains except IDMDomain.

4. Replace the value of `TAXONOMY_URL` in the `fusion_env.properties`, `fusion_prov.properties`, and `atgpf_env.properties` files located in *APPLICATIONS_CONFIG*`/fapatch` with *DOMAINADMINVH* if the Administration Server's listen address is updated with the virtual IP (VIP) for CommonDomain.

5. The changes will not take effect until the Administration Server is restarted. Follow these steps to restart the Administration Server:
   a. In the Summary of Servers page, select the **Control** tab.
   b. Select **AdminServer(admin)** in the table and then click **Shutdown**.
6. Set the following environment variable:

```
WLST_PROPERTIES="-Dweblogic.security.SSL.trustedCAKeyStore=
APPLICATIONS_CONFIG/keystores/fusion_trust.jks"
```

7. Start the Administration Server again from the command line using the `nmconnect` user name and password.

```
PROVISIONED_HOST> APPLICATIONS_BASE/fusionapps/wlserver_10.3/common/bin/wlst.sh

PROVISIONED_HOST> nmConnect(username='username', password='password',
domainName='domain_name', host='DOMAINADMINVH',port='5556', nmType='ssl',
domainDir='APPLICATIONS_CONFIG/domains/PROVISIONED_HOST/domain_name')

PROVISIONED_HOST> nmStart('AdminServer')
PROVISIONED_HOST> exit ()
```

8. Restart the Managed Servers:
   a. Log in to the Oracle WebLogic Server Administration Console (`http://domain_nameinternal.mycompany.com/console`).
   b. Navigate to ***Domain_Name*** **> Environment > Servers > Control**.
   c. Select all the Managed Servers and click **Stop**.
   d. After all the servers have shut down, select all the servers in the table and then click **Start**.

18.2.10.4 Manually Failing Over the Administration Server to SCALED_OUT_HOST

In case a node fails, you can fail over the Administration Server to another node. This section describes how to fail over the Administration Server from *PROVISIONED_HOST* to *SCALED_OUT_HOST*.

18.2.10.4.1 Prerequisites for the Manual Failover Ensure the following:

- The Administration Server is configured to listen on a domain-specific administrative virtual host, and not on **any** address
- When failover happens, the Administration Server is failed over from *PROVISIONED_HOST* to *SCALED_OUT_HOST* and the two nodes have the following IPs:
  - *PROVISIONED_HOST*: 100.200.140.165
  - *SCALED_OUT_HOST*: 100.200.140.205
  - *DOMAINADMINVH*: 100.200.140.206. This is the VIP where the domain-specific Administration Server is running, assigned to `ethX:Y`, available in *PROVISIONED_HOST* and *SCALED_OUT_HOST*.
  - The domain directory where the Administration Server is running on *PROVISIONED_HOST* is on shared storage and is mounted from *SCALED_OUT_HOST*

18.2.10.4.2 Performing the Failover The following procedure explains how to fail over the Administration Server to a different node (*SCALED_OUT_HOST*) with the

Administration Server still using the same Oracle WebLogic Server machine. (This machine is a logical machine, not a physical one.)

To fail over the Administration Server:

1. Stop the Administration Server.
2. Migrate the IP to the second node:
   a. Run the following command as root on *PROVISIONED_HOST* to (where `X:Y` is the current interface used by *DOMAINADMINVH*):

      PROVISIONED_HOST`> /sbin/ifconfig ethX:Y down`

   b. Run the following command as root on *SCALED_OUT_HOST*:

      SCALED_OUT_HOST`> /sbin/ifconfig` *interface:index IP_Address* `netmask` *netmask*

      For example:

      ```
      /sbin/ifconfig eth0:1 100.200.140.206 netmask 255.255.255.0
      ```

      Note: Ensure that the netmask and interface to be used to match the available network configuration in *SCALED_OUT_HOST*.

3. Update the routing tables with arping. For example, run the following command as root:

   SCALED_OUT_HOST`> /sbin/arping -q -U -c 3 -I eth0 100.200.140.206`

4. Validate that the address is available by pinging it from another node. For example:

   ```
   /bin/ping 100.200.140.206
   ```

5. Start the Administration Server on *SCALED_OUT_HOST* using the procedure in Section 18.2.10.1.3.
6. Test access to the Administration Server on *SCALED_OUT_HOST*:
   a. Ensure that you can access the domain-specific Oracle WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control. For example, for the Oracle Fusion Customer Relationship Management domain, use these URLs:
      - `http://crminternal.mycompany.com/console`
      - `http://crminternal.mycompany.com/em`
   b. Repeat Step a for other domain by replacing the domain-specific URL.

      Note: The Administration Server does not use Node Manager for failing over. After a manual failover, the machine name that appears in the Current Machine field in the Administration Console for the server is *PROVISIONED_HOST*, and not the failover machine, *SCALED_OUT_HOST*. Since Node Manager does not monitor the Administration Server, the machine name that appears in the Current Machine field, is not relevant and you can ignore it.

18.2.10.5 Failing the Administration Server Back to PROVISIONED_HOST

You also must ensure that you can fail back the Oracle WebLogic Server Administration Server, that is, stop it on *SCALED_OUT_HOST* and run it on *PROVISIONED_HOST*. To do this, migrate *DOMAINADMINVH* back to *PROVISIONED_HOST* node.

To migrate *DOMAINADMINVH*:

1. Stop the Administration Server on *SCALED_OUT_HOST*.
2. Run the following command as root from *SCALED_OUT_HOST* to shut down the network stack virtual interface:

   ```
   SCALED_OUT_HOST> /sbin/ifconfig ethX:Y down
   ```

3. Run the following command as root from *PROVISIONED_HOST* to restart the virtual interface:

   ```
   PROVISIONED_HOST> /sbin/ifconfig ethX:Y 100.200.140.206 netmask 255.255.255.0
   ```

   Note: Ensure that the netmask and interface to be used match the available network configuration in *PROVISIONED_HOST*.

4. Run the following command from *PROVISIONED_HOST* to update the routing tables through arping:

   ```
   PROVISIONED_HOST> /sbin/arping -q -U -c 3 -I eth0 100.200.140.206
   ```

5. Validate that the address is available by pinging it from another node. For example:

   ```
   /bin/ping 100.200.140.206
   ```

6. Start the Administration Server again on *PROVISIONED_HOST* using the procedure in Section 18.2.10.1.3.
7. Test access to the Administration Server on *PROVISIONED_HOST*:
   a. Ensure that you can access the domain-specific Oracle WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control. For example, for the Oracle Fusion Customer Relationship Management domain, use these URLs:
      - `http://crminternal.mycompany.com/console`
      - `http://crminternal.mycompany.com/em`
   b. Repeat Step a for other domain by replacing the domain-specific URL.

18.3 Setting Up Server Migration for Oracle Fusion Applications

This section describes how to configure server migration according to Oracle Fusion Applications recommendations.

18.3.1 Prerequisites for Setting Up Server Migration

Before migrating Oracle Fusion Applications domains, ensure you have done the following for all Managed Servers needing to be migrated:

- Enabled the Virtual IPs on *PROVISIONED_HOST* and *SCALED_OUT_HOST*. (For more information, see Section 18.2.9.2, "Enabling Virtual IPs on PROVISIONED_HOST and SCALED_OUT_HOST".)

- Set the listen address for the `soa_servern` Managed Servers. (For more information, see Section 18.2.9.3, "Setting the Listen Address for soa_servern".)

18.3.2 Migrating Oracle Fusion Applications

The procedures in this section apply to these domains and applications:

> **Note:** The list of domains may differ depending on the product offerings that are provisioned in your environment.

- Oracle SOA Suite in the Oracle Fusion Customer Relationship Management domain
- Oracle SOA Suite in the Oracle Fusion Financials domain
- Oracle SOA Suite and Oracle WebCenter Content: Imaging in the Oracle Fusion Common domain
- Oracle Fusion Common domain
- Oracle SOA Suite in the Oracle Business Intelligence domain
- Oracle SOA Suite in the Oracle Fusion Human Capital Management domain
- Oracle SOA Suite in the Oracle Fusion Supply Chain Management domain
- Oracle SOA Suite in the Oracle Fusion Project Portfolio Management domain
- Oracle SOA Suite in the Oracle Fusion Procurement domain
- Oracle SOA Suite in the Oracle Incentive Compensation domain

18.3.3 About Configuring Server Migration

The procedures described in this chapter must be performed for various components of the topology (for example, web tier, application tier, database tier). Variables are used in this chapter to distinguish between component-specific items:

- *WLS_SERVER1* and *WLS_SERVER2* refer to the managed Oracle WebLogic Servers for the enterprise deployment component
- *PROVISIONED_HOST* and *SCALED_OUT_HOST* refer to the host machines for the enterprise deployment component
- *CLUSTER* refers to the cluster associated with the enterprise deployment component

The values to be used to these variables are provided in the component-specific chapters in this guide.

In this enterprise topology, you must configure server migration for the *WLS_SERVER1* and *WLS_SERVER2* Managed Servers. The *WLS_SERVER1* Managed Server is configured to restart on *SCALED_OUT_HOST* should a failure occur. The *WLS_SERVER2* Managed Server is configured to restart on *PROVISIONED_HOST* should a failure occur. For this configuration, the *WLS_SERVER1* and *WLS_SERVER2* servers listen on specific floating IP addresses that are failed over by Oracle WebLogic Server migration. Configuring server migration for the Oracle WebLogic Servers consists of the following steps:

- Step 1: Set up a user and tablespace for the server migration leasing table
- Step 2: Create a multi-data source using the Oracle WebLogic Server Administration Console

- Step 3: Edit Node Manager's properties file
- Step 4: Set environment and superuser privileges for the `wlsifconfig` script
- Step 5: Configure server migration targets
- Step 6: Test the server migration

18.3.4 Setting Up a User and Tablespace for the Server Migration Leasing Table

The first step is to set up a user and tablespace for the server migration leasing table.

> **Note:** If other servers in the same domain have already been configured with server migration, the same tablespace and data sources can be used. In that case, the data sources and multi-data source for database leasing do not need to be re-created, but they will have to be retargeted to the cluster being configured with server migration.

To set up a user and tablespace:

1. Create a tablespace called 'leasing'. For example, log on to SQL*Plus as the sysdba user and run the following command:

   ```
   SQL> create tablespace leasing logging datafile
   'DB_HOME/oradata/orcl/leasing.dbf'
   size 32m autoextend on next 32m maxsize 2048m extent management local;
   ```

2. Create a user named 'leasing' and assign to it the leasing tablespace:

   ```
   SQL> create user leasing identified by password;
   SQL> grant create table to leasing;
   SQL> grant create session to leasing;
   SQL> alter user leasing default tablespace leasing;
   SQL> alter user leasing quota unlimited on LEASING;
   ```

3. Create the leasing table using the `leasing.ddl` script:

   a. Copy the `leasing.ddl` file located in either the *APPLICATIONS_BASE*`/fusionapps/wlserver_10.3/server/db/oracle/817` or the *APPLICATIONS_BASE*`/fusionapps/wlserver_10.3/server/db/oracle/920` directory to your database node.

   b. Connect to the database as the leasing user.

   c. Run the `leasing.ddl` script in SQL*Plus:

      ```
      SQL> @Copy_Location/leasing.ddl;
      ```

18.3.5 Creating a Multi-Data Source Using the Oracle WebLogic Server Administration Console

The second step is to create a multi-data source for the leasing table from the Oracle WebLogic Server Administration Console. You create a data source to each of the Oracle RAC database instances during the process of setting up the multi-data source, both for these data sources and the global leasing multi-data source.

Please note the following considerations when creating a data source:

- Make sure that this is a non-XA data source

- The names of the multi-data sources are in the format of <*MultiDS*>-*rac0*, <*MultiDS*>-*rac1*, and so on
- Use Oracle's Driver (Thin) Version 9.0.1, 9.2.0, 10, 11
- Use Supports Global Transactions, One-Phase Commit, and specify a service name for your database
- Target these data sources to the cluster assigned to the enterprise deployment component

Creating a Multi-Data Source

To create a multi-data source:

1. In the Domain Structure window in the Oracle WebLogic Server Administration Console, click the **Data Sources** link.
2. Click **Lock & Edit**.
3. Select **Multi Data Source** from the **New** dropdown list.

   The Create a New JDBC Multi Data Source page is displayed.
4. Enter `leasing` as the name.
5. Enter `jdbc/leasing` as the JNDI name.
6. Select **Failover** as algorithm (default).
7. Click **Next.**
8. Select the cluster that must be migrated. In this case, SOA cluster.
9. Click **Next**.
10. Select **non-XA driver** (the default).
11. Click **Next**.
12. Click **Create a New Data Source**.
13. Enter `leasing-rac0` as the name. Enter `jdbc/leasing-rac0` as the JNDI name. Enter `oracle` as the database type. For the driver type, select Oracle Driver (Thin) for Oracle RAC Service-Instance connections, Versions 10 and later.

    Note: When creating the multi-data sources for the leasing table, enter names in the format of <*MultiDS*>-rac0, <*MultiDS*>-rac1, and so on.
14. Click **Next**.
15. Deselect **Supports Global Transactions**.
16. Click **Next**.
17. Enter the following for your leasing schema:
    - **Service Name:** The service name of the database.
    - **Database Name:** The Instance Name for the first instance of the Oracle RAC database.
    - **Host Name:** The name of the node that is running the database. For the Oracle RAC database, specify the first instance's VIP name or the node name as the host name.

- **Port:** The port number for the database (1521).
- **Database User Name:** Enter `leasing`.
- **Password:** The leasing password.

18. Click **Next**.
19. Click **Test Configuration** and verify that the connection works.
20. Click **Next**.
21. Target the data source to the cluster assigned to the enterprise deployment component (*CLUSTER*).
22. Click **Finish**.
23. Click **Create a New Data Source** for the second instance of your Oracle RAC database, target it to the cluster assigned to the enterprise deployment component (*CLUSTER*), repeating the steps for the second instance of your Oracle RAC database.
24. Add `leasing-rac0` and `leasing-rac1` to your multi-data source.
25. Make sure the initial connection pool capacity of the data sources is set to 0 (zero). In the Datasources screen do the following:
    a. Select **Services**, then select **Datasources**.
    b. Click **Datasource Name**, then click the **Connection Pool** tab.
    c. Enter `0` (zero) in the **Initial Capacity** field.
26. Click **Save**, then click **Activate Changes**.

18.3.6 Editing Node Manager's Properties File

The third step is to edit Node Manager's properties file, which is located at:

APPLICATIONS_CONFIG/nodemanager/*PROVISIONED_HOST*

APPLICATIONS_CONFIG/nodemanager/*SCALED_OUT_HOST*

This must be done for the node managers in both nodes where server migration is being configured. For example:

```
Interface=eth0
NetMask=255.255.255.0
UseMACBroadcast=true
```

- **Interface:** This property specifies the interface name for the floating IP (for example, `eth0`).

  Do not specify the sub-interface, such as `eth0:1` or `eth0:2`. This interface is to be used without `:0` or `:1`. Node Manager's scripts traverse the different :*X*-enabled IPs to determine which to add or remove. For example, the valid values in Linux environments are `eth0`, `eth1`, `eth2`, `eth3`, `ethn`, depending on the number of interfaces configured.

- **NetMask:** This property specifies the net mask for the interface for the floating IP. The net mask should the same as the net mask on the interface; 255.255.255.0 is used as an example in this document.

- **UseMACBroadcast:** This property specifies whether to use a node's MAC address when sending ARP packets, that is, whether to use the -b flag in the arping command.

Verify in Node Manager's output (shell where Node Manager is started) that these properties are being used, or problems may arise during migration. You should see something like this in Node Manager's output:

```
...
StateCheckInterval=500
Interface=eth0
NetMask=255.255.255.0
...
```

> **Note:** The steps below are not required if the server properties (start properties) have been properly set and Node Manager can start the servers remotely.

1. Set the following property in the nodemanager.properties file:
   - **StartScriptEnabled:** Set this property to 'true'. This is required for Node Manager to start the Managed Servers using start scripts.
2. Restart Node Manager on *PROVISIONED_HOST* and *SCALED_OUT_HOST* by running the startNodeManagerWrapper.sh script, which is located in the *APPLICATIONS_CONFIG*/nodemanager/*PROVISIONED_HOST* and *APPLICATIONS_CONFIG*/nodemanager/*SCALED_OUT_HOST_HOST* directories.

18.3.7 Setting Environment and Superuser Privileges for the wlsifconfig.sh Script

The fourth step is to set environment and superuser privileges for the wlsifconfig.sh script:

1. Ensure that your PATH is set with the environment variables in the terminal from where Node Manager is started, and that it includes these files:

Table 18–5 Files Required for the PATH Environment Variable

File	Located in these directories
wlsifconfig.sh	*APPLICATIONS_CONFIG*/domains/*PROVISIONED_HOST/ManagedServerName*_Domain/bin/server_migration *APPLICATIONS_CONFIG*/domains/*SCALED_OUT_HOSTHOST/ManagedServerName*_Domain/bin/server_migration
wlscontrol.sh	*APPLICATIONS_BASE*/fusionapps/wlserver_10.3/common/bin
nodemanager.domains	*APPLICATIONS_CONFIG*/nodemanager/*PROVISIONED_HOST* *APPLICATIONS_CONFIG*/nodemanager/*SCALED_OUT_HOST*

2. Grant sudo configuration for the wlsifconfig.sh script.
   - Configure sudo to work without a password prompt.
   - For security reasons, sudo should be restricted to the subset of commands required to run the wlsifconfig.sh script. For example, perform these steps to set the environment and superuser privileges for the wlsifconfig.sh script:

a. Grant `sudo` privilege to the Oracle WebLogic Server user ('oracle') with no password restriction, and grant execute privilege on the `/sbin/ifconfig` and `/sbin/arping` binaries.

b. Make sure the script is executable by the Oracle WebLogic Server user ('oracle'). The following is an example of an entry inside `/etc/sudoers` granting sudo execution privilege for `oracle` and also over `ifconfig` and `arping`:

```
oracle ALL=NOPASSWD: /sbin/ifconfig,/sbin/arping
```

Note: Ask the system administrator for the `sudo` and system rights as appropriate to this step.

18.3.8 Configuring Server Migration Targets

The fifth step is to configure server migration targets. You first assign all the available nodes for the cluster's members and then specify candidate machines (in order of preference) for each server that is configured with server migration.

Enterprise deployment recommends using cluster-based migration. Perform the following steps, including a step to enable automatic server migration (Step 10), to configure cluster-based migration for all Managed Servers in a cluster:

1. Log in to the Oracle WebLogic Server Administration Console. For example, `http://`*`domain_name`*`internal.mycompany.com`.
2. In the Domain Structure window, expand **Environment** and select **Clusters**. The Summary of Clusters page is displayed.
3. Click the cluster for which you want to configure migration (***CLUSTER***) in the Name column of the table.
4. Click the **Migration** tab.
5. Click **Lock & Edit**.
6. In the **Available** field, select the machine to which to allow migration and click the right arrow. In this case, select *`PROVISIONED_HOST`* and *`SCALED_OUT_HOST`*.

   Note: When there are three (3) hosts, select all three.

7. Select the data source to be used for automatic migration. In this case, select the leasing data source.
8. Click **Save**.
9. Click **Activate Changes**.
10. Enable automatic server migration for all Managed Servers in the cluster. (You must perform this task for all of the Managed Servers.)

    Note: Although you are using cluster-based migration for the Managed Servers, you must perform this step (from the **Migration** tab) to enable automatic server migration for all the Managed Servers in the selected cluster.

a. In the Domain Structure window of the Oracle WebLogic Server Administration Console, expand **Environment** and select **Servers**.

   Tip: Click **Customize this table** in the Summary of Servers page and move Current Machine from the Available window to the Chosen window to view the machine on which the server is running. This will be different from the configuration if the server gets migrated automatically.

b. Select the server for which you want to configure cluster-based migration.

c. Click the **Migration** tab, and then click **Lock & Edit**.

d. Select **Automatic Server Migration Enabled**. This enables Node Manager to start a failed server on the target node automatically.

e. Click **Save**.

f. Click **Activate Changes**.

g. Restart the administration server, node managers, and the servers for which server migration has been configured.

18.3.9 Testing the Server Migration

The sixth and final step is to test the server migration. Perform these steps to verify that server migration is working properly:

From PROVISIONED_HOST:

1. Stop the *WLS_SERVER1* Managed Server. To do this, run this command:

   ```
   PROVISIONED_HOST > kill -9 pid
   ```

   where *pid* specifies the process ID of the Managed Server. You can identify the pid in the node by running this command:

   ```
   PROVISIONED_HOST > ps -ef | grep WLS_SERVER1 | grep domain_name_SOACluster
   ```

2. Watch the Node Manager console. You should see a message indicating that *WLS_SERVER1*'s floating IP has been disabled.

3. Wait for Node Manager to try a second restart of *WLS_SERVER1*. It waits for a fence period of 10 seconds before trying this restart.

4. After Node Manager restarts the server, stop it few times. Node Manager should now log a message indicating that the server will not be restarted again locally.

From SCALED_OUT_HOST:

1. Watch the local Node Manager console. Ten (10) seconds after the last try to restart *WLS_SERVER1* on *PROVISIONED_HOST*, Node Manager on *SCALED_OUT_HOST* should prompt that the floating IP for *WLS_SERVER1* is being brought up and that the server is being restarted in this node.

2. As an example, for Oracle SOA Suite Managed Servers, access the soa-infra console in the same IP.

Verification from the Administration Console

Migration can also be verified in the Administration Console:

1. Log in to the Administration Console.

2. Click **Domain** on the left console.
3. Click the **Monitoring** tab and then the **Migration** subtab.

   The Migration Status table provides information on the status of the migration.

> **Note:** To complete server migration in a cluster, perform the same steps on the second, third, and so on, managed servers.

18.4 What to Do Next

If you have installed the Oracle Fusion Customer Relationship Management product offering, continue to Chapter 19. Otherwise, go to the chapter that corresponds to the product offering that is installed.

19

Completing Oracle Fusion Customer Relationship Management Post-Installation Tasks

This chapter describes the Oracle Fusion Customer Relationship Management (Oracle Fusion CRM) post-installation tasks you should review and complete before you can start working with your Oracle Fusion CRM implementation.

This chapter contains the following sections:

19.1 Installing and Configuring the Bounce Handling Daemon

The E-Mail Marketing Server is a combination of components designed to support high volume, personalized e-mail messages, and to track e-mail bounces and click-through responses. The bounce handling daemon (BHD) tracks e-mail messages that cannot be delivered, parses the returned e-mail messages, and records the cause of the e-mail bounce.

The bounce handling daemon installation program is available on the Oracle Fusion Middleware companion disk. Prior to installing the program, ensure you have provisioned the Marketing application, noting the Oracle SOA Suite Server host and port, and determined the designated server to place the daemon. The designated server must have port 25 available.

> **Note:** It is recommended that you place the bounce handling daemon in the DMZ. Optionally, you can place the bounce handling daemon behind an inbound mail transfer agent (MTA). The approach that you choose depends on the configuration of your network, DMZ, existing inbound mail transfer agent, and firewall.

Complete the following steps to install and configure the bounce handling daemon:

1. Using the companion disk, locate and run the installation program: `fusionbhd/Disk1/runInstaller`. Provide information when prompted, such as the JDK location, designated BHD server installation directory, and the http or https protocol, host and port for the Marketing SOA URL.
2. Navigate to the `WLS_HOME/config/fwmconfig` directory and copy the files and directory listed below to the `$HOME/bhd/fusionapps/crm/ewm/bhd/bin` directory.
   - jps-config-jse.xml
   - default-keystore.jks
   - bootstrap directory (including the cwallet.sso)
3. Update the root user permissions to allow read, write, and execute access to the jps-config-jse.xml and default-keystore.jks files and the bootstrap directory.
4. Update the root user permissions to allow read, write, and execute access to the BHD server installation directory, it's subdirectories and files. The top level BHD server installation directory is specified during the install process.
5. Grant read access to the fusionapps/crm/ewm/bhd/logs directory to nonroot users to provide availability to application log files.
6. Log in as a root user and enter the following to start the BHD service for port 25:

Server Platform	Action
UNIX	Navigate to the `fusionapps/crm/ewm/bhd` directory and enter the following command: ▪ `$ ./bin/bhd-onpremise-ctl.sh start`
Windows	Run the `bhd.exe` executable file.

For more information on provisioning, see Chapter 13, "Provisioning a New Oracle Fusion Applications Environment". For more information about configuring other aspects of the e-mail server for marketing, see the *Oracle Fusion Applications Marketing Implementation Guide*.

19.2 Setting Up SMS Marketing

To use the SMS marketing campaign capability within Oracle Fusion Customer Relationship Management, you need to enable it after installing Oracle Fusion Applications. Customers interested in SMS marketing campaigns will need to complete SMPP Driver configuration in the SOA suite component Oracle User Messaging Service.

An instance of the SMPP driver is already installed as part of the Oracle Fusion Applications installation and is a part of the Oracle User Messaging Service, but it does not point to any User Messaging Server. To configure the SMPP driver, you need to have an account with an SMPP driver gateway vendor.

IMPORTANT

Before proceeding with the enabling process, ensure that you have access rights to update and deploy applications on the WebLogic Administration Console and Oracle Enterprise Manager associated with the Customer Relationship Management domain.

1. Log in to the WebLogic Administration Console associated with the Customer Relationship domain.

   Under Deployments, you see the application **usermessagingdriver-smpp** in the **Installed** state.

2. Expand **usermessagingdriver-smpp** and navigate to Targets tab. The Current Targets column shows (None specified), indicating that no target is configured.

3. On the console, switch to the **Lock & Edit** mode, update the target to all servers in the CRM_SOACluster, and save the changes.

4. While remaining in the **Lock & Edit** mode for the console, navigate to Deployments, select the checkbox next to **usermessagingdriver-smpp**, and click Update. The Update Application Assistant wizard appears.

5. For the **Deployment Plan Path** field, click **Change Path** and select the Fusion Applications specific deployment plan:
   APPTOP`/instance/applications/ums/crm/usermessagingdriver-smpp_FusionPlan.xml`.

6. On the next screen of the Update Application Assistant wizard, select **Release Configuration** to commit the changes made until this point. The state of the application **usermessagingdriver-smpp** changes to **Active**.

7. Log out of WebLogic Administration Console.

8. Log in to the Oracle Enterprise Manager associated with the Customer Relationship Management domain.

9. Expand **CRMDomain - User Messaging Service**, right-click the application **usermessagingdriver-smpp** and select **SMPP Driver Properties** from the context menu.

10. Configure the driver and apply the changes.

11. Restart the usermessagingdriver-smpp application to bring into effect the driver configuration changes.

You can now use the SMS Marketing capability of Oracle Fusion Customer Relationship Management.

19.3 Setting Up Informatica Identity Resolution for Data Quality

Defining data quality involves setting up two functionalities, matching and address cleansing, by performing related regular and manual setup and maintenance tasks. Manual setup and maintenance tasks are performed on the related third-party data quality (DQ) engine, Informatica Identity Resolution (IIR).

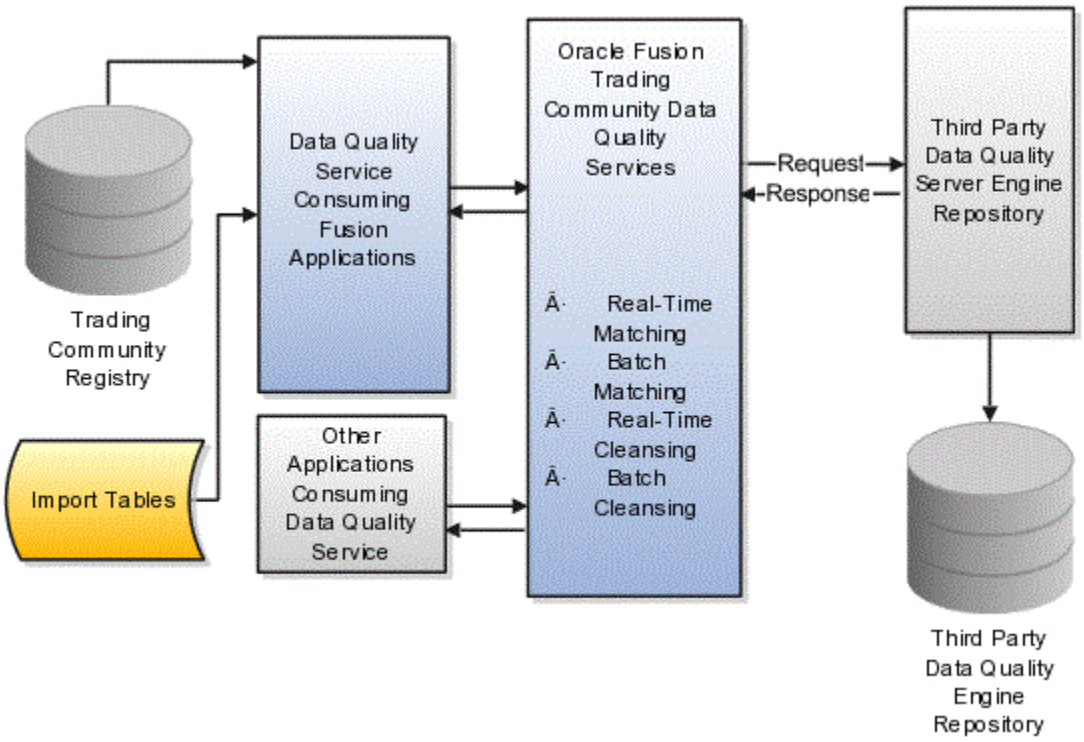
The Oracle Fusion Trading Community Data Quality matching and address cleansing services are designed to cater to all Oracle Fusion applications that use the trading community registry.

Matching is the identification of potential duplicates for organizations, persons, and locations. Potential duplicate records are identified and displayed in the data quality functionality consuming Oracle Fusion Applications during a variety of activities such

as duplicate prevention in real-time when a customer record is being created or duplicate identification in batch mode for existing records.

Address cleansing is the process of correction and validation of address data, based on postal requirements. For example, if a user enters valid values for postal code, city, and country, the data quality functionality may return a value for state. Likewise, if a user enters valid values for city, state, and country, the data quality functionality automatically supplies a postal code value.

The following figure illustrates the data quality management architecture. The data quality services receive matching or cleansing requests, such as duplicate prevention or address validation, from a variety of consuming applications, such as Oracle Fusion Sales and Oracle Fusion Trading Community Hub, and then internally invoke the appropriate third party services based either on a default configuration or a specific configuration passed to the services.



Matching and address cleansing are independent functionalities and are set up separately using the following steps:

- Setting up the third-party data quality (DQ) engine, Information Identity Resolution (IIR)

  Note: You can find the IIR vendor documentation in *APPLICATIONS_BASE*/InformaticaIR/pdf directory within the IIR Installation.

- Setting up the Fusion DQ Connector to IIR, by performing data quality related regular setup and maintenance tasks, such as defining and managing lookup choices and configurations used in data matching, cleansing, and matching index synchronization.

- Connecting Oracle Fusion Applications to the third-party data quality (DQ) engine, Informatica Identity Resolution (IIR).

19.3.1 Managing Lookups

Review and define lookup values that provide choices for data matching and cleansing, such as address fields, quality error messages, and match tolerances.

19.3.2 Managing Data Quality Configurations

Perform the configurations required to enable data quality processes such as data quality matching and cleansing operations.

You can enable data quality processes such as matching and address cleansing for real-time or batch matching and cleansing, and as part of the data import process.

Real-time matching can prevent individual entry of duplicate trading community entities, such as organization, person, or location, into the trading community registry. Batch matching leads to identification of duplicate entries in the trading community registry.

As part of defining and managing data quality configurations, you search, review, and edit seeded matching and cleansing configurations for real-time and batch matching and cleansing of trading community entities.

19.3.3 Managing Server Configurations

Define, review, and update the data quality server configurations to integrate with the embedded data quality engine.

Next, associate the server name with the matching and cleansing configurations to perform duplicate prevention, batch duplicate identification, and real-time and batch data cleansing.

19.3.4 Managing Matching Index Synchronization

Review and update matching index synchronization options, to synchronize Oracle Fusion Trading Community Hub registry data with the data quality engine repository, such as system and identity tables. View the latest synchronization results, evaluate errors, and reset for continued processing after resolving error conditions.

19.3.5 Managing Data Quality Engine

This section describes details to verify the installation of the third-party data quality (DQ) engine, Informatica Identity Resolution (IIR), used by Oracle Fusion Trading Community Data Quality, and perform IIR setup operations. The IIR setup operation are manual setup and maintenance tasks performed using the UI of the third-party data quality (DQ) engine.

Note: If you are working on the 64-bit operating systems of Oracle Enterprise Linux, Windows, AIX, or Solaris Sparc, when you provision Oracle Fusion CRM using the provisioning framework, an instance of IIR (64-bit) is automatically provisioned along side. However, for Solaris X-64-bit platform, IIR does not get provisioned. You need to install it manually on any of the other 64-bit operating systems. Except for the manual installation of IIR on a different platform, all the setup steps for Solaris X-64-bit platform are identical to other platforms.

Once the Oracle Fusion Applications environment is provisioned by Oracle Fusion Applications Provisioning Framework, do the following to verify IIR installation:

- Check whether InformaticaIR directory exists under *APPLICATIONS_BASE*.
- Check whether IIR is already running using `ps -ef | grep InformaticaIR`. There should be eight processes (or four pairs of parent-child processes) runing per server.

Note: If IIR post-provisioning verifications fail, perform IIR maintenance activities.

This table lists the processes that run when IIR is working

Table 19–1 IIR Processes

Server Name	Process Name	Port	Purpose
License Server	`ssalisv`	1601	Meant for licensing matching requests. You can configure the value of this port.
Search Server	`ssasrsv`	1666	Serves as an incoming matching request. Connects to the Rulebase server for system or Rulebase information.
Connection Server	`ssacssv`	1667	Meant for improving performance of search clients.
Console server	`ssacosv`	1669	Enables Informatica IR Console Client to access the Rulebase and other files and to launch other IIR utilities.
Rulebase Server	`ssasrsv`	1668	Meant for accessing the IIR Rulebase in the database and is relevant only for matching. There is no separate process for this. It is started as part of `ssasrsv`.

An instance of IIR uses seven ports. If IIR is provisioned through the framework, the value of the license server port is determined by the value of the `property provisioning.setup.app-ports.core.iir.port` that is set in the provisioning plan. If IIR is installed manually, the value of the license server port is determined by `IIR_INSTANCE_1_PORT` in the `install.props` file.

The seven ports are listed here. For example, if the port value set for `provisioning.setup.app-ports.core.iir.port` uses the default value 1601, the ports occupied for Informatica Identity Resolution would have the following values:

- SSA_LIPORT= <value set for the property `provisioning.setup.app-ports.core.iir.port`>=1601
- SSA_SEPORT=1666
- SSA_COPORT=1667
- SSA_RBPORT=1668
- SSA_CSPORT=1669
- SSA_XMPORT=1670
- SSA_HTPORT= <value set for the property `provisioning.setup.app-ports.core.iir.port`> + 11= 1612

> **Note:** The value of `SSA_LIPORT` can be found in *`APPLICATIONS_BASE`*`/InformaticaIR/env/envs` and the values of all other ports can be found in *`APPLICATIONS_BASE`*`/InformaticaIR/env/isss`.

When post-provisioning checks are successful, perform these post-provisioning operations sequentially to set up IIR:

1. IIR Matching Setup. For more information, see: Informatica Identity Resolution Matching Setup: Procedures.
2. IIR Address Cleansing Setup. For more information, see: Informatica Identity Resolution Address Cleansing Setup: Procedures.
3. Oracle Fusion Data Quality Connector Setup. For more information, see: Fusion Data Quality Connector Setup: Procedures.

19.3.5.1 Setting Up Multiple Informatica Identity Resolution Instances: Overview

Set up multiple Informatica Identity Resolution (IIR) instances to make use of client load balancing capabilities of IIR to implement failover. You can configure the Oracle Fusion Data Quality Connector to allow Oracle Fusion Applications to speed up data quality management operations and to avoid overload by sending matching and cleansing calls to different IIR instances. Note that the multiple instances do not require any data or repository replication and can work with one Oracle Fusion Application Database.

> **Note:** The setup mentioned in this section is not mandatory and should be used only based on use cases, and in a specific deployment scenario.

Use multiple instances of the IIR and setup the Oracle Fusion Data Quality Connector appropriately to make use of load balancing to implement failover as follows:

- Load balacing by matching and cleansing on different dedicated hosts
- Load Balancing by matching with a secondary match server
- Load Balancing and failover by matching and cleansing using a secondary instance

For more information on these load balancing and failover scenarios, refer to the Related Topics.

Note: Informatica Identity Resolution (IIR) Server does not support native server load balancing.

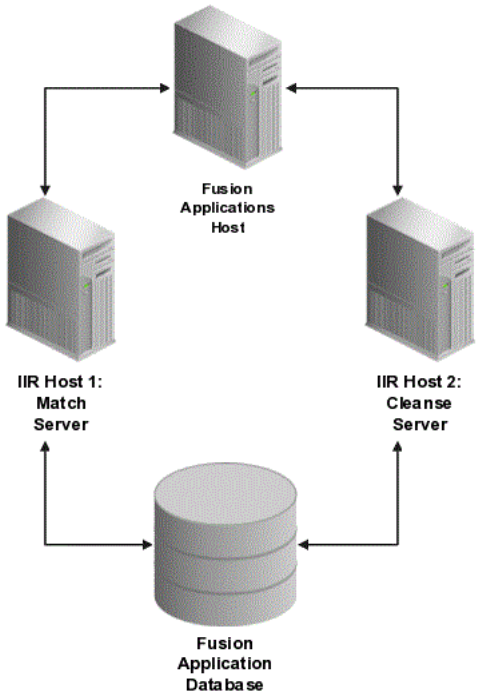
Take note of the following assumptions and constraints before using multiple instances of the IIR and the Oracle Fusion Data Quality Connector setup for load balancing and failover:

- Oracle Fusion CRM is provisioned with only one instance of IIR. Consequently, load balancing and failover using multiple instances of the IIR and the Oracle Fusion Data Quality Connector setup require manual installation of IIR for every additional instance. Since the installation of IIR through provisioning includes a bare minimum of IIR schema objects required in Oracle Fusion Applications Database, make sure that those schema objects are not installed again during the manual installation of IIR.
- Load balancing cleansing is not described as a separate scenario. Instead, the steps for load balancing and failover of cleansing operations are included as optional steps in the scenarios for load balancing and failover of matching operations.
- One or more instances of Oracle Fusion Applications and IIR may be installed on an Oracle Fusion Applications host.
- You cannot load balance and failover the update synchronizer. It can run only on one host.
- Any rollback of changes, for example reverting to a single instance, while load balancing using a secondary server requires a `delete_secondary_server.sql` and also requires the bouncing of application servers hosting Oracle Fusion Applications that use real-time data quality.

19.3.5.2 Load Balancing by Matching and Cleansing on Different Dedicated Hosts: Procedures

This section describes details for load balancing with no specific requirement for high availability, or failover, by performing the matching and cleansing operations on dedicated hosts.

The following figure provides a visual representation of the load balancing process achieved by matching and cleansing on different dedicated hosts.



19.3.6 Configuring the Primary and Secondary IIR Hosts

Use the following steps to configure the IIR hosts:

1. Manually install Informatica Identity Resolution (IIR) on the secondary host, making sure `INSTALL_IIR_OBJECTS=N`. In other words, make sure that the schema objects installed during installation of IIR through provisioning are not installed again during the manual installation of IIR. For more information, see: Manually Installing Informatica Identity Resolution: Procedures
2. Perform all the matching setup steps in the primary IIR host.
3. Perform all the cleansing setup steps in the secondary IIR host.

19.3.7 Configuring the Oracle Fusion Data Quality Connector

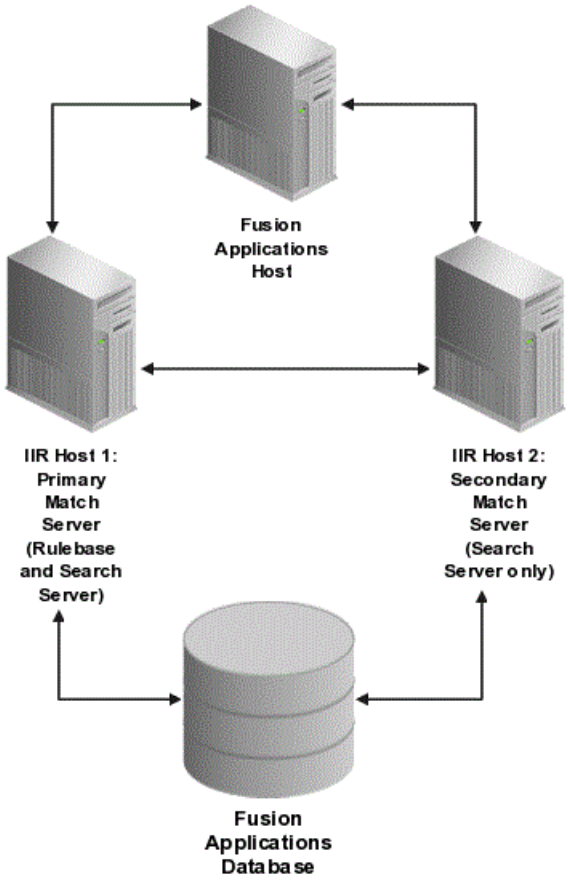
Use the following steps to configure Oracle Fusion Data Quality Connector:

1. In the Real-time and Batch Basic Server, enter the server address and server port of the primary IIR host, the IIR Matching Server.
2. In the Real-Time Cleanse Server and Batch Cleanse Server, enter the server address and server port of the secondary IIR host, the IIR cleansing server.

19.3.7.1 Load Balancing by Matching and Cleansing with Secondary Servers: Procedures

Use this procedure for load balancing with no specific requirement for high availability, or failover, by performing the matching operations on a secondary match server.

This figure provides a visual representation of the load balancing process for matching operations achieved by matching with a secondary match server.



19.3.8 Configuring the Secondary Match Server

Use the following steps to configure the secondary match server:

1. Manually install Informatica Identity Resolution (IIR) on the secondary match server, making sure `INSTALL_IIR_OBJECTS=N`. In other words, make sure that the schema objects installed during installation of IIR through provisioning are not installed again during the manual installation of IIR. For more information, see: Manually Installing Informatica Identity Resolution: Procedures.
2. Make sure IIR on the secondary match server has access to an Oracle DB client to connect to the Fusion Application Database and the `tnsnames.ora` has all the relevant SID information. Shut down IIR on the secondary match server.
3. Perform all the matching setup steps using IIR on primary match server. Shut down IIR on primary match server.
4. Start IIR on primary match server.
5. Start IIR as a search server only on the secondary match server by doing the following:

   APPLICATIONS_BASE`/InformaticaIR/bin > bash`

```
APPLICATIONS_BASE/InformaticaIR/bin  > . ./setfusionEnv.sh
APPLICATIONS_BASE/InformaticaIR/bin  > . ../env/isss
APPLICATIONS_BASE/InformaticaIR/bin  > ./ssasrsv -n{SEPORT2}
-h{RBHOST1}:{RBPORT1} -1$SSATOP/iirlog/idssrsv.log -2$SSATOP/iirlog/idssrsv.err
-3$SSATOP/iirlog/ids.dbg &
```

Note: The Search Server in Host 2 is started by pointing its port (SEPORT2) to the Rulebase Server's host (RBHOST1) and port (RBPORT1) in the primary match server. Here:

- SEPORT2 = Search Server Port (SSA_SEPORT defined in InformaticaIR/env/isss on IIR Host 2. The default port is 1666).
- RBHOST1 = Hostname or IP of IIR Host 1
- RBPORT1 = Rulebase Server Port (SSA_RBPORT defined in InformaticaIR/env/isss on IIR Host 2. The default port is 1668.

6. On Host 1 (Primary Host), start the IIR Update Synchronizer process using the following steps:
    1. Log in the Informatica Identity Resolution (IIR) host machine.
    2. Enter `cd APPLICATIONS_BASE/InformaticaIR/bin`.
    3. Enter `setfusionEnv.sh`.
    4. Start the IIR console client using the admin option, `./idsconc -a`.
    5. Select Run Synchronizer on the Tools menu to launch the synchronizer.
    6. In the Update Synchronizer dialog, select **All** as the value for **IDT Name**, use the default values for the rest of the fields and click **OK**.
    7. Verify that the updated and newly created person records are available in IIR by searching for person sin the Per-dup tab of IIR Web Search Client.
    8. Log out of the Informatica Identity Resolution (IIR) user interface.
7. In the Oracle Fusion DQ Connector, on the Manage Server Configuration page, update the `SecondaryServer1Address` and `SecondaryServer1Port` values respectively for the host name and port of the Secondary Server (Host 2). These parameters can be found in the Server Parameter Values section.
8. Select the **Enable High Availability** checkbox for each server operation.
9. Click **Save and Close**.

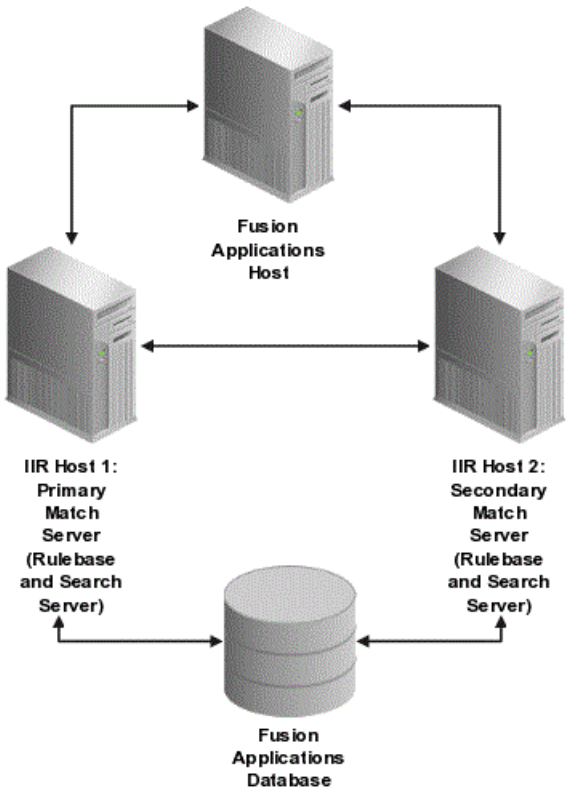
Note: Repeat Steps 7, 8, and 9 for each server configuration: Realtime and BatchBasic Server, Batch Cleanse Server, and Realtime Cleanse Server.

10. Restart the Oracle Fusion Applications instances that require data quality management to enable Oracle Fusion Data Quality Connector to commence load balancing and failover.

19.3.9 Load Balancing and Failover by Matching and Cleansing Using a Secondary Instance: Procedures

Use this procedure for load balancing to implement high availability, or failover, by performing both matching and cleansing operations using a secondary instance of Informatica Identity Resolution (IIR).

The following figure provides a visual representation of the load balancing and failover process achieved by matching and cleansing using a secondary instance.



19.3.10 Configuring the Secondary Instance of IIR to Load Balance and Failover

Use the following steps to configure the secondary instance of Informatica Identity Resolution (IIR) to load balance and failover matching and cleansing:

1. Manually install Informatica Identity Resolution (IIR) on the secondary host, making sure `INSTALL_IIR_OBJECTS=N`. In other words, make sure that the schema objects installed during installation of IIR through provisioning are not installed again during the manual installation of IIR. For more information, see: Manually Installing Informatica Identity Resolution: Procedures.

Note: Since there are two Oracle Fusion Applications instances in this scenario, the secondary IIR instance may already be installed. In such cases, you need to only configure the Oracle Fusion Data Quality Connector so that it points to the same Oracle Fusion Database as the primary IIR instance. For more information, see: Oracle Fusion Data Quality Connector Setup: Procedures.

2. Make sure IIR on the secondary host has access to an Oracle DB client to connect to the Fusion Application Database and the `tnsnames.ora` has all the relevant SID information. Shut down IIR on the secondary host.
3. Perform all the matching setup steps using IIR on primary host. Shut down IIR on primary host.
4. Start IIR on primary host, Host 1, by starting the Rulebase Server first followed by starting the Search Server.

```
APPLICATIONS_BASE/InformaticaIR/bin > bash
APPLICATIONS_BASE/InformaticaIR/bin  > . ./setfusionEnv.sh
APPLICATIONS_BASE/InformaticaIR/bin  > . ../env/isss
APPLICATIONS_BASE/InformaticaIR/bin  > ./ssasrsv -m{RBPORT1}
-gFusionRBSG,ssa:rtunitrb -w1 -1$SSATOP/iirlog/priRB.log
-2$SSATOP/iirlog/priRB.err -3$SSATOP/iirlog/priRB.dbg &
APPLICATIONS_BASE/InformaticaIR/bin  >./ssasrsv -n{SEPORT1}
-gFusionRBSG,ssa:rtunitrb -1$SSATOP/iirlog/priSE.log -2$SSATOP/iirlog/priSE.err
-3$SSATOP/iirlog/priSE.dbg &
```

5. Start IIR on the secondary host, Host 2, by starting the Rulebase Server first, followed by starting the Search Server.

```
APPLICATIONS_BASE/InformaticaIR/bin > bash
APPLICATIONS_BASE/InformaticaIR/bin  > . ./setfusionEnv.sh
APPLICATIONS_BASE/InformaticaIR/bin  > . ../env/isss
APPLICATIONS_BASE/InformaticaIR/bin  >./ssasrsv -m{RBPORT2}
-gFusionRBSG,ssa:rtunitrb -w1-1$SSATOP/iirlog/secRB.log
-2$SSATOP/iirlog/secRB.err -3$SSATOP/iirlog/secRB.dbg &
APPLICATIONS_BASE/InformaticaIR/bin  >./ssasrsv -n{SEPORT2}
-gFusionRBSG,ssa:rtunitrb -1$SSATOP/iirlog/secSE.log -2$SSATOP/iirlog/secSE.err
-3$SSATOP/iirlog/secSE.dbg &
```

6. Start IIR Console on the primary host, Host 1.

```
APPLICATIONS_BASE/InformaticaIR/bin > ./ssacssv -o -n{CSPORT1}
-hselocalhost:{SEPORT1} -hcolocalhost:{COPORT1}
-hhtlocalhost:{HTPORT1} -gFusionRBSG,ssa:rtunitrb -w$SSATOP/ids
-1$SSATOP/iirlog/cons.log -2/$SSATOP/iirlog/cons.err
-3$SSATOP/iirlog/cons.dbg &
```

   For example:

```
APPLICATIONS_BASE/InformaticaIR/bin > ./ssacssv -o -n1669 -hselocalhost:1666
-hcolocalhost:1667
-hhtlocalhost:1612 -gFusionRBSG,ssa:rtunitrb -w$SSATOP/ids
-1$SSATOP/iirlog/cons.log -2/$SSATOP/iirlog/cons.err
-3$SSATOP/iirlog/cons.dbg &
```

7. Start IIR Connection Server on the primary host, Host 1.

```
APPLICATIONS_BASE/InformaticaIR/bin > ./ssacosv -hlocalhost:1666 -n1667 -t5
-1$SSATOP/iirlog/conn.log
-2/$SSATOP/iirlog/conn.err -3$SSATOP/iirlog/conn.dbg &
```

Note:

- RBPORT1 and RBPORT2 respectively are the ports for the Rulebase Server on IIR Host 1 and IIR Host 2 respectively. The values for these parameters should respectively be the value of SSA_RBPORT in `InformaticaIR/env/isss` on Hosts 1 and 2.
- SEPORT1 and SEPORT2 respectively are the ports for the Search Server on IIR Host 1 and IIR Host 2. The values for these parameters should respectively be the value of SSA_SEPORT in `InformaticaIR/env/isss` on Hosts 1 and 2.
- CSPORT1 is the port for the Console Server on IIR Host 1. The values for this parameter should be the value of SSA_CSPORT in `InformaticaIR/env/isss` on Hosts 1.
- COPORT1 is the port for the Connection Server on IIR Host 1. The values for this parameter should be the value of SSA_COPORT in `InformaticaIR/env/isss` on Hosts 1.
- HTPORT1 is the port for the HTTP Search Server on IIR Host 1. The values for this parameter should be the value of SSA_ HTPORT in `InformaticaIR/env/isss` on Hosts 1.
- The parameter w1 specifies that the polling frequency of the Secondary Server to determine if the Primary Server is active is one second. For example, if the value of the parameter is set to w10 then the polling frequency of the Secondary Server to determine if the Primary Server is active will be 10 seconds.
- Steps 4 and 5 essentially start the Rulebase Servers in a group, making sure, that even if one matching instance fails, the other can continue to function. Only one Rulebase server (primary) in the group is permitted to respond to queries and the other (secondary) server periodically polls the primary server to determine if it is active.
- In the scenario in which load balancing is done by matching with a secondary match server, if the primary server (Host 1) fails, matching will stop functioning unless it is restored. In contrast, in the present scenario, if the primary server (Host 1) fails, the secondary server (Host 2) takes the role of the primary server, with no expectation of Host 1 to be restored. However, there is a small latency in the secondary server assuming the role of the primary server and there could be a loss of the matching functionality during this temporary latency period.

8. On Host 1 (Primary Host), start the IIR Update Synchronizer process using the following steps:
    1. Log in the Informatica Identity Resolution (IIR) host machine.
    2. Enter `cd` *`APPLICATIONS_BASE`*`/InformaticaIR/bin`.
    3. Enter `setfusionEnv.sh`..
    4. Start the IIR console client using the admin option, `./idsconc -a`.
    5. Select **Run Synchronizer** on the **Tools** menu to launch the synchronizer.

6. In the Update Synchronizer dialog, select **All** as the value for **IDT Name**, use the default values for the rest of the fields and click **OK**.
7. Verify that the updated and newly created person records are available in IIR, by searching for persons in the Per-dup tab of IIR Web Search Client.
8. Log out of the Informatica Identity Resolution (IIR) user interface.

9. In the Oracle Fusion DQ Connector, on the Manage Server Configuration page, update the `SecondaryServer1Address` and `SecondaryServer1Port` values respectively for the host name and port of the Secondary Server (Host 2). These parameters can be found in the Server Parameter Values section.
10. Select the **Enable High Availability** checkbox for each server configuration.
11. Click **Save and Close**.

> **Note:** Repeat Steps 9 to 11 for each server operation: Realtime and BatchBasic Server, Batch Cleanse Server, and Realtime Cleanse Server.

12. Restart the Oracle Fusion Applications instances that require data quality management to enable Oracle Fusion Data Quality Connector to commence load balancing and failover.

19.3.11 Informatica Identity Resolution Server Maintenance and Administration: Procedures

Administration and maintenance includes start up and shutdown activities of the Informatica Identity Resolution (IIR) server and how Oracle database interacts with the IIR server. It also includes locking and unlocking of the Rulebase and how you can use the Informatica IR Console Client.

To start the IIR server, enter the following commands:

```
APPLICATIONS_BASE/InformaticaIR/bin> bash
APPLICATIONS_BASE/InformaticaIR/bin>. ./setfusionEnv.sh
```

> **Note:** If you are using C Shell, use the command `source setfusionEnv.csh`.

```
APPLICATIONS_BASE/InformaticaIR/bin> ./liup
APPLICATIONS_BASE/InformaticaIR/bin> ./idsup
APPLICATIONS_BASE/InformaticaIR/bin> ./idsconc -a
```

> **Note:** Start the Update Synchronizer from the IIR Admin Console. However, after starting the Update Synchronizer, shut down the IIR Admin Console, For more information on Starting Up and Shutting Down Update Synchronizer, refer to the topic Informatica Identity Resolution Matching Setup: Procedures.

To shut down the server, enter the following commands:

Note: If the Update Synchronizer is running (check for the `updsync` process), stop it from the IIR Admin Console. After stopping the Update Synchronizer, shut down the IIR Admin Console. For more information on Starting Up and Shutting Down Update Synchronizer, refer to the topic Informatica Identity Resolution Matching Setup: Procedures.

```
APPLICATIONS_BASE/InformaticaIR/bin> bash
APPLICATIONS_BASE/InformaticaIR/bin>. ./setfusionEnv.sh
```

Note: If you are using C Shell, use the command `source setfusionEnv.csh`.

```
APPLICATIONS_BASE/InformaticaIR/bin> ./idsdown
APPLICATIONS_BASE/InformaticaIR/bin> ./lidown
```

Note: It is strongly recommended that you verify the Informatica Identity Resolution after every startup or a restart.

To shut down the primary and secondary servers make sure the following steps are followed:

1. Stop Update Synchronizer on the primary server.
2. Stop license server on the Primary and all other servers on both Primary and Secondary server as follows:

```
APPLICATIONS_BASE/InformaticaIR/bin > bash
APPLICATIONS_BASE/InformaticaIR/bin > . ./setfusionEnv.sh
 APPLICATIONS_BASE/InformaticaIR/bin > lidown
 APPLICATIONS_BASE/InformaticaIR/bin > ./ssashut -h<HOST>:<PORT>
```

Note: Do the `ssashut` for all servers started using their respective host and port.

Before handing over an environment for business use, you need to perform certain checks to determine if IIR is working properly. Perform the checks after performing either of these activities:

- Setting Up Informatica Identity Resolution sever for the first time
- Restarting the Informatica Identity Resolution sever for any reason such as after a maintenance window or a scheduled downtime (patching, bouncing the database, troubleshooting and so on)

If any of the IIR configuration checks fail, the data quality functionality will not work. For information on troubleshooting, refer to the Troubleshooting Informatica Identity Resolution and Data Quality Setup: Overview help topic listed in the Related Topics section.

Perform the following checks to verify Informatica Identity Resolution (IIR) configuration:

- IIR Server Check: Verify that the total number of processes running for IIR search components is eight.

The following table lists the names and numbers of the processes running for IIR search components.

Table 19–2 IIR Search Component Processes Numbers

IIR Search Component Process name	Number of Processes
ssasrsv	2
ssalisv	2
ssacssv	2
ssacosv	2

On a Linux operating system, run the following command to verify that the total number of processes running for IIR search components is eight:

```
ps -ef | grep InformaticaIR | grep -v updsync
```

- IIR Update Synchronizer Check: Verify that the total number of processes running for Update Synchronizer is two.

  On a Linux operating system, run the following command to verify that the total number of processes running for Update Synchronizer is two:

  ```
  ps -ef | grep InformaticaIR | grep updsync
  ```

- IIR Test Search Client Check: Use the following steps to perform this check:

  1. Run the following command to get the search client: `grep SSA_HTPORT` *`APPLICATIONS_BASE`*`/InformaticaIR/env/isss`.
  2. In a browser, access the client application: `http://Your_IIR_Host_Env_IP_Address:SSA_<HTPORT>/systems`.

     For example: `http://xyz123.us.zzz.com:1612/systems`
  3. Select any system from the dropdown list and click **Next**.
  4. Type an appropriate value and click **Submit Search**.

     Note that there are no errors.

- IIR Wiring Check: Verify that the data quality Web Services are up and running and Oracle Enterprise Manager is accessible. Use the following steps to perform this check:

  1. Log in to Oracle Enterprise Manager.
  2. From the Navigation menu, select **Fusion Applications - Oracle Fusion Customer Relationship Management**.
  3. Select `CrmCommonApp` and then select `CRMCommonServer_1`.
  4. Under the Web Services section, select `DQRealTimeService` and click **Test** to launch the Web Service Tester.
  5. On the Test Web Service Page, select **cleanseAddress** from the **Operation** drop down list.
  6. On the Request tab, select **Custom Policy** security option and enter the Policy URL syntax `oracle/wss11_username_token_with_message_protection_client_policy` and the username and password for a user who has the **ZCH_MASTER_DATA_MANAGEMENT_APPLICATION_ADMINISTRATOR_**

JOB role. For example, in development environments, this could be `MDM_ADMIN_V1`.

7. Under Input Arguments, select **XML View**.
8. Run the following blocks of code by selecting the corresponding operation from the dropdown list for each block of code and clicking **Test Web Service**.
   - Select **cleanseAddress** from the **Operation** dropdown list and submit the following payload:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Body
xmlns:ns1="http://xmlns.example.com/apps/cdm/dataQuality/realTime/publi
cModel/types/">
<ns1:cleanseAddress>
<ns1:input
xmlns:ns2="http://xmlns.example.com/apps/cdm/dataQuality/realTime/publi
cModel/">
  <ns2:DataQualityRequestId />
  <ns2:ConfigCode>RT_LOC_CLEANSE</ns2:ConfigCode>
  <ns2:ErrorCode />
  <ns2:Message />
  <ns2:DataQualityAddress>
  <ns2:DataQualityRequestId />
  <ns2:DataQualityRecordType />
  <ns2:AddressLine1>500 oracle pky</ns2:AddressLine1>
  <ns2:AddressLine2 />
  <ns2:AddressLine3 />
  <ns2:AddressLine4 />
  <ns2:City />
  <ns2:Country>US</ns2:Country>
  <ns2:CountrySubEntity />
  <ns2:LocationIdentifier />
  <ns2:PostalCode>94065</ns2:PostalCode>
  </ns2:DataQualityAddress>
  </ns1:input>
  </ns1:cleanseAddress>
  </soap:Body>
  </soap:Envelope>
```

   - Select the operation **matchOrganization** from the **Operation** drop-down list and submit the following payload:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Body
xmlns:ns1="http://xmlns.example.com/apps/cdm/dataQuality/realTime/publi
cModel/types/">
<ns1:matchOrganization>
<ns1:input
xmlns:ns2="http://xmlns.example.com/apps/cdm/dataQuality/realTime/publi
cModel/">
  <ns2:DataQualityRequestId />
  <ns2:ConfigCode>RT_ORG_DUP_PREV</ns2:ConfigCode>
  <ns2:ErrorCode />
  <ns2:Message />
  <ns2:DataQualityOrg>
  <ns2:OrganizationName>Yamaha</ns2:OrganizationName>
  </ns2:DataQualityOrg>
  </ns1:input>
  </ns1:matchOrganization>
  </soap:Body>
  </soap:Envelope>
```

9. Check if the responses to the above requests do not return the following `ErrorCode`:

```
<ns0:ErrorCode>ERRORED</ns0:ErrorCode>
<ns0:Message>ZCQ_CMN_ENG_CONNECT_ERR</ns0:Message>
```

If you are setting up IIR for matching, you must understand how the IIR Server interacts with the Oracle database. When you start an IIR server, the Rulebase Server also starts, but it does not connect to the Oracle database until the first client makes a request. For example, for a search request, a match call made from Oracle Fusion Applications. For an administrator request, a user starting the Informatica IR Console client. A Rulebase server uses and maintains this connection unless IIR is brought down with an idsdown command. Once a Rulebase server connects to the Oracle database, it creates a lock that ensures that no other Rulebase server connects to the Rulebase.

When the IIR server is up and the Oracle database is shut down or crashes, or if there is a network issue that affects connectivity, the Rulebase lock remains active. In such cases where a lock is active, all future search requests fail with an error that indicates there is another Rulebase server running.

The following table lists various situations that can occur after the IIR and Oracle database connection has been established.

Table 19–3 Procedures for IIR and Oracle Database Connection Possibilities

Possibility	Procedure
Shutting down Oracle Database	Shut down the IIR Server before shutting down the Oracle database. Else, the Rulebase is locked and it fails all future requests. Once Rulebase is locked, you need to manually unlock it.
Database crashes or there is a connectivity issue	Unlock the Rulebase manually.
IIR server crashes or reboots due to power outage, or any similar case	Rulebase is automatically unlocked by the first client. No manual intervention is required.
IIR is shut down improperly, for example, with the Update Synchronizer running	TheRulebase can become corrupt. Clean the Rulebase or create it again.

Every time an IIR server starts, a new pair parent/child Rulebase also starts. The parent server generates a new unique ID and this ID is stored in the Rulebase. In case of a Rulebase lock, if the ID generated by the parent is not equal to the ID stored in the Rulebase, the child server fails to start.

You must unlock the Rulebase manually. To do this, set an environment variable to the same ID that locks the Rulebase. Here is an example of a message that appears when a Rulebase lock is in force:

```
IS ANOTHER RULEBASE SERVER RUNNING?
Rulebase sdb:file:c:\a3i\ids\rule In use by ssa.identitysystems.com
IP=203.2.203.109 on port=1668, SSA_RB_RESTART_ID=281753650
```

For this message, enter *`APPLICATIONS_BASE`*`/InformaticaIR/bin > set SSA_RB_RESTART_ID=281753650` and then start the IIR server.

When the Rulebase server starts, it uses the environment variable to unlock the Rulebase when the two IDs match. It then uses the freshly generated parent ID to lock it again. A locked Rulebase can be unlocked only once using the same ID.

You can use the Informatica IR Console client for the following operations:

- For creating and indexing IIR search systems.
- Starting or monitoring the Update Synchronizer.
- Perform test searches using the search client or enabling search traces to understand or debug search behavior.
- For advanced configuration, where an existing system is edited using hte System Editor to change its behavior.

These are the restrictions on using the Informatica IR Console client:

- The console client is not a multiuser application when it is used with `-a` (administrative) option, which has `read` and `write` privileges. Only single invocation of the client is possible with `-a` option. Without `-a` option, the Rulebase opens `read only`.
- Once the administration operations have been performed, there is no need for the client to be open. Close it after use. For example, after starting the Update Synchronizer, you can close the console client but this does not affect the synchronizer.
- If the Informatica IR Console client is left connected for several days and there is a database or network interruption, the following situations can occur:
  - Update Synchronizer fails, it cannot be restarted through the client unless the client is restarted.
  - Client loses all functionality except for **Tools** and **Search Client** unless restarted.
  - You do not need to restart the IIR server for restarting client connection.

19.3.12 Encrypting the Informatica Identity Resolution Dictionary-alias File: Explained

Clients such as Console Client or Fusion Real-Time and Batch that connect to IIR, pass a mandatory parameter called Rulebase name. It is an alias for the connection string required by IIR to connect to the FUSION_DQ schema in the Oracle Fusion Applications Database. The alias is defined in a file called `ssadb.dic` in *`APPLICATIONS_BASE`*`/InformaticaIR/ids` directory.

The following example shows how a typical `ssadb.dic` would look.

```
rtunitrb odb:0:fusion_dq/fusion_dq@rws65311
fusion_s01 odb:1:fusion_dq/fusion_dq@rws65311
btunitrb odb:1:fusion_dq/fusion_dq@rws65311
fusion_s02 odb:2:fusion_dq/fusion_dq@rws65311
zcqsrc odb:99:fusion_dq/fusion_dq@rws65311
```

The alias `rtunitrb` is the alias for the Rulebase name. The remaining aliases are used for different purposes. For example, `fusion_s01` is used to create the FusionDQRealtime System, `zcqsrc` is used by the loader process to get source data from Oracle Fusion and so on.

Note: The setup mentioned here is not mandatory and should be used only based on use cases, and in a specific deployment scenario.

19.3.13 Changing Rulebase Names

In Oracle Fusion, the predefined alias for the Rulebase name is `rtunitrb`. If there is ever a need to change the Rulebase name, you can change it in the dictionary file, and ensure that the change is also carried over to the Server Operation Page (used in IIR Matching). For example, if `rtunitrb` is changed to `foo`, then the Rulebase alias in the Server Operation Page should be changed from `ssa:rtunitrb` to `ssa:foo`. If you made this change while the server was up and running, you need to restart the IIR Server to bring the change into effect.

19.3.14 Encryption ssadb.dic

It is recommended to create a backup copy of the `ssadb.dic` file and store it as a template for future use, before encrypting it. It is also recommended to replace the password on the backup copy with an empty string. You can later provide a password for this backed up copy, if you intend to use it.

Access the directory where PERL is available, either using `$PATH` or the absolute path and do the following:

- On Windows, run the following commands:
  - *APPLICATIONS_BASE*`\InformaticaIR\bin > isss.bat`
  - *APPLICATIONS_BASE*`\InformaticaIR\bin > perl convfusiondict.pl <password>`
- On OracleEnterprise Linux, run the following commands:
  - *APPLICATIONS_BASE*`/InformaticaIR/bin >. .setfusionEnv.sh`

    Note: If using C-SHELL, use source `setfusionEnv.csh` instead of `setfusionEnv.sh`

  - *APPLICATIONS_BASE*`/InformaticaIR/bin > perl convfusiondict.pl <password>`

    Note: In these commands, <password> can be any string that the administrator chooses. Password protects the dictionary file from being edited (either to add a new entry or delete an existing entry). In Oracle Fusion Applications, this password is a place holder to run the `iirdict` utility.

19.3.15 Changing Password after Encryption

After `ssadb.dic` is encrypted, there may be occasions where the password for `FUSION_DQ` might be changed by a database administrator, as part of security due diligence.

To change the password for `ssadb.dic`, do the following.

1. Take a backup of the existing `ssadb.dic` (as mentioned in the earlier section).
2. Delete the existing `ssadb.dic` (in use).
3. Enter the new password for the backup up file and rename the file to `ssadb.dic`.
4. Encrypt the file as mentioned previously.

19.3.15.1 Manually Installing Informatica Identity Resolution: Procedures

This topic describes the provisioning and platform support, software requirements, and the steps for the manual installation of Informatica Identity Resolution (IIR).

19.3.16 Assessing Provisioning and Platform Support

Use this information to determine whether you need to install IIR manually.

When Oracle Fusion CRM is provisioned using the provisioning framework, an instance of IIR (64-bit) is provisioned on the following platforms: OEL 64-bit, Windows 64-bit, AIX 64-bit, Solaris Sparc 64-bit.

However, IIR is not provisioned as part of Oracle Fusion CRM Provisioning for the Solaris X-64-bit platform. For this platform, install IIR manually on any of the supported platforms such as OEL 64-bit. Except for the manual install, IIR setup steps for Solaris X-64-bit platform are identical to those for other platforms such as OEL 64-bit.

19.3.17 Assessing Software Requirements

Use this information to ensure compliance with the software requirement for the manual installation of IIR.

The host on which IIR is installed should have access to an Oracle DB Client for connecting to the Oracle Fusion Applications Database.

The host should have its `GNU libc` version 2.5

The size of `FUSION_TS_DQ` (the default table space for the Oracle Fusion data quality and hence the repository for IIR), should have a table space size at least 10 times the size of the data. The data here represents the fields used in `FusionDQ Realtime.sdf`.

19.3.18 Installing Informatica Identity Resolution

Use the following steps to manually install IIR on the OEL 64-bit platform.

1. Unzip the following files in an appropriate location:
   - `IIR_901sp1_linux_amd64.zip`
   - `Fusion-Exts-IIR-901sp1.zip`

   Note: This file resolves to `fusion_iir` after unzipping.

2. Go to the `fusion_iir` directory and edit the `install.props` file to make sure the properties described in the following table are populated correctly.

   Note: The following table describes the properties and their values that must be populated correctly for installing IIR manually. None of the properties except the ones mentioned in this table should be modified.

Table 19–4 Properties for Manual Install

Properties	Value Descriptions (To be Replaced with Actual Values	Sample Values
ORACLE_HOME	Oracle home for DB client used by IIR	
TNS_ADMIN	TNS_ADMIN for DB client used by IIR	
LD_LIBRARY_PATH	Library path on IIR host	
FUSION_STAGE_DIR	Directory where Fusion Ext Zip is unzipped	
IIR_STAGE_DIR	Directory where IIR Zip is unzipped	
IIR_VERSION	Name of the version to which the IIR unzip resolves	IIR_901sp1_linux_amd64
IIR_DB_HOSTNAME	Fusion Application DB host	
IIR_DB_PORT	Fusion Application DB port	
IIR_DB_SID	Fusion Application DB SID	
IIR_DB_SUSER	fusion_dq	
IIR_DB_PASSWD	Credentials for fusion_dq	
IIR_INSTALL_LOG_LOC	Location to which Install logs should go	
IIR_INSTANCE_1_PORT	Start port for the license server	1660 (if available, this port should work fine as the default port)
INSTALL_IIR_OBJECTS	Yes or No	No (if IIR is installed as a Secondary Server; for more information, see: Setting up Multiple Informatica Identity Resolution Instances: Overview

3. Execute the following command after changing to the fusion_iir directory: runInstaller.sh install.props.

   It typically takes about 8 to 12 minutes to install IIR.

> **Note:** Use the same steps to install IIR on the Windows 64-bit platform, except for running runInstaller.bat in fusion_iir.

19.3.19 Manage Server Configurations

Server configurations are predefined configurations for third-party data quality servers.

You can search, review, and edit server configurations. Although you can edit the configuration name, server address, and values of some of the configuration parameters, you cannot add or delete a server configuration parameter.

These are four predefined server configurations:

- Real-Time and Batch Basic Match Server
- Real-Time Cleanse Server
- Batch Cleanse Server
- Advanced Batch Match Server

19.3.20 Real-Time and Batch Basic Match Server

Used for basic real-time duplicate prevention and batch data matching and duplicate identification. This configuration requires you to synchronize the Oracle Fusion Trading Community Hub registry data with the third-party data quality engine repository periodically to ensure appropriate matching indexes are updated continuously.

19.3.21 Real-Time Cleanse Server

Used for real-time data cleansing operations that happen at touch point applications, such as Oracle Fusion Sales and Oracle Fusion Customer Center, and therefore do not need synchronization.

19.3.22 Batch Cleanse Server

Used for batch cleansing operations during which records in a batch are sent to the data quality server for cleansing one at a time, and the data quality engine returns the cleansed record to the registry likewise, one at a time, thus completing the loop.

19.3.23 Advanced Batch Match Server

Used for advanced batch matching that finds duplicates in a group of records before uploading them to the Oracle Fusion Trading Community Hub registry. For example, an acquiring company may do an advanced batch match of the legacy data of the acquired company before uploading the data to the registry. In such a case, data is uploaded to the repository of the data quality engine directly for duplication identification and after the duplication identification processing it is imported to the Oracle Fusion Trading Community Hub registry.

19.3.23.1 Oracle Fusion Data Quality Connector Setup: Procedures

Once you complete the Informatica Identity Resolution (IIR) matching and cleansing setups, you must ensure that Oracle Fusion Applications is connected to the data quality engine.

19.3.24 Connecting Oracle Fusion Applications to Data Quality Engine

To connect Oracle Fusion Applications to the data quality engine:

1. Map Oracle Fusion Applications to IIR Matching Server.
    1. Log in to the Functional Setup Manager application as an administrator user.
    2. Under **Assigned Implementation Tasks**, search for `Manage Server Configuration` setup tasks.
    3. Select **Go to Task**. This opens the task-flow page.
    4. Click **Search** to find all existing configurations.

5. In the **Search Results**, select **Realtime and BatchBasic Server**.
6. Select **Actions-Edit**.
7. Enter the **Server Address** and **Server Port** of the IIR Matching Server. The default port is 1666.To know the current port, use grep SSA_ SEPORT=$*APPLICATIONS_BASE*/InformaticaIR/env/isss.
8. Select `Enable Matching`.
9. (Optional) Select **Enable High Availability**.
10. Click **Save and Close**

2. Map Oracle Fusion Applications to IIR Cleansing server.
   1. Log in to the Functional Setup Manager Application as an administrator user.
   2. Under Assigned Implementation Tasks, search for **Manage Server Configuration** setup tasks.
   3. Select **Go to Task**. This opens the task-flow page.
   4. Click **Search** to find all existing configurations.
   5. In the **Search Results**, select **Realtime Cleanse Server**.
   6. Select **Actions - Edit**.

      Note: Repeat the steps to select Batch Cleanse Server from the search results and edit it.

   7. Enter the **Server Address** and Server Port of the IIR Cleansing server. The default port is 1666. To know the current port, use grep SSA_ SEPORT=$*APPLICATIONS_BASE*/InformaticaIR/env/isss.
   8. Select **Enable Cleansing**.
   9. (Optional) Select **Enable High Availability**.
   10. Click **Save and Close**.

      Note: By default, the IIR server instance is the same for both matching and cleansing, but you can configure separate instances if required.

19.3.25 Manage Data Quality Engine Matching Setup

When you use the configurations provided by Oracle Fusion Trading Community Data Quality, matching consists of initial indexing and index synchronization.

19.3.26 Initial Indexing

Perform the following for initial indexing:

1. Log in to the Informatica Identity Resolution (IIR) Host machine.
2. Enter `cd` *APPLICATIONS_BASE*`/InformaticaIR/bin`.
3. Run `setfusionEnv.sh`.
4. Start the Informatica IR Console using `./idsconc -a` option.

5. On the launched console, select **Rulebase Type** as `SSA` and **Alias** as `rtunitrb`.
6. Click **OK**.
7. Select **Yes** for a new Rulebase.
8. In Informatica IR Console, navigate to **System - New - Create a system from SDF**.

   Enter the following information:

   - **System Name**: `FusionDQRealtime`
   - **System Definition File**:`<FULLPATH>/InformaticaIR/ids/FusionDQRealtime.sdf`.
   - **DB Type** : `SSA`
   - **Alias**: `fusion_s01`.
9. Go to **System** and select **System Name** as `FusionDQRealtime`.
10. Click **OK**.
11. Go to **System - Load IDT**.

    Use **Loader Definition** list to load the following ID tables one by one:

    - load_location
    - load_organization
    - load_org_address
    - load_person
    - load_per_address
    - load_per_phone
12. Click **OK** for each ID table.

The IIR load jobs launched from the Informatica IR Console pull the data from the Oracle Fusion Applications database and create keys for them. It then prepares the data in the IIR Server and uses SQL loader to load the data back into the Oracle Fusion Applications database. During this process, if any load job fails and a fix has been applied, you must delete the corresponding .dat file from the *APPLICATIONS_BASE*`/InformaticaIR/ids` directory and then refresh the applicable ID table.

To refresh an ID table:

1. Go to **System - Refresh**.
2. Select **Refresh Selected Objects**.
3. Change the ID table name to refresh.
4. Click **OK**.

19.3.27 Index Synchronization

Once initial indexing is done, you can continue with adding or editing records, however you must synchronize the index as follows:

1. Start the Update Synchronizer on IIR.

> **Note:** See Starting Up and Shutting Down Update Synchronizer.

2. Start the Oracle Fusion Synchronization Oracle Enterprise Scheduler job.

> **Note:** Refer to Running the Schedule Synchronization Process section of the following help topic Synchronizing Trading Community Registry and Data Quality Engine Repository Data: Worked Example.

19.3.28 Starting Up and Shutting Down Update Synchronizer

The Update Synchronizer is a batch job that runs on the IIR Server. The primary function of an Update Synchronizer is to take records in the no source access (NSA) table periodically, create the keys for them, and synchronize these to identity tables (IDTs) and identity indexes (IDXs). The records in NSA are created by the Oracle Fusion Synchronization Oracle Enterprise Scheduler job. Once the Update Synchronizer has completed the job, it would clear the records from NSA.

Starting Up Update Synchronizer: You can start the Update Synchronizer from the Informatica IR console

1. Log in to informatica IR Console.
2. Go to **System** and select **System Name** as `FusionDQRealtime`.
3. Go to **Tools - Synchronizer - Run Synchronizer**.
4. Click **OK**.

   Select the **All** option for **IDT Name** and retain the rest of the defaults.
5. Click **OK**.

Shutting Down Update Synchronizer: Once started, the Update Synchronizer can be left running for the lifecycle of the IIR Server unless there is a need to shut it down.

1. Log in to Informatica IR Console.
2. Double click **Update Synchronizer** under **Launched Jobs** to open the Synchronize window.
3. Select **Yes**. The Synchronizer terminates within 60 seconds.
4. Close the Synchronize window after shutdown.

When there is loss of connectivity with the database, Update Synchronizer stops functioning. You must then restart it.

19.3.28.1 Extending Predefined IIR Matching Configurations: Procedures

This section describes how to extend predefined Informatica Identity Resolution (IIR) matching configurations to overcome the skewness of matching results when fields or attributes of the records being matched are null.

> **Note:** The ability to extend predefined IIR matching configurations is currently not available in Oracle Cloud implementations.

When a record is sent for matching to Informatica Identity Resolution (IIR), the engine returns the final set of matches, by performing a two-step process. The consecutive steps are listed below:

1. Search or Candidate Selection: As part of this step, IIR searches and shortlists candidate records from among the repository records (also called file records).

2. Matching or Scoring: During this step, IIR does a field by field level comparison of the candidate record against the corresponding field in the record being matched (also called the searched record). The individual score of a field is: `weight * score`. The total score is the sum of all individual scores.

> **Note:** For more information on the IIR matching process and predefined matching configurations, refer the IIR vendor documentation in *APPLICATIONS_BASE*/InformaticaIR/pdf directory within the IIR Installation.

Since the total score is the sum of all individual scores, scoring produces skewed results if an attribute or field in either the searched record (the record being matched) or in the candidate record (the file record) is null, because the weight contribution of such a field would be 0.

The following table provides an example of how scoring results can be skewed, if an attribute or field in either the searched record (the record being matched) or in the candidate record (the file record) is null.

Table 19–5 Scoring Results

Searched Record (the record being matched)	File or Candidate Record	Score
Lawrence, 105 E. Graham Ave	Lawrence	(100 * 800)/800 = 100
Lawrence	Lawrence, 105 E. Graham Ave	(100 * 800)/800 = 100

In this example the score is 100 percent even when the address field is missing, because predefined IIR matching configurations ignore weight contributions for any null attribute or field in either the searched record (the record being matched) or in the candidate record (the file record).

To overcome the skewness of matching results when fields or attributes of the records being matched are null, Oracle Fusion Data Quality ships a set of custom Rulebase population, which when used, ensures that the weight for any attribute is 0, only if that attribute is null for the searched record (the record being matched).

The following table provides an example of scoring done using the custom Rulebase population that ensure that the weight for any attribute is 0, only if attribute is null for the searched record (the record being matched).

Table 19–6 Scoring Using the Custom Rulebase Population

Searched Record (the record being matched)	File or Candidate Record	Score (predefined population)	Score (custom popul
Lawrence, 105 E. Graham Ave	Lawrence	(100 * 800)/800 = 100	{(100 * 800)(0 * 200)}/{8
Lawrence	Lawrence, 105 E. Graham Ave	(100 * 800)/800 = 100	(100 * 800)/800 = 100

19.3.29 Extending Predefined IIR Matching Configuration

Use this procedure to extend predefined Informatica Identity Resolution (IIR) matching configurations.

1. Log in to **IIR Admin Console** and select `FusionDQRealtime` system.

2. Stop the **Update Synchronizer** if it is running.
3. Start S**ystem Editor**.
4. Select **Edit** and select **Yes, this time only** or **Yes, do not ask me again for this session** as appropriate.
5. Select **Org-dup** (under Search) in the System Editor.
6. Select the **Score Logic** tab, and on the **Controls** field add `Fusion_` right after the `Purpose=` In other words, after the change, the `Match Purpose` should be `Fusion_Organization`, as opposed to `Organization`.
7. Click **Load**. Close the **Edit System** pop up once you see the message `Job completed`, and repeat Step 5 for all the remaining eight searches from `location_dup` through `person_dup` in the **System Editor**.
8. (Recommended) Restart the IIR to avoid caching and to ensure that the new scoring mechanism is used.

Note: ■The out-of-the-box predefined configurations use the US population: `usa.ycp`. To create other custom populations, select the relevant population out of the 64 populations from the zipped file `OracleCustomPopulations.zip` in the `InformaticaIR/pr/default directory` and customize it.

- To revert to the out of the box predefined population, undo the steps above, by removing `Fusion_` from the `Match Purpose`, from all the nine searches in the **System Editor** and by doing a load using the Step 7.

19.3.30 Managing Data Quality Engine Cleansing Setup

Oracle Fusion Applications Installer installs a demo version of AddressDoctor postal reference data and product license keys that you can use to test address cleansing functionality; however, this demo is restrictive and provides you with a small subset of the complete functionality. For complete functionality, you must request a production license and postal reference data.

19.3.30.1 Using a Demo License and Demo Postal Reference Data

If you are using demo keys and data, no specific setup is required for the address cleansing server. You can quickly verify the setup using *`APPLICATIONS_BASE`*`/InformaticaIR/bin > asmcli -b`. When successful, it launches the Address Standardization Module (ASM) client.

19.3.30.2 Using a Production License and Postal Reference Data

AddressDoctor postal reference data and product license keys are not sold or distributed by Oracle. To acquire a license key and postal reference data, contact Informatica/AddressDoctor by sending an e-mail to OracleAV@informatica.com. The AddressDoctor license key restricts the use of address validation to the purchased countries or territories and represents a twelve (12) month subscription to the postal reference data. Once AddressDoctor receives the e-mail request through OracleAV@informatica.com, an AddressDoctor representative will contact you to define the requirements and complete the transaction. Once finalized, AddressDoctor will provide the license key and download credentials/instructions for accessing the postal reference data. Notification of regular updates to the postal reference data will be provided through e-mail.

Once the production license key and postal reference data are obtained, perform the following:

- *APPLICATIONS_BASE*/InformaticaIR/bin > idsdown
- *APPLICATIONS_BASE*/InformaticaIR/bin > cd *APPLICATIONS_BASE*/InformaticaIR/ssaas/ad5/ad/db.
- *APPLICATIONS_BASE*/InformaticaIR/ssaas/ad5/ad/db > cp mylocation/key. Here, Key is a text file that contains the license provided by AddressDoctor.
- *APPLICATIONS_BASE*/InformaticaIR/ssaas/ad5/ad/db > cp mylocation/[*.MD]. Here, [*.MD] stands for the postal reference data file. AddressDoctor supports 248 countries and each MD file is per country or a group of countries. Each of these files should be copied to this directory.

19.3.31 Managing Data Synchronization

Real-time duplicate prevention during data entry and batch duplicate identification of trading community entities in the Oracle Fusion Trading Community Hub registry and during the data import process require both initial indexing and index synchronization of the integrated third party data quality engine repository with the registry.

Periodic index synchronization of the third party data quality engine repository with the Oracle Fusion Trading Community Hub registry lets you account for the continual updates made to the registry.

Some of the entities that need to be synchronized to the matching engine repository are organization, person, and location. The synchronization should be done when these entities are created or updated.

However, no data synchronization is required for advanced batch match configuration and real-time and batch cleanse operations because of the following reasons:

- Advanced configuration is used only for batch matching such as finding duplicates within a set of interface tables records before running a bulk import process to load the records in the registry.
- Data synchronization is not needed for real-time address cleansing functions as the address is checked against the country specific postal address files and not against the existing address in the registry. Note that the postal reference files need to be updated periodically.
- During the batch cleanse operation, records in a batch are sent to the data quality server for cleansing one at a time and the data quality engine returns the cleansed record to the registry likewise, one at a time, thus completing the loop.

19.3.31.1 Synchronizing Trading Community Registry and Data Quality Engine Repository Data: Example

This example demonstrates the index synchronization of the integrated third party data quality engine repository with the trading community registry. Index synchronization facilitates accounting for the changes made to the registry as part of creating new and updating existing organization, person, and location records since initial indexing. This example focuses on the index synchronization of person party records for the third-party data quality engine Informatica Identity Resolution (IIR).

Index synchronization for the Informatica Identity Resolution data quality engine involves the following tasks:

- Scheduling the synchronization process: Schedule this task to run periodically to account for the continual updates to the Oracle Fusion Trading Community Hub

registry. While running the synchronization process you can select the entities for which you want to synchronize updates and specify the date and time from which to synchronize the updates. A synchronization request performs index synchronization from the last synchronized date and time until the date and time it is submitted.

- Starting Informatica Identity Resolution (IIR) Update Synchronizer: Administrators and integrators typically perform this task. Once started the synchronizer can be left running, for the life cycle of the Informatica Identity Resolution server, unless there is a need to bring it down as part of a maintenance window. However, whenever there is a loss of connectivity with the database Update Synchronizer stops functioning and needs to be manually restarted.

> **Note:** Initial indexing and index synchronization are required only for performing matching operations aimed real-time duplicate prevention and batch duplicate identification. Real-time and batch cleanse operations do not require initial indexing and Index synchronization.

19.3.32 Running the Schedule Synchronization Process

1. Navigate to Setup and Maintenance from the Tools menu.
2. Search for the Manage Data Synchronization task.
3. Click the **Go to Task** icon.
4. Select **Refresh Identity Table Information** option from the Actions menu on the Manage Data Synchronization page.
5. Enable all the relevant identity tables (for this example PER_PRIMARY_IDT, PER_ADDRESS_IDT, PER_PHONE_IDT) by selecting **Enable for Sync**, checkbox.
6. Enter the following Synchronization Options for each identity table:

Table 19–7 Synchronization Options for Each Identity Table

Field	Value
Country	Leave blank when using the predefined system, FusionDQRealtime, for all countries. If using country specific system, enter the country, such as US.
Last Synchronized Time	Select Date and Time: 3/23/11 9:30:15 AM

7. Click **Save**.
8. Click the **Schedule Synchronization Process** button.
9. Click **Advanced**.
10. Select Using a Schedule. From the Frequency drop-down list, select Hourly/Minute and provide a value for the frequency. For example, 5 minutes.

Note: The frequency needs to be determined by the business requirement.

11. From the Calendar, select the End Date.

Note: The end date needs to be determined by the business requirement.

12. Submit the scheduled Sync ESS Job.
13. Click **OK** to return to the Manage Data Synchronization page.
14. Hover on the Process Status field corresponding to each relevant identity table to know the status of the child synchronization request spawned for that table.
15. Click **Save and Close**.

19.3.33 Starting Informatica Identity Resolution Update Synchronizer

1. Log in the Informatica Identity Resolution (IIR) host machine.
2. Enter `cd` *`APPLICATIONS_BASE`*`/InformaticaIR/bin`.
3. Enter `setfusionEnv.sh`
4. Start the IIR console client using the admin option, `./idsconc -a`
5. Select **Run Synchronizer** on the **Tools** menu to launch the synchronizer.
6. In the Update Synchronizer dialog, select **All** as the value for **IDT Name**, use the default values for the rest of the fields, and click **OK**.
7. Verify that the updated and newly created person records are available in IIR, by searching for persons in the Per-dup tab of IIR Web Search Client.
8. Log out of the Informatica Identity Resolution (IIR) user interface.

19.3.33.1 Synchronizing and Optimizing Database Search Indexes for Oracle Fusion CRM Objects

You can synchronize and optimize database search indexes for your Oracle Fusion CRM objects to make your users' searches faster and more efficient. To do this, you can schedule two Enterprise Scheduler Service (ESS) jobs to perform the synchronization and optimization operations.

19.3.34 Synchronizing Database Search Indexes

The Synchronize Database Search Indexes for Oracle Fusion CRM Objects job is a common ESS job that refreshes text indexes for customer, contact, and party name, lead name, and opportunity name columns. It calls the CTX_SYNC_INDEX API to synchronize the text index to process inserts, updates, and deletes to the base table, and ensures that any changes made to these columns are reflected in the database index for the columns..

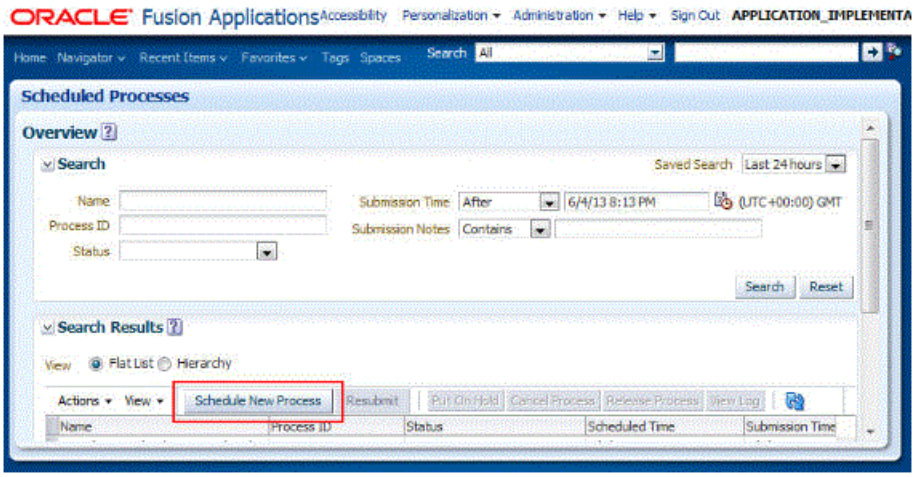
The recommended minimum interval for scheduling the database synchronization job is five minutes; you should allow a longer interval if possible.

You must have the CRM Application Administrator Duty role to see the Synchronize Database Search Indexes for Oracle Fusion CRM Objects job in the job list, and the Run Search Index Scheduler privilege to run the job.

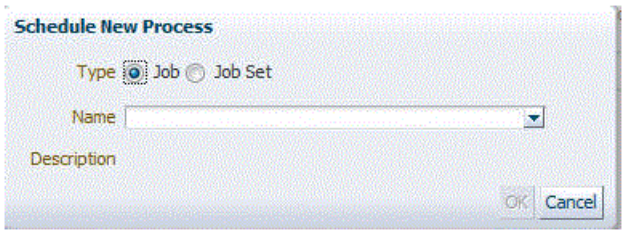
To schedule the database synchronization job:

1. Navigate to the Scheduled Processes page by selecting Scheduled Processes under the Tools menu in the Navigator.

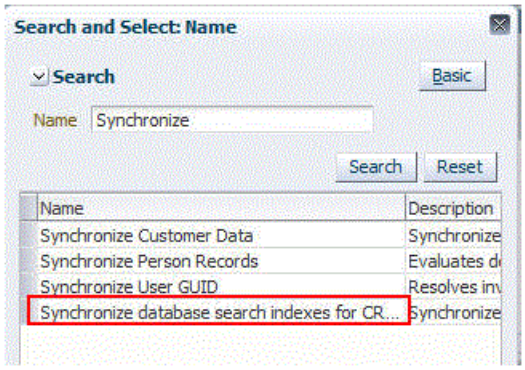
2. Click the **Schedule New Process**.



3. Specify Job in the Type field on the Schedule New Process dialog box if it is not already specified.



4. Search for and select the job type of Synchronize database search indexes for Oracle Fusion CRM objects.



5. Click **OK**.

19.3.35 Optimizing Database Search Indexes

The Optimize Oracle Fusion CRM Search Indexes for Oracle Fusion CRM Objects job is a common ESS job that optimizes the search indexes. It calls the `CTX_OPTIMIZE_INDEX` API to perform the optimization, removing old data and minimizing index fragmentation, which can improve query response time.

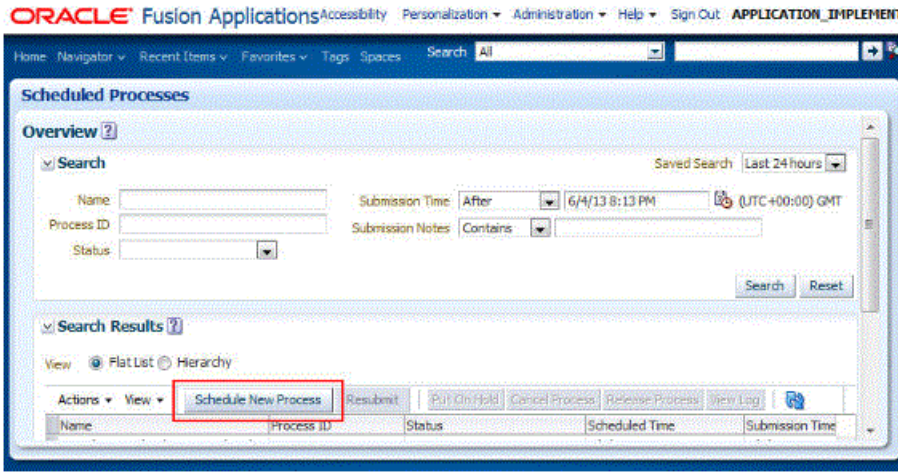
You can run this job on a weekly, monthly, or as-needed basis if search performance is becoming poor. The recommended minimum interval for scheduling the database optimization job is five minutes; you should allow a longer interval if possible.

You must have the CRM Application Administrator Duty role to see the Optimize Oracle Fusion CRM Search Indexes for Oracle Fusion CRM Objects job in the job list, and the Run Search Index Scheduler privilege to run the job.

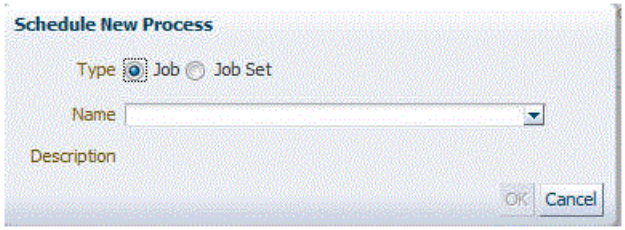
To schedule the database optimization job:

1. Navigate to the Scheduled Processes page by selecting Scheduled Processes under the Tools menu in the Navigator.

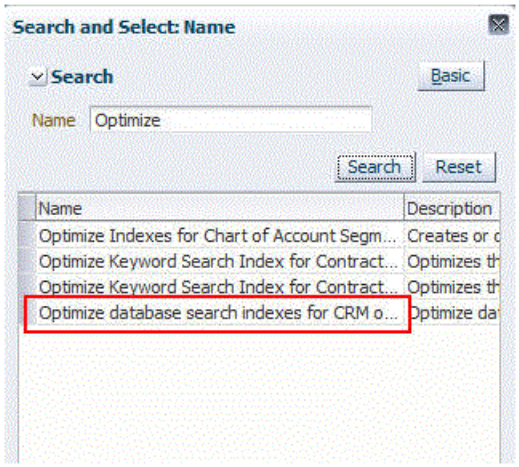
2. Click **Schedule New Processes**.



3. Specify Job in the Type field on the Schedule New Process dialog box if it is not already specified.



4. Search for and select the job type of Optimize database search indexes for Oracle Fusion CRM objects.



5. Click **OK**.

19.3.36 Troubleshooting Oracle Fusion Data Quality Services and IIR Servers

This overview contains various Informatica Identity Resolution (IIR) and Data Quality (DQ) troubleshooting methods, which help an administrator examine the symptoms, identify possible root causes, and take necessary steps to restore their normal functionality.

The log files (ids.dbg) in IIR or iirlog contain useful information that can help in diagnosing the root cause of the functional problems.

The troubleshooting process involves the following scenario checks:

- Matching Service
- Matching Server Administration (including Synchronizer)
- Cleansing Service
- Cleansing Server Administration

The troubleshooting steps for each scenario are grouped, and each group forms a tier. Since different root causes may share the same symptoms, the tiers are arranged in the ascending order of complexity. For effective resolution of the problem, you need to go through these tiers in the same order as presented here. Proceed to the next tier only when you are unable to confirm the root cause in the current tier.

Note: For all the scenario checks, it is assumed that IIR is running with 8 InformaticaIR processes, and that its intra-connectivity is established on the DQ Server Configuration using the correct Host and Port information.

19.3.36.1 Matching Service Troubleshooting: Explained

The Matching Service troubleshooting is spread across six tiers. Each tier indicates certain symptoms, lists possible root causes, contains the log descriptions, and prescribes the recovery procedure. While following the troubleshooting process, ensure that as part of the recovery procedure, you check for UPD locks on the Update Synchronizer before bringing up IIR.

Table 19–8 Tier 1

Stage	Checkpoint
Symptoms	Oracle Fusion `DQ Realtime Match` Web services fail with a message of `ZCQ_DQ_MATCH_SERVER_DISABLED` or Oracle Fusion `DQ Batch Match` jobs fail returning a batch summary status of `ERROR_STATUS_1` thus failing the Match Check Point.
Possible Root Cause	The Match Server Operation is disabled. To confirm, go to the Server Configuration page and check whether the Enabled checkbox is deselected for Realtime and Batch Basic Server.
IIR Logs	NA
Recovery	Select the Enable Matching checkbox for Realtime and Batch Basic Server.

Table 19–9 Tier 2

Stage	Checkpoint
Symptoms	Oracle Fusion `DQ Realtime Match` Web services fail with a message of `ZCQ_DQ_MATCH_SERVER_DISABLED` or Oracle Fusion `DQ Batch Match` jobs fail returning a batch summary status of `ERROR_STATUS_1` thus failing the Match Check Point.
Possible Root Cause	The Match Server Operation is disabled. To confirm, go to the Server Configuration page and check whether the Enabled checkbox is deselected for Realtime and Batch Basic Server.
IIR Logs	NA
Recovery	Select the Enable Matching checkbox for Realtime and Batch Basic Server.

Table 19–10 Tier 4

Stage	Checkpoint
Symptoms	Fusion DQ Realtime Match Services or Fusion DQ Batch Match Jobs fail with an Engine Connection Error `ZCQ_CMN_ENG_CONNECT_ERR`, thus failing the Match Check Point.
Possible Root Cause	Any of the following: ■ IIR was started without setting setfusionEnv.sh or setfusionEnv.csh. This is the most common cause. ■ DB Client on IIR was not set up correctly. For example, tnsnames.ora does not have the entry for the FUSION DB to which IIR should connect. ■ The password for FUSION_DQ has changed or is incorrect.

Table 19–10 (Cont.) Tier 4

Stage	Checkpoint

IIR Logs	`[518135036 ssasrsv 22/ 12] errmsg_put 'SQLConnect: OCIInitialize failed 1804'`
	`[518135036 ssasrsv 22/ 12] errmsg_put 'ssaoci.c 2646 rc 2'`
	`[518135036 ssasrsv 22/ 12] errmsg_put 'ssa_odbc_ connect: cannot connect to Data Source'`
	`[518135036 ssasrsv 22/ 12] errmsg_put 'ssaodbc.c 1436 rc 8 1*100'`
	`[518135036 ssasrsv 22/ 12] errmsg_put 'db_ connect_user: Cannot connect to service 'rws65311' with uid 'fusion_dq''`
	`[518135036 ssasrsv 22/ 12] errmsg_put 'ssaodbc.c 4112 rc 9 108*100'`
	`[518135036 ssasrsv 22/ 12] errmsg_put 'ssadb8_db_ opn failed'`
	`[518135036 ssasrsv 22/ 12] errmsg_put 'ssaodbc.c 4441 rc 10 10809*100'`
	`[518135036 ssasrsv 22/ 12] errmsg_put 'dbops.c 1561 rc 4 1080910*100'`
	`[518135036 ssasrsv 22/ 12] errmsg_put 'dbldr.c 1203 rc 9 108091004*1000'`
	`[518135036 ssasrsv 22/ 12] errmsg_put 'ssarbnl_ rulebase_open: 'odb:0:fusion_dq/@rws65311' db open failed -91004009'`
	`[518135036 ssasrsv 22/ 12] errmsg_put 'ssarbn.c 3026 rc 7 91004009*100'`
	`[518135036 ssasrsv 22/ 12] ssarbn.c(2841) ssarbnl_rulebase_destroy: rbh=0`
	`[518135036 ssasrsv 22/ 12] ssarbn.c(2909) ssarbnl_rulebase_destroy: 'odb:0:fusion_ dq/@rws65311' RULEBASE CLOSE`

Recovery	Follow each recovery instruction and proceed to the next step in the given order only if the current step does not fix the issue. Also, shut down IIR before performing these steps and restart it later as per instructions given for the Matching Setup. **1.** Set the environment variables using `setfusionEnv.sh` or `setfusionEnv.csh`. **2.** Add correct entry to `tnsnames.ora`. **3.** Check if the correct password is used for FUSION_ DQ in `InformaticaIR/ids/ssadb.dic`.

Table 19–11 Tier 5

Stage	Checkpoint
Symptoms	Fusion DQ Realtime Match Services or Fusion DQ Batch Match Jobs fail with an Engine Connection Error `ZCQ_CMN_ ENG_CONNECT_ERR`, thus failing the Match Check Point

Table 19–11 (Cont.) Tier 5

Stage	Checkpoint
Possible Root Cause	Any of the following: ■ IIR was shut down without shutting down the Admin Client (presumably running in a different session) as per the prescribed procedure. The shutdown procedure helps in detecting any active client console. ■ IIR was incorrectly shut down when Update Synchronizer (UPD) was running. It led to a Rule base corruption. ■ The DB crashed or was shut down when IIR was running.

Table 19–11 (Cont.) Tier 5

Stage	Checkpoint
IIR Logs	[518143012 ssasrsv 25/ 12] errmsg_put 'ssadb8_l_ file_add: FileId 3 (inuse) already exists' [518143012 ssasrsv 25/ 12] errmsg_put 'ssaodbc.c 8245 rc 5' [518143012 ssasrsv 25/ 12] errmsg_put 'dbops.c 4363 rc 3 5*100' [518143012 ssasrsv 25/ 12] errmsg_put 'dbldr.c 3912 rc 9 503*1000' [518143012 ssasrsv 25/ 12] errmsg_put 'ssarbnl_ inuse_add: Cannot create RB INUSE table' [518143012 ssasrsv 25/ 12] errmsg_put 'ssarbn.c 2543 rc 2 503009*100' [518143012 ssasrsv 25/ 12] errmsg_put 'IS ANOTHER RULEBASE SERVER RUNNING?' [518143012 ssasrsv 25/ 12] errmsg_put 'Rulebase 'odb:0:fusion_dq/@rws65311' in use by rws65311fwks.us.example.com IP=130.35.116.108 on port=1668, SSA_RB_RESTART_ID=726050355' [518143012 ssasrsv 25/ 12] errmsg_put 'Server started at 'Wed May 18 14:21:31 2011'' [518143012 ssasrsv 25/ 12] errmsg_put 'Rulebase opened at 'Wed May 18 14:23:31 2011'' [518143012 ssasrsv 25/ 12] errmsg_put 'Rulebase opened as 'odb:0:fusion_dq/@rws65311'' [518143012 ssasrsv 25/ 12] errmsg_put 'env has SSA_RB_RESTART_ID=0' [518143012 ssasrsv 25/ 12] errmsg_put 'Owner information: ip=130.35.116.108 pid=1236 host='rws65311fwks.us.example.com' ps='260152864 /scratch/<username>/InformaticaIR/bin/ssasrsv-n166 6-m1668-x1670-H1671-v-1/scratch/<username>/Informa ticaIR/iirlog/idssrsv.'' [518143012 ssasrsv 25/ 12] errmsg_put 'Owner is running' [518143012 ssasrsv 25/ 12] errmsg_put 'Rulebase is locked' [518143012 ssasrsv 25/ 12] errmsg_put 'ssarbnl_ inuse_create: inuse_add failed -50300902' [518143012 ssasrsv 25/ 12] errmsg_put 'ssarbn.c 2583 rc 1' [518143012 ssasrsv 25/ 12] errmsg_put 'ssarbn.c 3031 rc 8 1*100' [518143012 ssasrsv 25/ 12] ssarbn.c(2841) ssarbnl_rulebase_destroy: rbh=0 [518143012 ssasrsv 25/ 12] ssarbn.c(2909) ssarbnl_rulebase_destroy: 'odb:0:fusion_ dq/@rws65311' RULEBASE CLOSE

Table 19–11 (Cont.) Tier 5

Stage	Checkpoint
Recovery	Follow each recovery instruction and proceed to the next step in the given order only if the current step does not fix the issue. Also, shut down IIR before performing these steps and restart it later as per instructions given for the Matching Setup. 1. If the Admin Client is running, end the process or shut it down to unlock. 2. Unlock the Rulebase, using command line as described in Matching Setup. 3. Drop the table IDS_NN_INUSE [where nn represents the Rulebase number] using the command `DROP IDS_00_INUSE`; and remove the "inuse" record from `IDS_FDT_META` using the command `DELETE from IDS_FDT_META where Name = 'IDS_00_INUSE'`. 4. Create the Rulebase and re-index the data afresh as described in Matching Setup. IMPORTANT Option 3 is not a supported workaround. Therefore, if it does not yield results, it is upto the Administrator to use discretion in applying Option 4.

Table 19–12 Tier 6

Stage	Checkpoint
Symptoms	Fusion DQ Realtime Match Services work normally, but Fusion DQ Batch Match Jobs (using Match within Batch) fail, resulting in an error.
Possible Root Cause	A typical case of DB connectivity where locks gets created on certain Rule base tables while Update Synchronizer (UPDSYNC) was still running. As a result, the Rule base is locked and cannot be accessed. The IIR Real time Services uses the Search API (which caches Rule base Information) and Scoring API (used by Match with in Batch), but it fails because it cannot access the Rule base Information.

Table 19–12 (Cont.) Tier 6

Stage	Checkpoint

IIR Logs	// UPDSYNC FAILED DUE TO CONNECTION LOST WITH
	// DB SERVER WHILE IT WAS WRITING. THIS
	CAUSED A LOCK.
	[426200601 updsync 9/ 2] errmsg_put
	'ssaoci_exec: OCIStmtExecute failed -1,
	ORA-03135'
	[426200601 updsync 9/ 2] errmsg_put
	'ssaoci.c 3577 rc 13'
	[426200601 updsync 9/ 2] errmsg_put
	'ssadb8_sql_alloc_next_recid_table: [01]
	SQLExecute ssaodbc.c 15980 failed SQLRET=-1
	SQLSTATE=' ' NATIVE_ERR=0'
	[426200601 updsync 9/ 2] errmsg_put
	'ssadb8_sql_alloc_next_recid_table: [02]
	Reason: [SSAOCI,1] OCIStmtExecute ssaoci.c
	3561 failed 'ORA-03135: connection lost
	contact
	Process ID: 24861
	Session ID: 2108 Serial number: 50953''
	[426200601 updsync 9/ 2] errmsg_put
	'ssadb8_sql_alloc_next_recid_table: [03]
	Reason: [SSAOCI,2] Stmt: 'SELECT /*+ CHOOSE */
	NEXT_RECID FROM IDS_FDT_RECID WHERE TFNO = :x0
	FOR UPDATE ''
	[426200601 updsync 9/ 2] errmsg_put
	'SQLEndTran: rollback failed -1'
	[426200601 updsync 9/ 2] errmsg_put
	'ssaoci.c 3121 rc 3'
	[426200601 updsync 9/ 2] errmsg_put
	'ssadb8_sql_alloc_next_recid_table: Error
	Execute ids_fdt_recid'
	[426200601 updsync 9/ 2] errmsg_put
	'ssaodbc.c 15985 rc 12 1*100'
	[426200601 updsync 9/ 2] errmsg_put
	'ssaodbc.c 16262 rc 2 112*100'
	[426200601 updsync 9/ 2] errmsg_put 'vrec_
	add_sql failed'
	[426200601 updsync 9/ 2] errmsg_put
	'ssaodbc.c 10645 rc 10 11202*100'
	[426200601 updsync 9/ 2] errmsg_put
	'dbops.c 2736 rc 3 1120210*100'
	[426200601 updsync 9/ 2] errmsg_put
	'dbldr.c 2263 rc 9 112021003*1000'
	[426200601 updsync 9/ 2] errmsg_put
	'updsync.c 5971 rc 8 21003009*100'
	[426200601 updsync 9/ 2] errmsg_put
	'updsync.c 6821 rc 24 100300908*100'
	[426200601 updsync 9/ 2] errmsg_put 'Error
	processing txn #20110426200506222280'
	[426200601 updsync 9/ 2] errmsg_put
	'updsync.c 7039 rc 46 30090824*100'
	[426200601 updsync 9/ 2] errmsg_put
	'updsync process_txn failed -9082446'
	[426200601 updsync 9/ 2] errmsg_put
	'updsync.c 10522 rc 26 9082446*100'
	
	// SEARCHES THROUGH SCORING API USED IN BATCH
	// START FAILING, SINCE THE RULEBASE READ
	FAILS
	[427125914 ssasrsv 10/ 10] errmsg_put
	'ssadb_object_status_get: rulebase_read_first
	failed -10104021'

Table 19–12 (Cont.) Tier 6

Stage	Checkpoint
Recovery	Shut down and start IIR after checking UPD locks and unlocking them as per the instructions in Update Synchronizer troubleshooting.

19.3.36.2 IIR Matching Server Administration Troubleshooting: Explained

The Matching Server Administration troubleshooting is spread across four tiers. Each tier indicates certain symptoms, lists possible root causes, contains the log descriptions, and prescribes the recovery procedure. While following the troubleshooting process, ensure that as part of the recovery procedure, you check for UPD locks on the Update Synchronizer before bringing up IIR.

Table 19–13 Tier 1

Stage	Checkpoint
Symptoms	When starting the IIR Admin Console Client, it shows a pop up with a confirmation message "Rulebase doesn't exist. Do you want to create it again". **Note**: This popup also appears when you create a Rulebase for the first time during initial setup. However, it is an indication of problem if it appears while starting IIR Admin Console as part of regular maintenance, after the Rulebase has been created.
Possible Root Cause	Any of the following: ■ IIR was started without setting `setfusionEnv.sh` or `setfusionEnv.csh`. This is the most common cause. ■ DB Client on IIR is not set up correctly. For example, tnsnames.ora doesn't have the entry for the FUSION DB to which IIR should connect. ■ The password for FUSION_DQ has changed or is incorrect.

Table 19–13 (Cont.) Tier 1

Stage	Checkpoint
IIR Logs	`[518135036 ssasrsv 22/ 12] errmsg_put 'SQLConnect: OCIInitialize failed 1804' [518135036 ssasrsv 22/ 12] errmsg_put 'ssaoci.c 2646 rc 2' [518135036 ssasrsv 22/ 12] errmsg_put 'ssa_odbc_ connect: cannot connect to Data Source' [518135036 ssasrsv 22/ 12] errmsg_put 'ssaodbc.c 1436 rc 8 1*100' [518135036 ssasrsv 22/ 12] errmsg_put 'db_ connect_user: Cannot connect to service 'rws65311' with uid 'fusion_dq'' [518135036 ssasrsv 22/ 12] errmsg_put 'ssaodbc.c 4112 rc 9 108*100' [518135036 ssasrsv 22/ 12] errmsg_put 'ssadb8_db_ opn failed' [518135036 ssasrsv 22/ 12] errmsg_put 'ssaodbc.c 4441 rc 10 10809*100' [518135036 ssasrsv 22/ 12] errmsg_put 'dbops.c 1561 rc 4 1080910*100' [518135036 ssasrsv 22/ 12] errmsg_put 'dbldr.c 1203 rc 9 108091004*1000' [518135036 ssasrsv 22/ 12] errmsg_put 'ssarbnl_ rulebase_open: 'odb:0:fusion_dq/@rws65311' db open failed -91004009' [518135036 ssasrsv 22/ 12] errmsg_put 'ssarbn.c 3026 rc 7 91004009*100' [518135036 ssasrsv 22/ 12] ssarbn.c(2841) ssarbnl_rulebase_destroy: rbh=0 [518135036 ssasrsv 22/ 12] ssarbn.c(2909) ssarbnl_rulebase_destroy: 'odb:0:fusion_ dq/@rws65311' RULEBASE CLOSE`
Recovery	Following each recovery instruction and proceed to the next step in the given order only if the current step does not fix the issue. Also, shut down IIR before performing these steps and restart it later as per instructions given for the Matching Setup. **1.** Set the environment variables using `setfusionEnv.sh` or `setfusionEnv.csh`. **2.** Add correct entry to tnsnames.ora. **3.** Check password for `FUSION_DQ` in `InformaticaIR/ids/ssadb.dic` and make sure it is correct.

Table 19–14 Tier 2

Stage	Checkpoint
Symptoms	■ Starting the IIR Admin Console Client fails with a Rulebase Lock Error: "Is another Rulebase Server running?" ■ Starting the HTTP Search Client fails with a Rulebase Lock Error - "Is another Rulebase Server running?"

Table 19–14 (Cont.) Tier 2

Stage	Checkpoint
Possible Root Cause	Any of the following: ■ IIR was shut down without shutting down the Admin Client (presumably running in a different session) as per the prescribed procedure. The shutdown procedure helps in detecting any active client console. ■ IIR was incorrectly shut down when Update Synchronizer (UPD) was running. It led to a Rulebase corruption. ■ The DB crashed or was shut down when IIR was running.

Table 19–14 (Cont.) Tier 2

Stage	Checkpoint
IIR Logs	[518143012 ssasrsv 25/ 12] errmsg_put 'ssadb8_l_ file_add: FileId 3 (inuse) already exists' [518143012 ssasrsv 25/ 12] errmsg_put 'ssaodbc.c 8245 rc 5' [518143012 ssasrsv 25/ 12] errmsg_put 'dbops.c 4363 rc 3 5*100' [518143012 ssasrsv 25/ 12] errmsg_put 'dbldr.c 3912 rc 9 503*1000' [518143012 ssasrsv 25/ 12] errmsg_put 'ssarbnl_ inuse_add: Cannot create RB INUSE table' [518143012 ssasrsv 25/ 12] errmsg_put 'ssarbn.c 2543 rc 2 503009*100' [518143012 ssasrsv 25/ 12] errmsg_put 'IS ANOTHER RULEBASE SERVER RUNNING?' [518143012 ssasrsv 25/ 12] errmsg_put 'Rulebase 'odb:0:fusion_dq/@rws65311' in use by rws65311fwks.us.example.com IP=130.35.116.108 on port=1668, SSA_RB_RESTART_ID=726050355' [518143012 ssasrsv 25/ 12] errmsg_put 'Server started at 'Wed May 18 14:21:31 2011'' [518143012 ssasrsv 25/ 12] errmsg_put 'Rulebase opened at 'Wed May 18 14:23:31 2011'' [518143012 ssasrsv 25/ 12] errmsg_put 'Rulebase opened as 'odb:0:fusion_dq/@rws65311'' [518143012 ssasrsv 25/ 12] errmsg_put 'env has SSA_RB_RESTART_ID=0' [518143012 ssasrsv 25/ 12] errmsg_put 'Owner information: ip=130.35.116.108 pid=1236 host='rws65311fwks.us.example.com' ps='260152864 /scratch/<username>/InformaticaIR/bin/ssasrsv-n166 6-m1668-x1670-H1671-v-1/scratch/<username>/Informa ticaIR/iirlog/idssrsv.'' [518143012 ssasrsv 25/ 12] errmsg_put 'Owner is running' [518143012 ssasrsv 25/ 12] errmsg_put 'Rulebase is locked' [518143012 ssasrsv 25/ 12] errmsg_put 'ssarbnl_ inuse_create: inuse_add failed -50300902' [518143012 ssasrsv 25/ 12] errmsg_put 'ssarbn.c 2583 rc 1' [518143012 ssasrsv 25/ 12] errmsg_put 'ssarbn.c 3031 rc 8 1*100' [518143012 ssasrsv 25/ 12] ssarbn.c(2841) ssarbnl_rulebase_destroy: rbh=0 [518143012 ssasrsv 25/ 12] ssarbn.c(2909) ssarbnl_rulebase_destroy: 'odb:0:fusion_ dq/@rws65311' RULEBASE CLOSE

Table 19–14 (Cont.) Tier 2

Stage	Checkpoint
Recovery	Follow each recovery instruction and proceed to the next step in the given order only if the current step does not fix the issue. Also, shut down IIR before performing these steps and restart it later as per instructions given for the Matching Setup. **1.** If the Admin Client is running, end the process or shut it down to unlock. **2.** Unlock the Rulebase, using command line as described in Matching Setup. **3.** Drop the table IDS_NN_INUSE [where nn represents the Rulebase number] using the command `DROP IDS_00_INUSE`; and remove the "inuse" record from `IDS_FDT_META` using the command `DELETE from IDS_FDT_META where Name = 'IDS_00_INUSE'`. **4.** Create the Rulebase and re-index the data afresh as described in Matching Setup. IMPORTANT Option 3 is not a supported workaround. Therefore, if it does not yield results, it is up to the Administrator to use discretion in applying Option 4.

Table 19–15 Tier 3

Stage	Checkpoint
Symptoms	Starting the IIR Admin Console fails with an error: "connection lost to peer".
Possible Root Cause	DB connectivity issues caused by either DB shut down, or DB crash or network connectivity issues, when IIR was running.

IIR Logs	`[517153446 ssasrsv 0/ 5] 31344/xm> server started: Tue May 17 15:34:46 2011`
	`[517153447 ssacssv 4/ 5] errmsg_put 'send(h=2, os=9) failed: Reason: Broken pipe'`
	`[517153447 ssacssv 4/ 5] errmsg_put 'socket.c 1096 rc 11'`
	`[517153447 ssacssv 4/ 5] errmsg_put 'socket.c 2559 rc 4 11*100'`
	`[517153447 ssacssv 4/ 5] errmsg_put 'ssarbc1.c 693 rc 3 1104*100'`
	`[517153447 ssacssv 4/ 5] errmsg_put 'cssys.c 2185 rc 3 502020401*100'`
	`[517153447 ssacssv 4/ 5] errmsg_put 'ssacssi.c 2125 rc 1 202040103*100'`
	`[517153448 ssacssv 4/ 5] errmsg_put 'send(h=2, os=9) failed: Reason: Broken pipe'`
	`[517153448 ssacssv 4/ 5] errmsg_put 'socket.c 1096 rc 11'`
	`[517153448 ssacssv 4/ 5] errmsg_put 'socket.c 2559 rc 4 11*100'`
	`[517153448 ssacssv 4/ 5] errmsg_put 'ssarbc1.c 7725 rc 3 1104*100'`

Table 19–15 (Cont.) Tier 3

Stage	Checkpoint
Recovery	Close the Admin Console and restart IIR as per the Server Administration instructions.

19.3.36.3 Update Synchronizer Troubleshooting: Explained

The root cause of Update Synchronizer (UPD) locks is either an incorrect shut down where the Search Server was shut down while UPD was still running followed by ending the UPD process or an abrupt loss in DB connectivity when UPD was processing rows to be synchronized. To restore normal functioning of IIR, you need to delete the UPD locks.

To detect UPD locks, if there are any, run the command `./lockmgr list uq -rssa:<Rulebase alias> -h<IIR RB Host>:<IIR RB Port> -l` in *APPLICATIONS_BASE*`/InformaticaIR/bin`. For example, if you run the following command:

```
./lockmgr list uq -rssa:rtunitrb -haufsn4ayf04:1668 -l
```

it returns the following details:

```
sorted locks:
uq: updsync:1302896463:6826
  obj: idtsyncsystem
    id: system=fusiondqrealtime
      type: w
      lock: ip=144.23.252.42 pid=31928
host='aufsn4agf04.oracleoutsourcing.com' ps='80154501
/u01/APPLTOP/fusionapps/InformaticaIR/bin/updsync-t60-m100-haufsn4agf04.oracle
outsourcing.com:1668-rssa:rtunitrb-vus-pf'
```

> **Note:** UPD Locks should be deleted only when you find them, even when UPD has been shut down and you do not have any `UPDSYNC` process running.

To delete the locks, run the command `./lockmgr del uq -rssa:<Rulebase alias> -h<IIR RB Host>:<IIR RB Port>` in *APPLICATIONS_BASE*`/InformaticaIR/bin`. For example,

```
./lockmgr del  updsync:1302896463:6826 -rssa:rtunitrb -haufsn4ayf04:1668
```

19.3.36.4 Cleansing Service Troubleshooting: Explained

Table 19–16 Tier 1

Stage	Checkpoint
Symptoms	Fusion DQ Realtime Cleanse Web Services fail with a message of `ZCQ_CLEANSE_SERVER_DISABLED` or Fusion DQ Batch Match Jobs fail returning a Batch Summary Status of `ERROR_STATUS_1` thus failing the Cleanse Check Point.

Table 19–16 (Cont.) Tier 1

Stage	Checkpoint
Possible Root Cause	The Cleanse Server Operation is disabled. To confirm, go to the Edit Server Configuration page and check whether the **Enable Cleansing** checkbox is deselected for Realtime Cleanse Server and Batch Cleanse Server.
IIR Logs	NA
Recovery	Select the **Enable Cleansing** checkbox for Realtime Cleanse and Batch Cleanse Servers.

Table 19–17 Tier 2

Stage	Checkpoint
Symptoms	Fusion DQ Cleansing Services or Fusion DQ Batch Cleanse Jobs fail with an Engine Connection Error `ZCQ_CMN_ENG_CONNECT_ERR`, thus failing the Cleansing Check Point.
Possible Root Cause	IIR connection setup is missing or incorrect in the cleansing configuration. Using the Manage Server Configuration FSM task, check the Server Host and Port information for the cleansing servers.
IIR Logs	NA
Recovery	Setup IIR Host and Port in Cleansing Configuration page

Table 19–18 Tier 3

Stage	Checkpoint
Symptoms	Fusion DQ Cleansing Services or Fusion DQ Batch Cleanse Jobs fail with an Engine Connection Error `ZCQ_CMN_ENG_CONNECT_ERR`, thus failing the Cleansing Check Point.
Possible Root Cause	ASM Key stored in `InformaticaIR/ssaas/ad5/ad/db` has expired.

IIR Logs	`[523163408 ssasrsv 14/ 12] errmsg_put 'as_init: Object init failed: (-1601) Critical Error: The engine usage period has expired'`
	`[523163408 ssasrsv 14/ 12] errmsg_put 'ssaas5.c 1338 rc 4'`
	`[523163408 ssasrsv 14/ 12] errmsg_put 'ssaas5.c 1390 rc 1 4*100'`
	`[523163408 ssasrsv 14/ 12] errmsg_put 'ssaas5.c 3097 rc 2 401*100'`
	`[523163408 ssasrsv 14/ 12] errmsg_put 'ssasesi_addr_init: Error -40102 initializing Addr Std module'`
	`[523163408 ssasrsv 14/ 12] errmsg_put 'ssasesi.c 13477 rc 9 40102*100'`

Recovery	Get the correct ASM key from Address Doctor and replace the existing key in the file called key in `InformaticaIR/ssaas/ad5/ad/db`. Subsequently, restart the IIR Server.

Table 19–19 Tier 4

Stage	Checkpoint
Symptoms	Fusion DQ Cleansing Services or Fusion DQ Batch Cleanse Jobs fail with an Engine Connection Error `ZCQ_CMN_ENG_CONNECT_ERR`, thus failing the Cleansing Check Point.
Possible Root Cause	ASM Key stored in `InformaticaIR/ssaas/ad5/ad/db` is either incorrect or corrupt.

IIR Logs	`// junk or error ASM key error`
	`[523163604 ssasrsv 14/ 12] errmsg_put 'as_init: Object init failed: (-1600) Critical Error: No valid unlock code was given'`
	`[523163604 ssasrsv 14/ 12] errmsg_put 'ssaas5.c 1338 rc 4'`
	`[523163604 ssasrsv 14/ 12] errmsg_put 'ssaas5.c 1390 rc 1 4*100'`
	`[523163605 ssasrsv 14/ 12] errmsg_put 'ssaas5.c 3097 rc 2 401*100'`
	`[523163605 ssasrsv 14/ 12] errmsg_put 'ssasesi_addr_init: Error -40102 initializing Addr Std module'`
	`[523163605 ssasrsv 14/ 12] errmsg_put 'ssasesi.c 13477 rc 9 40102*100'`

Recovery	Get the correct ASM key from Address Doctor and replace the existing key in the file called key in `InformaticaIR/ssaas/ad5/ad/db`. Subsequently, restart the IIR Server.

Table 19–20 Tier 5

Stage	Checkpoint
Symptoms	Fusion DQ Cleansing Services or Fusion DQ Batch Cleanse Jobs fail with an Engine Connection Error `ZCQ_CMN_ENG_CONNECT_ERR`, thus failing the Cleansing Check Point.
Possible Root Cause	ASM Key stored in `InformaticaIR/ssaas/ad5/ad/db` does not exist.

Table 19–20 (Cont.) Tier 5

Stage	Checkpoint

IIR Logs	`[523163811 ssasrsv 14/ 12] errmsg_put 'fopen('/slot/ems4517/appmgr/InformaticaIR/ssaas/ad5/ad/db/key', 'r') failed 16: No such file or directory'`
	`[523163811 ssasrsv 14/ 12] errmsg_put 'fopen.c 985 rc 19'`
	`[523163811 ssasrsv 14/ 12] errmsg_put 'fopen.c 1070 rc 3 19*100'`
	`[523163811 ssasrsv 14/ 12] errmsg_put 'fopen.c 1141 rc 2'`
	`[523163811 ssasrsv 14/ 12] errmsg_put 'ssasesil_addr_get_key_and_workdir: open Addr Std license key file '/slot/ems4517/appmgr/InformaticaIR/ssaas/ad5/ad/db/key' failed'`
	`[523163811 ssasrsv 14/ 12] errmsg_put 'ssasesi.c 13293 rc 6'`
	`[523163811 ssasrsv 14/ 12] errmsg_put 'ssasesi.c 13443 rc 6 6*100'`

Recovery	Get the correct ASM key from Address Doctor and create a file called key in `InformaticaIR/ssaas/ad5/ad/db`. Subsequently, restart the IIR Server.

19.3.36.5 IIR Cleansing Server Administration Troubleshooting: Explained

The Cleansing Server Administration troubleshooting process indicates certain symptoms, lists possible root causes, contains the log descriptions, and prescribes the recovery procedure.

Table 19–21

Stage	Checkpoint
Symptoms	The IIR Cleansing Console does not respond to the start command `asmcli -b` run from `InformaticaIR/bin`, thus failing the Cleansing Setup Checkpoint.
Possible Root Cause	ASM Key stored in `InformaticaIR/ssaas/ad5/ad/db` has either expired, is either incorrect or corrupt, or does not exist.

Table 19–21 (Cont.)

Stage	Checkpoint
IIR Logs	`[523163408 ssasrsv 14/ 12] errmsg_put 'as_ init: Object init failed: (-1601) Critical Error: The engine usage period has expired' [523163408 ssasrsv 14/ 12] errmsg_put 'ssaas5.c 1338 rc 4' [523163408 ssasrsv 14/ 12] errmsg_put 'ssaas5.c 1390 rc 1 4*100' [523163408 ssasrsv 14/ 12] errmsg_put 'ssaas5.c 3097 rc 2 401*100' [523163408 ssasrsv 14/ 12] errmsg_put 'ssasesi_addr_init: Error -40102 initializing Addr Std module' [523163408 ssasrsv 14/ 12] errmsg_put 'ssasesi.c 13477 rc 9 40102*100'`  `[523163604 ssasrsv 14/ 12] errmsg_put 'as_ init: Object init failed: (-1600) Critical Error: No valid unlock code was given' [523163604 ssasrsv 14/ 12] errmsg_put 'ssaas5.c 1338 rc 4' [523163604 ssasrsv 14/ 12] errmsg_put 'ssaas5.c 1390 rc 1 4*100' [523163605 ssasrsv 14/ 12] errmsg_put 'ssaas5.c 3097 rc 2 401*100' [523163605 ssasrsv 14/ 12] errmsg_put 'ssasesi_addr_init: Error -40102 initializing Addr Std module' [523163605 ssasrsv 14/ 12] errmsg_put 'ssasesi.c 13477 rc 9 40102*100'`
Recovery	Get the correct ASM key from Address Doctor and replace the existing key in the file called key in `InformaticaIR/ssaas/ad5/ad/db`. Subsequently, restart the IIR Server.

19.4 Setting Up Sales Prediction Engine

To run the Oracle Fusion Sales Prediction Engine in Oracle Fusion Customer Relationship Management (Oracle Fusion CRM), perform the following post-installation tasks if you deployed Oracle Business Intelligence Applications and have created the Oracle Business Analytics Warehouse. For information on deploying and setting up Oracle Business Intelligence Applications, see the *Oracle Business Intelligence Applications Installation Guide*.

However, if you deployed only Oracle Transactional Business Intelligence, you need not perform these steps to run the Oracle Fusion Sales Prediction Engine.

19.4.1 Creating Data Warehouse Objects

You can create the Data Warehouse objects using the Sales Predictor Repository Creation Utility (RCU). To run the Sales Predictor RCU, ensure that the Oracle Business Intelligence Application (OBIA) Data Warehouse database and the related schema including database objects such as tables, are available. The Sales Predictor

RCU creates Sales Predictor related Data Warehouse database objects such as Oracle Data Mining tables, views, packages, Oracle Real-time Decisions (RTD) Inline Service Processing tables, and the purge package in the existing OBIA schema.

Initiate the Sales Predictor RCU following these instructions:

1. Access the `rcuBIZSPApps.zip` file from the following location, and extract its contents to a local directory.
   - In Windows NT, the location is *`REPOSITORY_LOCATION`*`\installers\crm_rcu\windows\rcuBIZSPApps.zip`.
   - In Linux, the location is *`REPOSITORY_LOCATION`*`/installers/crm_rcu/linux/rcuBIZSPApps.zip`.
2. Run the following command pointing to the `BIN` folder within the local directory:
   - In Windows NT, use `rcu -variables BI_SCHEMA_NAME=<OBIA Schema name>`
   - In Linux, use `./rcu -variables BI_SCHEMA_NAME=<OBIA Schema name>`

   Note: <OBIA Schema name> refers to the name of the OBIA schema that is used, and is an input parameter for the Sales Predictor RCU.

   The Sales Predictor RCU wizard appears.
3. On the Welcome page, click **Next** and on the Create Repository page, ensure that the default option **Create** is selected and click **Next**.
4. On the Database Connection Details page, provide the following information and click **Next**.
   - Host Name: Name of the server where the database is located.
   - Port: The database port number.
   - Service name: The service name of the database.
   - Username: SYS - It is the user name associated with an administrative role.
   - Password: Password used in combination with the user name to access the database.
   - Role: SYSDBA - It is the role with administrative access rights.

   This information is processed through a prerequisite check.
5. On the confirmation dialog box, click **OK**.
6. On the Select Components page, select the Oracle Application Components, and click **Next**.
7. On the confirmation dialog box, click **OK**.
8. On the Schema Passwords page, ensure that the **Use same passwords for all schemas** option is selected. Selecting this option provides the password used with the existing OBIA Schema Name.
9. Enter the password again to confirm it, and click **Next**.
10. On the Map Tablespaces page, click **Next** and on the confirmation box that subsequently appears, click **OK**.
11. On the Summary page, review the database information provided until this point. If necessary, click **Back** to change details in the previous pages.

12. Click **Create** to create the Data Warehouse objects. The Completion Summary page confirms the successful creation of the objects.

19.4.2 Creating Data Warehouse Data Source in Oracle Real-Time Decisions WebLogic Server

The Data Warehouse requires a Java Naming and Directory Interface (JNDI) data source connection named DWDS that points to the Online Analytical Processing (OLAP) database residing on Oracle BI server. To create the data source using the Oracle Real-Time Decisions WebLogic Server console, follow these instructions.

1. In the WebLogic Server console, open **Services - JDBC - Data Sources** and click **New**.
2. On the JDBC Data Source Properties page, provide the following details and click **Next**.
   - Name: Fusion_OLAP_DS
   - JNDI Name: DWDS
   - Database Type: Oracle
   - Database Driver: Oracle Driver (Thin) for Instance connections
3. On the Transaction Options page, ensure that the default property **Supports Global Transactions** is selected, and click **Next**.
4. On the Connection Properties page, provide the following values, and click **Next**.
   - Database Name: The Unique System ID (SID) of the database
   - Host Name: The name of the computer that hosts the database
   - Port: The port number of the database
   - Database User Name: User credential to access the database
   - Password: The password used in combination with the Database User Name to access the database
5. On the Test Database Connections page, review the details provided until this point, test the connectivity to the database, and click **Next**.
6. Select the **Oracle BI Server** where you want to make the data source available, and click **Finish**.

19.4.3 Pointing Oracle Real-Time Decisions to the Data Warehouse

The Sales Predictor Inline Service within Oracle Real-Time Decisions uses the profile option to point to the Data Warehouse tables.

You can point Oracle Real-Time Decisions to the Data Warehouse in one of the following ways:

- Restart the Oracle Real-Time Decisions application server. The Sales Predictor Inline Service is reloaded and points to the Data Warehouse.
- Manually redeploy the Sales Predictor Inline Service if restarting the Oracle Real-Time Decisions application server does not work. Before you manually redeploy, ensure that the following prerequisites are met:
  - You have roles allowing access to deploy the Sales Predictor Inline Service.

- Java Development Kit (JDK) 1.6 or higher version is available and running on the same server.
- You must have access to the command line tool zip file `rtd-deploytool-11.1.1.zip`. The zip file resides within the Oracle Real-Time Decisions client zip file (`rtd_client_11.1.1.3.0.zip`), which is available in the *`APPLICATIONS_BASE`*`/fusionapps/bi/clients/rtd` directory.

To manually redeploy the Sales Predictor Inline Service, follow these instructions:

1. Extract the contents of the file `rtd_client_11.1.1.3.0.zip` to a local directory.
2. In the local directory, go to the folder `./client/CommandLineDeploy`, locate `rtd-deploytool-11.1.1.zip` and extract its contents to a folder.
3. In that folder, locate `./OracleBI/RTD/deploytool` folder and within that folder, open a command prompt terminal.

> **Note:** Ensure that the JDK classpath is set for the command prompt terminal.

4. Run the command: `java -jar deploytool.jar -deploy -server <Server Host> -port <Port> -terminateSessions true <Full path of Directory/ Zip File>.`
5. When prompted, provide the user name and password to connect to the RTD server.

The message **Deploymentstateid: id. Deployed SPE_ILS.zip to server port in state: Development** appears indicating completeness of deployment of the Sales Predictor Inline Service.

19.5 Setting Up Implicit Personalization Behavior

This topic covers the post-deployment activities required for Oracle Fusion CRM applications that support implicit personalization behavior.

Performing these activities fixes the inconsistent implicit personalization behavior between sessions in the following Oracle Fusion CRM applications:

- Oracle Fusion CRM Common
- Oracle Fusion Territory Management
- Oracle Fusion Customer Center
- Oracle Fusion Marketing
- Oracle Fusion Order Capture Common Components
- Oracle Fusion Sales

19.5.1 Post-Deployment Activities

Make the following changes to the `adf-config.xml` file as a post-deployment activity.

> **Note:** These steps are applicable only for the Oracle Fusion CRM applications where implicit personalization behavior is supported.

1. Shut down the domain where the application is deployed.
2. Search for `adf-config.xml` file. For example, for Sales application, this file is typically located at `Sales <deploy directory>/SalesApp/V2.0/app/SalesApp/adf/META-INF/adf-config.xml`
3. Back up `adf-config.xml` file.
4. Open `adf-config.xml` file in a text editor and comment out all occurrences of the tag `<adf-faces-config>` under the root node `<adf-config>. . .</adf-config>`. For example:

```
<!-- adf-faces-config xmlns="http://xmlns.example.com/adf/faces/config">. . .
</adf-faces-config -->
```

5. Add the following after the commented section.

```
<adf-faces-config xmlns="http://xmlns.example.com/adf/faces/config">

        <persistent-change-manager>

<persistent-change-manager-class>oracle.adf.view.rich.change.MDSDocumentChangeM
anager</persistent-change-manager-class>

        </persistent-change-manager>

        <taglib-config>
                        <taglib uri="http://xmlns.example.com/adf/pageeditor">
                                <tag name="layoutCustomizable">
                                        <!-- Added to pass JAudit-->
                                        <attribute name="layout">

<persist-changes>true</persist-changes>
                                        </attribute>
                                </tag>
                        </taglib>

                <taglib uri="http://xmlns.example.com/adf/faces/customizable">
                        <tag name="showDetailFrame">
                                <persist-operations>all</persist-operations>
                                <!-- Added to pass JAudit-->
                                <attribute name="disclosed">
                                       <persist-changes>true</persist-changes>
                                </attribute>
                                <attribute name="height">
                                       <persist-changes>true</persist-changes>
                                </attribute>
                        </tag>

                        <!-- Added to pass JAudit-->
                        <tag name="portlet">
                                <attribute name="disclosed">
                                        <persist-changes>true</persist-changes>
                                </attribute>
                                <attribute name="height">
                                        <persist-changes>true</persist-changes>
                                </attribute>
                        </tag>
                </taglib>


                <taglib uri="http://xmlns.example.com/adf/faces/rich">
```

```
                        <tag name="column">
                                <persist-operations>all</persist-operations>
                                <attribute name="displayIndex">
                                        <persist-changes>true</persist-changes>
                                </attribute>
                                <attribute name="visible">
                                        <persist-changes>true</persist-changes>
                                </attribute>

                                <attribute name="width">
                                        <persist-changes>true</persist-changes>
                                </attribute>
                        </tag>
                </taglib>
        </taglib-config>
</adf-faces-config>
```

6. Specifically for Customer Center application, and as an additional step, locate these lines under the `<mds:cust-config>` section:

```
<mds:match path="/oracle/apps/">
        <mds:customization-class
name="oracle.apps.fnd.applcore.customization.ProductFamilyCC"/>
        <mds:customization-class
name="oracle.apps.fnd.applcore.customization.SiteCC"/>
</mds:match>
```

   When you comment the lines, they appear as:

```
<!--mds:match path="/oracle/apps/">
        <mds:customization-class
name="oracle.apps.fnd.applcore.customization.ProductFamilyCC"/>
        <mds:customization-class
name="oracle.apps.fnd.applcore.customization.SiteCC"/>
</mds:match>
```

7. Save and close the file.
8. Start up the domain that hosts the Oracle Fusion CRM application.

19.6 What To Do Next

If you have installed the Oracle Fusion Financials product offering, go to Chapter 20. Otherwise, go to the chapter that corresponds to the product offering that is installed.

20

Completing Oracle Fusion Financials Post-Installation Tasks

This chapter describes the Oracle Fusion Financials post-installation tasks you should review and complete before you can start working with your Oracle Fusion Applications Oracle Fusion Financials implementation.

This chapter contains the following sections:

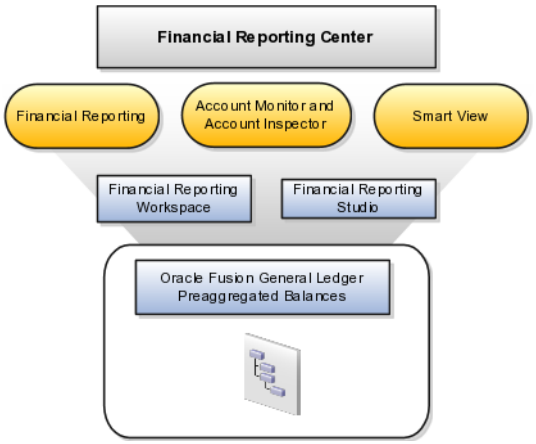
20.1 Setting Up the Financial Reporting Center

The Oracle Fusion Financial Reporting Center provides functionality for reporting on Oracle Fusion General Ledger balances. It provides secure, self-service access to reports that use real time account information.

You can design traditional financial report formats such as balance sheets, profit and loss statements, and cash flow reports. You can also design nontraditional formats for financial or analytic data that include text and graphics.

The following figure shows the main components in the Financial Reporting Center: Financial Reporting, Account Monitor, Account Inspector, Smart View, Financial Reporting Workspace, and Financial Reporting Studio. These components use the Oracle Fusion General Ledger preaggregated balances as the staring data.

Figure 20–1 Financial Reporting Center



20.1.1 Components

Financial Reporting Center is comprised of numerous components:

- **Financial Reporting**: Financial users and analysts access live reports and books or published snapshot reports and books from previously scheduled batches in a variety of formats. Other functionality includes:
  - Refreshing report data using runtime points of view or parameters
  - Drill through capability from parents to other parents
  - Drill down to detail balances, journal lines, and subledger transactions.
- **Oracle Hyperion Smart View**: Financial analysts view, import, manipulate, distribute, and share data from your Oracle Fusion General Ledger balances in Microsoft Excel.
- **Account Monitor and Account Inspector**: Financial analysts monitor and track key account balances in real time at every level of your dimensions and hierarchies. These tools provide multidimensional account analysis and drill down capability.
- **Workspace**: Reporting administrators create, open, save, and delete folders and store report objects, reports, and snapshot reports.
- **Oracle Hyperion Financial Reporting Studio**: Report authors use an object-oriented graphical report layout with report objects, such as text boxes, grids, images, and charts, to design reports.

20.1.2 Setting Up Your Financial Reporting Center: Critical Choices

Oracle Fusion Financial Reporting Center is a powerful tool for accessing, designing, and presenting financial reports and analytic data. The critical choices required to configure and install the components in Financial Reporting Center consist of:

- Configuring Financial Reporting Center
- Installing and configuring Financial Reporting Studio, performed by your end users.
- Installing Smart View, performed by your end user.
- Configuring Workspace Database Connection, performed by your administrator.

- Configuring Oracle Fusion Transactional BI Dimensions

20.1.3 Configuring Financial Reporting Center

You have access to the reports through the folder structure in the Financial Reporting Center and Workspace installed with Oracle Fusion Financial Applications. Your Oracle Fusion Business Intelligence (BI) administrator defines the folder structure in Workspace considering your company's security requirements for folders and reports, as well as report distribution requirements for financial reporting batches. Security can be set on folders and reports from Workspace. You are granted access to the folders and reports you want to view by your BI administrator.

20.1.4 Installing and Configuring Financial Reporting Studio

Oracle Hyperion Financial Reporting Studio is client-based software. If you access Oracle Fusion Applications from Oracle Cloud, you connect to the Financial Reporting Studio through a Windows Remote Desktop Connection.

Otherwise, report authors download the installation files for Financial Reporting Studio from Workspace by clicking **Navigator > Financial Reporting Center > Open Workspace for Financial Reporting**. Once Workspace is launched, click **Tools > Install > Financial Reporting Studio**. After performing the prerequisites and completing the installation, launch the Financial Reporting Studio. Provide your user ID, password, and the Server URL. Derive the Server URL information by following the steps:

1. Open **Navigator > Financial Reporting Center > Open Workspace for Financial Reporting**.
2. Edit the Workspace URL by removing `workspace/index.jsp`.

   Following are two examples of Server URLs:

   - If the Workspace URL is `https://example.com/workspace/index.jsp`, the Server URL is `https://example.com`.
   - If the Workspace URL is `https://example.com:10622/workspace/index.jsp`, the Server URL is `https://example.com:10622`.
3. Copy the modified URL to the Server URL field.

Note: For end users installing the Oracle Fusion Financials Reporting Studio, the installer launches a separate console window that continues to run for a brief time after the installation completes the setup tasks. The process is normal, expected, and applies to Oracle Hyperion Reporting Studio installations in both the Oracle Fusion Applications and Enterprise Performance Manager modes.

Wait for the console window to close, which happens automatically before clicking **Finish** on the Financial Reporting Studio Installation dialog box. If you click **Finish** before the console window closes, the Financial Reporting Studio installation may not fully complete.

Note: You must save a new report before attempting to preview it with Web Preview.

Prerequisites needed for installing the Financial Reporting Studio are:

- Financial Reporting Studio Client Certifications
- Microsoft Office installed on your end-users computers.

> **Note:** For more information, see:
>
> - Oracle Enterprise Performance Management System Installation and Configuration Guide
> - Oracle Hyperion Enterprise Performance Management System EPM System Standard Deployment Guide

20.1.5 Installing Smart View

Smart View is a Microsoft Excel add-in that must be loaded to each client. To download the installation files from Workspace click **Navigator > Financial Reporting Center > Open Workspace for Financial Reporting**. Once the Workspace is launched, click **Tools > Install > Smart View**.

> **Note:** Since Smart View is an add-in to Microsoft Office products, you can install Smart View only on a Windows operating system.

Once Smart View is installed, it must be configured to connect to Oracle Fusion Applications. This is done using the Smart View Shared Connections URL. You can derive the Shared Connections URL by following the steps below:

1. Open Workspace for Financial Reporting from the Financial Reporting Center task panel.
2. Edit the Workspace URL, for example, if the Workspace URL is `https://example.com/workspace/index.jsp`. Remove `index.jsp` and add `SmartViewProviders` at the end of the URL.

   > **Note:** This is another example for a Cloud based environment: If the Workspace URL is `https://example.com:10622/workspace/index.jsp`, the Shared Connections URL is `https://example.com:10622/workspace/SmartViewProviders`.

3. Copy the URL.
4. Launch Excel.
5. Navigate to the **Smart View menu > Options > Advanced**.
6. Paste the URL in the Shared Connections URL field.
7. Click **OK**.

For more information on configuring Smart View client for users, see *Oracle Hyperion Smart View for Office User's Guide for Oracle Hyperion Smart View*.

To connect Oracle Fusion General Ledger Balances cubes in Smart View:

> **Note:** You need to perform these steps only once for a new server and database.

1. Open Smart View from **Start menu > Programs > Microsoft Office > Microsoft Excel 2007**.
2. Go to the **Smart View menu > Open**, in the **Start** on the ribbon > click the Smart View Panel that appears in the drop down box under the ribbon. This launches a task pane.
3. Click **Shared Connections** on the task pane.
4. Log in with your user name and password.
5. Select Essbase from the **Select Server to proceed** dropdown list of shared connections.

> **Note:** If the Essbase Server is not there, then it has to be added. Use the following steps:
>
> - Click the **Add Essbase Server** link on the bottom of the spreadsheet.
> - Specify the Essbase Server login and password.
> - Expand the Essbase sever and locate the cube under it.

6. Click **Expand** to expand the list of cubes.
7. Expand your cube (name of your chart of accounts).
8. Click **db**. A list of functions appears on the bottom of the panel.
9. Click **Ad hoc analysis**.

To set how the name and alias of the Essbase database appears:

1. Click **Options** on the ribbon **>** select the **Member Options >** select **Member Name Display**.
2. Set one of the following options:
   - **Distinct Member Name**: Only shows the full Essbase distinct path.
   - **Member Name and Alias**: Shows both the member name and the alias.
   - **Member Name Only**: Shows only the member name.

> **Note:** The Smart Slice feature is not supported in Oracle Fusion General Ledger. For all other documentation, refer to the *Oracle Hyperion Smart View for Office User's Guide for Oracle Hyperion Smart View*.

20.1.6 Configuring Workspace Database Connections

Administrators need to create database connections from Workspace so users can access the cubes from Workspace and Financial Reporting Studio.

> **Note:** Ledger setup has to be completed before the database connection can be created. Oracle Fusion General Ledger balances cubes are created as part of ledger setup. There is a separate cube for each combination of chart of accounts and accounting calendar. A database connection is needed for each cube.

To define a database connection, do the following:

1. From the **Navigator**, select **Financial Reporting Center**.
2. From the **Financial Reporting Center** task panel, select **Open Workspace for Financial Reporting**.
3. From within Workspace select the **Navigator** menu **> Applications >BI Catalog**.
4. From the **Tools** menu, select **Database Connection Manager.**
5. Click **New**.
6. Enter a user-friendly database connection.
7. Enter Essbase as the **Type**, your server, user name, and password.
8. Select **Application** (cube) and **Database** from the list of values. Expand the **Application** name to see the related **Database**, for example, db.
9. Click **OK** twice to save your selections.
10. Click **Close** in the Database Connection Manager window to save your connection.

For more information about configuring Essbase database connections in Workspace, see *Oracle Essbase Database Administrator's Guide for Oracle Essbase*.

Note: The database connection is available in both Workspace and Financial Reporting Studio. Optionally, it can be set up in Financial Reporting Studio when putting grids on a report. This should only be done by an administrator.

20.1.7 Configuring Oracle Fusion Transactional BI Dimensions

Within Oracle Fusion Transactional Business Intelligence (BI), Accounting Segment Dimensions such as Balancing segment or Cost Center segment are based on the Chart of Accounts configuration. These segments can be configured to be tree-enabled, which means that hierarchies are defined on the segment values for rollup purposes. In such scenarios, you must filter by a specific hierarchy when performing ad-hoc queries against tree-based accounting segments. Incorrect results may occur if tree filters are not applied. To apply tree filters, create a filter condition on Tree Filter attributes in Accounting Segment Dimensions.

Note: For information on setting up General Ledger accounting segments, see the *Oracle Fusion Transactional Business Intelligence Administrator's Guide*.

20.2 Setting Up Oracle Document Capture and Oracle Forms Recognition

Oracle Fusion Financials uses Oracle Document Capture to import payables invoice and expense receipt images from various sources including scanners, e-mail, and FTP sites. Oracle Fusion Payables also leverages Oracle Forms Recognition for intelligent data recognition for invoice entry.

Note: This task is not applicable to Oracle Cloud implementations.

If you plan to implement Oracle Fusion Expenses and use automated receipt image processing, then you must set up Document Capture and configure it for expenses. If you have licensed Oracle Fusion Automated Invoice Processing, then you must set up Forms Recognition in addition to Document Capture, and configure both for payables.

To set up Document Capture and Forms Recognition, perform these steps in the specified order:

1. Configure Document Capture and Forms Recognition network shares.
2. Install and configure Document Capture and Forms Recognition on Windows desktop.

> **Note:** For details regarding users and privileges for the setup, refer to the installation guides of Oracle Document Capture and Oracle Forms Recognition.

20.2.1 Configuring the Oracle Webcenter: Imaging and Process Management Input Directory Network Share

Oracle Document Capture and Oracle Forms Recognition save images to the Oracle Webcenter: Imaging (Imaging) input directory for further processing. Since Document Capture and Forms Recognition are Windows-based products, you need to configure the input directory as a network shared directory so that Document Capture and Forms Recognition can save images to this location.

> **Note:** This task is not applicable to Oracle Cloud implementations.

To install network sharing for Oracle Document Capture and Oracle Forms Recognition:

1. Verify the Imaging input directory path.
2. Configure the network share for the Imaging input directory.
3. Verify Imaging Input Agent.
4. Configure the Windows mapped network drive for the input directory.

20.2.1.1 Verifying the Oracle Webcenter: Imaging Input Directory Path

To verify the input directory path:

1. Log in to the Enterprise Manager on the Common Domain, as an Administrator.
2. Navigate to the Domain level.
3. Select **System MBean Browser**.
4. Open the `oracle.imaging.config.bean`.
5. Look for the **InputDirectories** value.
   - This is the Imaging input directory where Imaging and Process Management will check for incoming scanned invoices.
   - The path will point to a directory on the server running Imaging.
6. Open a terminal window for the server running Imaging and check the path specified for the Input Directory.

The path should be a symbolic link pointing to a folder on a storage server. Both the Imaging server and the Windows server must have read/write access to the same folder on the storage server.

20.2.1.2 Configuring the Network Share for the Oracle Webcenter: Imaging Input Directory

Enable the Imaging input directory to be accessed by Document Capture or Forms Recognition running on Windows:

- The storage server share should have Common Internet File System (CIFS) enabled for Windows compatible share names.
- The path to the Windows share name should be in Universal Naming Convention (UNC) format.

Note: If you have licensed Oracle Fusion Automated Invoice Processing, individual Oracle Document Capture workstations used for scanning invoices do not need access to the input directory.

The storage host must grant read/write access to the Imaging Input Agent running on the Common Domain host and at least one Windows user with login access to the server running Oracle Document Capture and Oracle Forms Recognition.

20.2.1.3 Verifying Oracle Webcenter: Imaging Input Agent

To verify if the Imaging Input Agent is operating correctly:

1. Log in to the Oracle Enterprise Manger for the Common Domain.
2. Navigate to the Imaging Server.
3. Restart the server.

   After the server restarts, check the input directory path referenced earlier. You should see a file named `InputAgent.lock`. If you do not see this file, verify that the image server is running and check the image server logs for errors. If you notice errors, check whether the Input Agent has the necessary permissions in the storage directory. The Input agent needs read/write file access to this directory.

   Additionally, verify that the Windows network drive is correctly mapped with permitted read/write access. You can do this by creating a folder or file from the Linux box where the Imaging server is running. Oracle Forms Recognition is not compatible with NFS mounted shares on Windows. You must use create CIFS shares for Windows instead. The Windows user should be able to view it on the Windows network drive and should be able to open and modify it.

20.2.1.4 Configuring the Windows Mapped Network Drive for the Input Directory

You must log in to the Windows desktop with a user ID that has explicit access to the input directory file share.

You need to map the drive on the Windows servers running Oracle Forms Recognition and Oracle Document Capture servers. The drive will not be mapped on individual user machines running Oracle Document Capture client for Invoicing.

1. Open Windows Explorer.
2. Right-click the folder icon that corresponds to your computer name.

3. Select Map Network Drive.
4. Select a drive letter, for example Y.
5. Specify the path for the shared directory on the storage host, using the UNC format: `\\<host name>\<name>`.
6. Click **OK** and verify that the network share now appears in Windows Explorer as the drive letter you specified. If Windows Explorer is unable to create the mapped drive, the issue may be that the Common Internet File System (CIFS) is not enabled on the storage host.
7. Verify that Windows users have read/write access to the input directory and all its file contents.
8. Verify that the Input Agent directory includes the `InputAgent.lock` file (the input directory may be a sub-directory of the share). If you do not see the `InputAgent.lock` file, the following are possible explanations:
   - The Imaging Server is not running and needs to be started.
   - The Imaging Server is running but the Input Agent does not have the appropriate access to the network share directory and cannot generate the `InputAgent.lock` file.
   - The Imaging Server configuration for Input Agent Directory does not point to the same network share as the mapped network drive, or it points to a sub-directory other than the one you are verifying.

Note: To verify that the Windows network drive is correctly mapped with permitted read/write access, create a folder or file from the Linux box where the Imaging server is running and check if the Windows user is able to view the folder or file on the Windows network drive and is able to open and modify it.

20.2.2 Configuring the Oracle Forms Recognition Project Network Share

The Oracle Forms Recognition project directory contains directories and files shared by Oracle Document Capture, Oracle Forms Recognition Designer, Oracle Forms Recognition Verifier, and Oracle Forms Recognition Runtime Service. In a typical installation scenario, these applications are not installed on the same computer. However, the project directory must be stored in a shared directory accessible to each application, regardless of where it is installed.

Note: This task is not applicable to Oracle Cloud implementations.

To configure the Oracle Forms Recognition project network share, do the following:

1. Configure the share for the Oracle Forms Recognition AP Project Folder.
2. Configure the Windows mapped network drive for the AP Project Folder.

20.2.2.1 Configuring the Network Share for the Oracle Forms Recognition AP Project Folder

Ensure that the Oracle Forms Recognition project directory is accessible to the Oracle Document Capture or Oracle Forms Recognition applications running on Windows.

- The storage server share should be configured with Common Internet File System (CIFS) enabled for Windows compatible share names.
- The Windows share name must be in universal naming convention (UNC) format.
- The network share is meant for exclusive use by the Oracle Document Capture or Oracle Forms Recognition applications running on Windows.

Configure the storage host to share the Oracle Forms Recognition Project directory with the Oracle Document Capture and Oracle Forms Recognition users.

20.2.2.2 Configuring the Windows Mapped Network Drive for the AP Project Folder

You must log on to the Windows desktop with a user ID that has explicit access to the Oracle Forms Recognition project file share.

Note: This mapping is done on the following:

- Windows servers running Oracle Forms Recognition and Oracle Document Capture servers for Expenses
- Servers running Oracle Forms Recognition Designer and Verifier
- Invoice scanning workstations running Oracle Document Capture

---

Perform the following steps to configure the Windows mapped network drive:

1. In Windows Explorer, identify the folder for the PC icon that displays the same name as that of the actual PC.
2. Right-click the folder icon that corresponds to your computer name.
3. Right-click the folder and select Map Network Drive.
4. Select a drive letter, for example X.
5. Specify the path for the shared directory on the storage host, using the UNC format: \\<host name>\<share name>.
6. Click **OK** and verify that the network share now appears in Windows Explorer as the drive letter you specified. If Windows Explorer is unable to create the mapped drive, the issue may be that CIFS is not enabled on the storage host.

20.2.3 Installing and Configuring Oracle Document Capture and Oracle Forms Recognition on Windows

To configure Oracle Document Capture and Oracle Forms Recognition to run on Windows, perform the following tasks in the given order:

Note: These tasks are not applicable to Oracle Cloud implementations.

---

1. Install prerequisites.
2. Run the setup utility.
3. Install Oracle Document Capture.
4. Configure Oracle Document Capture.

5. Configure Oracle Document Capture Import Server for Importing Images from E-Mail.
6. Install Oracle Forms Recognition for Payables.
7. Configure Oracle Forms Recognition for Payables.
8. Configure shared drive access for Oracle Forms Recognition Runtime Service Manager.

> **Note:** Ensure that you have configured the required network shares before performing these steps. Steps 4 to 7 (Configure Oracle Document Capture to Configure Oracle Forms Recognition for Payables) are required only if you have licensed Oracle Fusion Automated Invoice Processing.

For more information on performing post-installation tasks, see the *Oracle Document Capture Installation Guide* and the *Oracle Forms Recognition Installation Guide*.

20.2.3.1 Prerequisites

Before you proceed with the installation and configuration of Oracle Document Capture and Oracle Forms Recognition, do the following:

1. Ensure that the empty Document Capture schema is created in the Oracle database with at least three user profiles: a read-only user profile for reporting, a read/write user profile for schema administration, and a read/write user profile for the Document Capture runtime connection. Document Capture tracks batches and stores audit information in the schema tables. The Document Capture runtime connection configuration includes read/write user profile credentials so that Document Capture can write data to the schema tables without requesting a separate login.

   For more information on configuring the Document Capture database, see the *Oracle Document Capture Installation Guide*.
2. Install and Configure Oracle database support for Open Database Connectivity (ODBC) and OLEDB. For more information, see *Oracle Database Software Downloads* on Oracle Technology Network.
3. Ensure that Java Runtime Environment (JRE) 1.6 or higher is installed. For more information, see Java Downloads on Oracle Technology Network.
4. To configure expenses, create the folder `C:\ODC Projects\EXM\Import`. You need to share this folder with read-write permissions enabled for incoming expense documents.
5. Download the **Capture-FormsRec_FA.zip** file from the Oracle Fusion Applications repository. The zip file is located at `<repository_root>/installers/Capture-FormsRec`.

20.2.3.2 Running the Setup Utility

This program streamlines the installation and configuration of Oracle Document Capture and Oracle Forms Recognition.

1. Extract the contents of the Capture-FormsRec_FA.zip (downloaded earlier from the Oracle Fusion Applications repository) to a temporary folder and double-click **Setup.exe** to run the utility. The Oracle WebCenter Capture and Forms Recognition for Fusion Financials Setup window appears.

2. In the I/PM Input Agent Folder field, enter a UNC path of the folder from which IPM uploads the documents. For example, `\\<server_name>\<share_name>`.
3. In the Oracle Forms Recognition AP Project Folder field, provide the root directory for the AP project. For example, `<Drive Letter>:\OFR`. If the specified directory does not exist at the mentioned location, the installer creates a directory with the same name.

You are now ready to install and configure Oracle Document Capture and Oracle Forms Recognition. The relevant instructions are provided in the subsequent sections.

20.2.3.3 Installing Oracle Document Capture

Repeat the installation procedure on every machine that runs Oracle Document Capture.

> **Note:** If an error occurs while installing Oracle Document Capture, verify if the computer's print spooler service is running (Start - Settings - Control Panel - Administrative Tools - Services). Scroll down until you see Print Spooler. If the status shows that it has not started, right-click the Print Spooler service and select Start. You can now retry installing Oracle Document Capture.

1. On the Oracle WebCenter Capture and Forms Recognition for Fusion Financials Setup window, in the Oracle Document Capture region, click **Install**. The Oracle Document Capture installer appears.
2. Proceed through the installation steps to complete the installation. Once the installation is complete, the Setup utility initiates an additional process to install a patch.
3. Proceed through the options to complete the patch installation. After it is complete, the **Configure** button in the Oracle Document Capture region is enabled.

20.2.3.4 Configuring Oracle Document Capture

To configure Oracle Document Capture:

1. On the Oracle WebCenter Capture and Forms Recognition for Fusion Financials Setup window, in the Oracle Document Capture region, click **Configure**. The Oracle Document Capture Configuration Utility dialog box appears.
2. In the Batch Folder field, browse and select the folder where Oracle Document Capture batch files are stored.
3. In the Commit Folder field, browse and select the folder where Oracle Document Capture commits the captured files.

> **Note:** If you are using Oracle Forms Recognition, leave this blank for now. After you install Oracle Forms Recognition, you will come back and set the folder path to `<Drive Letter>:\OFR_Project\AP\Global\Import`. If you are not installing Oracle Forms Recognition, set this to the Image Processing Management Input Directory.

4. Click **OK**. The Capture Batch Setup dialog box appears.

Note: The Capture Batch Setup dialog box appears only when configuring Oracle Document Capture for the first time.

5. On the Capture Batch Setup dialog box, do the following:
   a. In the Enter Path to Network Batch Folder field, specify the same folder path that you have provided in the Batch Folder field on the Oracle Document Capture Configuration Utility dialog box.
   b. In the Enter Path to Network Commit Folder field, specify the same folder path that you have provided in the Commit Folder field on the Oracle Document Capture Configuration Utility dialog box.
   c. In the Capture Database Setup area, select the Other Database Platform option and click **Configure**. The Configure Database Connection dialog box appears.
   d. Click **Configure DB Connection**. The Data Link Properties dialog box appears.

      - On the **Provider** tab, select **Oracle Provider for OLE DB** and click **Next**.

      - On the **Connection** tab, do the following:

         a. In the **Data Source** field, enter the name of the Oracle database.
         b. Select the **Use a specific user name and password** option and provide the **User name** and **Password** that have read and write access to the Capture schema.
         c. Select the Allow saving password option.
         d. Click **Test Connection** to check for connectivity issue if any, and resolve it before you proceed with the configuration.

      - Click **OK**. The Data Link Properties dialog box closes.
   e. On the Configure Database Connection dialog box, click **OK**. The Configure Database Connection dialog box closes.
   f. On the Capture Batch Setup dialog box, click **Initialize DB** to populate the Capture schema in the Oracle database.

Note:

- Initializing the database is required when you configure Oracle Document Capture for the first time.
- If you are configuring a standalone instance of Oracle Document Capture for testing, you can use the default Capture database (capture.mdb) that is installed with the product. On most systems, this database is located in the Oracle Document Capture installation directory. On Windows 2008 R2, the Capture database is installed in the system `ALLUSERPROFILES\Oracle Document Capture` folder. By default, `ALLUSERSPROFILES` is `C:\ProgramData`.

  To use the default capture.mdb, you need to create a data source based on Microsoft Jet OLE DB 4.0. The local Capture database is only used for testing. For production environments, you must create the Capture schema in the Oracle database.

A warning message appears indicating loss of existing data in the Capture schema if you proceed with the initialization.

- Click **Yes**. The Security Model dialog box appears.

- Select the option that is appropriate to the system environment and click **OK**. The Microsoft Windows Open dialog box appears.

- Navigate to the Oracle Document Capture installation directory, search for the `Capture_ORACLE.sql` file, select it, and click **Open**. Oracle Document Capture runs the script of the Capture schema and creates the required tables in the Oracle database.

g. On the Capture Batch Setup dialog box, click **OK**. The Capture Batch Setup dialog box closes.

6. On the Oracle Document Capture Configuration Utility dialog box, click **OK**.

Note: If prompted for user credentials, enter the user name and password that have been used during the configuration process.

20.2.3.4.1 Configuring Additional Routing Attributes for Manual Scanning To configure additional routing attributes for manual scanning:

1. If you are installing the Automated Invoice Processing components for the first time you already have the latest cabinet files, so you can skip the unzip and import steps and proceed to Step 2. Otherwise, if you were already using Automated Invoice Processing, perform the following steps to import the latest cabinet files:

a. Unzip the Capture-FormsRec_FA.zip package.

b. Import the **ApInvoiceOdcCabinet.zip** and **ApInvoiceOfrCabinet.zip** files using the Document Capture Import Export utility.

2. Open Oracle Document Capture and select Indexing - Manage Index Profiles.

3. Select the Fields tab for index profiles Fusion Payable Invoices With OFR and Fusion Payable Invoices Without OFR and verify that they contain the following index fields: Routing_Attribute_1 through Routing_Attribute_5, and URN.

4. Select System - Manage Macros.

5. Select the Scan for ISIS category.

6. Select the OFR-Scan-ISIS-Macro macro.

7. Click **Setup**.

8. (Optional) Review and modify the Prompt User upon closing Review option in the Index Documents area to meet your requirements.

9. Select the Do not Commit Batch option in the Commit Options area.

10. Click **OK**.

11. (Optional) If you are not planning to use all five attributes, or you decide to use a longer length for each of the remaining attributes, you can change the maximum length of the index field attributes:

a. Select Admin - File Cabinets.

b. Select either Payables Invoice with OFR or Payables Invoices without OFR, depending on which file cabinet you are using.

c. Select the routing attribute that you want to edit.

d. Click **Edit**.

e. Update the Max Length field.

Note:

- Do not modify the index field names, otherwise the predefined attribute configuration will not work as expected.
- The sum of the maximum lengths is limited to the number of characters allowed by Oracle Forms Recognition (233), minus the number of characters in the file path where the image files are imported, minus the TIF file extension including the period (4), minus the characters reserved for internal use (40), minus one separator character per attribute.

  For example, if the image files are imported into the C:\OFR\Import\ directory and if you are using all five attributes, you should not exceed 170 characters (233-14-4-40-5).
- The number of characters for an attribute value cannot exceed the Max Length for that attribute. If the attribute value character count exceeds the specified maximum length, Oracle Document Capture's scan and commit will error.

---

f. Click **OK**.

20.2.3.5 Configuring Oracle Document Capture Import Server for Importing Images from E-Mail

To set up the Oracle Document Capture Import Server to import invoice images that are received through e-mail and to capture additional attributes for routing based on information in the e-mail subject, perform the following steps.

To configure additional routing attributes, do the following:

1. If you are installing the Automated Invoice Processing components for the first time, you already have the latest cabinet files, so you can skip the unzip and import steps and proceed to Step 2. Otherwise, if you were already using Automated Invoice Processing, perform the following steps to import the latest cabinet files:
   a. Unzip the **Capture-FormsRec_FA.zip** package.
   b. Import the **ApInvoiceOdcCabinet.zip** and **ApInvoiceOfrCabinet.zip** files using the Document Capture Import Export utility.
2. (Optional) Perform Step 11 in section "Configure Additional Routing Attributes for Manual Scanning" to change the maximum lengths of the index attribute fields.

To configure the Email Provider batch job, do the following:

1. Open the Oracle Document Capture Import Server.
2. Select Setup - Batch Jobs.
3. Expand the Email Provider folder.
4. Select the AP Email Provider batch job.

5. If you are not using Oracle Forms Recognition, perform the following steps, otherwise proceed to Step 6.
   a. Select the General tab.
   b. In the File Cabinet field, select Payables Invoice without OFR.
   c. In the Server Macro field, select <NONE>.
   d. Select the Processing tab.
   e. Uncheck the Commit Batches option.
6. Select the Image Output tab. The default resolution is set to 300 x 300.

   Important: Do not modify this setting.

7. Select the Email Provider Settings tab.
8. Select the Email Accounts subtab.
   a. In the Email Protocol field, select the e-mail protocol that is being used.
   b. In the Email Server Name field, specify the DNS name that the e-mail server uses.
   c. In the Email Addresses to Process field, enter the e-mail addresses that are designated to process scanned invoices.
9. Select the Email Filters subtab.
   a. Configure the settings in the Process Emails containing specified text area.

      Specify the e-mail text that the Oracle Document Capture Import Server must find to process an e-mail. If the designated e-mail account is responsible only for receiving scanned invoices, this section can be left blank.
   b. Configure the settings in the Attachment Processing area to process the invoice image attachments.
10. Select the Post-Processing subtab.
    a. In the Upon Successful Import area, select the action to take when the import process succeeds.

       The default setting is to delete the message from the e-mail account.
    b. In the Upon Failed Import area, select the action to take when the import process fails.

       The default setting is Don't Delete Message, which leaves the failed imported invoices in the e-mail account.
11. Click **Close**.

To schedule the Email Provider batch job, do the following:

1. Select Server - Schedule.
2. Click **Schedule New Event**.
3. In the Event field, select Email Provider - AP Email Provider.
4. In the Event Properties area, specify the intended frequency.

> **Note:** The recommended frequency setting is Every 1 Minute.

5. Select **Server - Activate** to run the job.

20.2.3.6 Installing Oracle Forms Recognition for Payables

You need to install Oracle Forms Recognition for Payables on two different servers, one server each for:

- The Runtime Service: The instance of Oracle Forms Recognition for the Runtime Service must be installed on a secure server accessible only to administrators. The Runtime Service normally runs without any user intervention. However, administrators need to access the Runtime Service to perform setup and configuration tasks.
- The Designer and Verifier: The instance of Oracle Forms Recognition for the Designer and Verifier needs to be installed on a server that is accessible to the users of the applications.

To install Oracle Forms Recognition, perform the following steps:

1. On the Oracle WebCenter Capture and Forms Recognition for Fusion Financials Setup window, in the Oracle Forms Recognition region, click **Install**. The Oracle Forms Recognition installer appears.

> **Note:** While installing it on each server, ensure that you select the Complete install option.

2. Proceed through the installation steps to complete the installation. Once the installation is complete, the Setup utility initiates an additional process to install a patch, if any.
3. Proceed through the options to complete the patch installation. After it is complete, the Configure button in the Oracle Forms Recognition region is enabled.

For more information about installing Oracle Forms Recognition, see the *Oracle Forms Recognition Installation Guide*.

20.2.3.7 Configuring Oracle Forms Recognition for Payables

To configure Oracle Forms Recognition for Payables, perform the following steps:

1. On the Oracle WebCenter Capture and Forms Recognition for Fusion Financials Setup window, in the Oracle Forms Recognition region, click **Configure**. The Oracle Forms Recognition Runtime Server Creation dialog box appears.

> **Note:** The Oracle Forms Recognition Runtime Server Creation dialog box appears if you have installed Oracle Forms Recognition for the first time. If Oracle Forms Recognition is already available and was earlier configured, the Oracle Forms Recognition Runtime Server Creation dialog box is skipped and the Oracle Forms Recognition Configuration Utility dialog box appears. The instructions here are provided assuming that Oracle Forms Recognition is installed for the first time.

2. On the Oracle Forms Recognition Runtime Server Creation dialog box, select one of the options to create the Runtime Service:
   - All (Import, OCR, Classification, Extraction, Export and Clean-up) to create and configure a single instance of the Runtime Service that performs all Oracle Forms Recognition workflow operations. This is the default option and is normally reserved for use by demonstration systems.
   - Custom to customize the creation of the Runtime Service based on several parameters as described here:

   Note:

   - For production environments, Oracle recommends that you create separate Runtime Service instances for each function using the Custom options described in the following table. If you need to increase system capacity, you need to add additional instances of OCR, Classification and Extraction Runtime Service.
   - If you plan to create separate instances for each function, create all of them at this point. This dialog box is available only during first time installation. You cannot access it later to add Runtime Service instances. If you want to add instances later, you need to create each of them manually.

Sub-option	Functional Description
Import	Selecting this checkbox creates an import enabled instance of the Runtime Service.
OCR, Classification and Extraction	Selecting this checkbox creates an OCR, Classification and Extraction enabled instance of the Runtime Service.
Number of Instances	You can specify the number of OCR, Classification and Extraction enabled instances that you want to create. The default value is 1. An OCR, Classification and Extraction enabled instance is CPU intensive and therefore, if you need to balance higher invoice loads, you need to create additional instances. However, it is recommended that the number of such instances must not exceed the number of cores on the server. You can add additional instances using the SET file created by the Setup utility. The SET file name is FusionAP - OCE.set, which is located in the Bin folder of the Forms Recognition install folder, for example `C:\Program Files\Oracle\Forms Recognition\Bin`.
Export and Clean-up	Selecting this checkbox creates an Export and Clean-up enabled instance of the Runtime Service.

3. Click **OK**. The Oracle Forms Recognition Runtime Server Creation dialog box closes and the Oracle Forms Recognition Configuration Utility dialog box appears.
4. In the AP Solution INI File field, ensure that the path is set to the automatically installed INI file.
5. In Database Connections, ensure that at least one connection is selected. In absence of a Database Connection, click **Create** to create a database connection. Ensure that the selected database connection has read-only access to the Fusion schema.
6. From the ODBC System DSN (32-bit) list, select one of the predefined ODBC System DSN value. If the list is blank, create an ODBC System DSN using the ellipsis button next to the field. Ensure that the ODBC connection has read-only access to the Fusion schema.

7. Enter the User ID and Password associated with the selected ODBC System DSN.
8. Click **Test Connections** to ensure that the selected database connection is active and working.
9. In the PO Format field, enter the format of the purchase order.

> **Note:** You can use # as a wildcard character to represent a single number and @ as a wildcard character to represent a single alphabet.

10. In the Ignore Characters field, specify the characters such as comma, hyphen, period that may appear as part of the purchase order but need to be ignored. The ignore characters are always associated with a PO format.
11. Click **Add**. The PO format is added to the Defined Formats list, while simultaneously storing the associated characters to be ignored when that PO format is in use.

For more information about installing Oracle Forms Recognition, see the *Oracle Forms Recognition Installation Guide*. For more information on PO Formats see the *AP Solution Guide* located at `<Drive Letter>:\OFR_Projects\AP`.

20.2.3.8 Configuring Shared Drive Access for Oracle Forms Recognition Runtime Service Manager

The Oracle Forms Recognition runtime service manager processes invoice images and exports them to a shared network drive. By design, Windows services are not allowed to access mapped network drives. Therefore, to access a network share, a Windows service must be running as an authenticated Windows user and it must access the share by specifying a UNC style path (`\\server_name\share_name`).

Subsequently, you must assign a Windows user profile to the Oracle Forms Recognition Runtime Service Manager. The specified user profile must have read/write access to the shared network drive.

1. On the server that hosts the Runtime Service, navigate to **Start > Control Panel > Administrative Tools**.
2. Select **Services**.
3. Right-click **Oracle Forms Recognition Runtime Service Manager** and select **Properties**.
4. Select the **Log On** tab.
5. Select the **This account** radio button, and enter the user name and password of the user granted read/write access to the shared network folder.
6. Click **Apply** and then click **OK**.

20.3 Oracle Fusion Advanced Collections Dunning

Oracle Fusion Advanced Collections Dunning feature utilizes Oracle Business Intelligence Publisher to distribute dunning letters to customers via E-mail, fax or print. To use this feature, you must configure Oracle Business Intelligence Publisher to connect to the deploying company's internal E-mail, or the print or fax servers.

20.3.1 Adding the E-Mail Server

To add an E-Mail server:

1. From the Admin page select E-mail. This displays the list of servers that have been added. Select Add Server.
2. Enter the Server Name, Host, and Port for the E-mail server.
3. Select a Secure Connection method to use for connections with the E-mail server. The options are: None or SSL. Use Secure Socket Layer. TLS (Transport Layer Security). Use TLS when the server supports the protocol; SSL is accepted in the response. TLS Required. If the server does not support TLS, then the connection is not made.
4. Optionally enter the following fields if appropriate: General fields; Port Security fields User name and Password.

20.4 Enabling Encryption of Sensitive Payment Information

Financial transactions contain sensitive information, which must be protected by a secure, encrypted mode. In Oracle Fusion Payments, you can enable the encryption process for various types of payment information. Before you can enable encryption for credit cards and external bank accounts, you must create a wallet file.

This task is not applicable to Oracle Cloud implementations.

Note: This task is optional and applies mainly to Receivables, Payables, Expenses, and Collections. You should know how to perform this task based on your organization's data security policies. Regardless of whether you choose to complete this setup, Oracle Fusion Applications functionality should not be affected.

After installing Oracle Fusion Applications, you can secure sensitive information by using any one of the following methods:

- Automatically create a wallet file, automatically generate a master encryption key, and manually enable encryption.
- Manually create a wallet file, automatically generate a master encryption key, and manually enable encryption.
- Manually create a wallet file, manually generate a master encryption key, and manually enable encryption.
- Automatically create a wallet file, automatically generate a master encryption key, and manually enable encryption.

20.4.1 Automatically Creating a Wallet File, Automatically Generating a Master Encryption Key, and Manually Enabling Encryption

To automatically create a wallet file, automatically generate an encryption key, and manually enable encryption, perform the following steps:

1. Navigate to the Manage System Security Options page as follows: Navigator link > Tools menu: Setup and Maintenance link > Overview page > All Tasks tab >

Search field: Task Lists and Tasks > Name field: Payments > Search button > Expand Define Payments Security folder > Manage System Security Options task: Go to Task icon > Manage System Security Options page.

2. In the Manage System Security Options page, click **Edit Master Encryption Key**. The Edit Master Encryption Key dialog box appears.
3. In the Edit Master Encryption Key dialog box, select the Application-generated radio button.
4. Click **Save and Close**.
5. In the Manage System Security Options page, click **Encrypt** in either the **Credit Card Data** region or the **Bank Account Data** region or in both regions to enable encryption for sensitive financial data.

20.4.2 Manually Creating a Wallet File, Automatically Generating a Master Encryption Key, and Manually Enabling Encryption

To manually create a wallet file, automatically generate an encryption key, and manually enable encryption, perform the following steps:

1. Create an empty Oracle Wallet, ewallet.p12, using the Oracle Wallet Manager utility.
2. Navigate to the Manage System Security Options page as follows: Navigator link > Tools menu: Setup and Maintenance link > Overview page > All Tasks tab > Search field: Task Lists and Tasks > Name field: Payments > Search button > Expand Define Payments Security folder > Manage System Security Options task: Go to Task icon > Manage System Security Options page.
3. In the Manage System Security Options page, click **Edit Master Encryption Key**. The Edit Master Encryption Key dialog box appears.
4. In the Edit Master Encryption Key dialog box, select the Application-generated radio button.
5. Click **Save and Close**.
6. In the Manage System Security Options page, click **Encrypt** in either the Credit Card Data region or the Bank Account Data region or in both regions to enable encryption for sensitive financial data.

20.4.3 Manually Creating a Wallet File, Manually Generating a Master Encryption Key, and Manually Enabling Encryption

To manually create a wallet file, manually generate an encryption key, and manually enable encryption, perform the following steps:

1. Create an empty Oracle Wallet, ewallet.p12, using the Oracle Wallet Manager utility.
2. Navigate to the Manage System Security Options page as follows: Navigator link > Tools menu: Setup and Maintenance link > Overview page > All Tasks tab > Search field: Task Lists and Tasks > Name field: Payments > Search button > Expand Define Payments Security folder > Manage System Security Options task: Go to Task icon > Manage System Security Options page.
3. In the Manage System Security Options page, click **Edit Master Encryption Key**. The Edit Master Encryption Key dialog box appears.
4. Take one of the following actions:

- In the Edit Master Encryption Key dialog box, select the User-defined radio button.

  In the Key File Location field, enter the path to the master encryption key, click **Save and Close**, and then click **Done**.

- Generate a secure, custom key by copying a file containing the bits of the key to the same directory as the empty Oracle wallet, ewallet.p12

  Note: After the wallet is created, ensure that you securely delete the file containing the key bits by using a utility that supports secure deletion.

5. In the Manage System Security Options page, click **Encrypt** in either the Credit Card Data region or the Bank Account Data region or in both regions to enable encryption for sensitive financial data.

20.4.4 Automatically Creating a Wallet File, Automatically Generating a Master Encryption Key, and Manually Enabling Encryption

To automatically create a wallet file, automatically generate an encryption key, and automatically enable encryption, perform the following steps:

1. Navigate to the Manage System Security Options page as follows: Navigator > Tools : Setup and Maintenance > Overview page > All Tasks tab > Search field: Task Lists and Tasks > Name field: Payments > Search > Expand Define Payments Security folder > Manage System Security Options task: Go to Task icon > Manage System Security Options page.
2. In the Manage System Security Options page, click **Apply Quick Defaults**. The Apply Quick Defaults dialog box appears.
3. In the Apply Quick Defaults dialog box, select all the checkboxes: Automatically create wallet file and encryption key, Encrypt credit card data, and Encrypt bank account data.
4. Click **Apply**.

For more information on Payments security, see "Define Funds Capture and Payments Security" in the *Oracle Fusion Applications Financials Implementation Guide*.

20.5 Configuring a Communication Channel to a Payment System

Note: This task is optional and applies mainly to Receivables, Payables, and Payments. You should know how to perform this task based on your organization's bank/payment system relationships and your organization's network topology. Your organization's IT department will be able to tell you whether to perform this setup step or if an alternate method is preferred within your organization.

To transmit or receive payment information to or from a payment system through a firewall, you must configure the communication channel used to communicate with the payment system by performing the following steps:

1. Configure and deploy a tunnel.

2. Set up SSL security to communicate with the payment system servlet.

> **Note:** This task is not applicable to Oracle Cloud implementations.

20.5.1 Configuring and Deploying a Tunnel

To communicate with a payment system through a firewall, you can use the Tunneling feature of Oracle Fusion Payments. The Tunneling feature is used to deliver data, such as a payment file or settlement batch, using two protocols, one of which encapsulates the other. Tunneling is also referred to as delegated transmission, since the initial transmission from Payments is a request to an external module (the transmission servlet) to deliver data using an independent transmission protocol. The name of the transmission protocol, its parameters, and the actual data to be delivered are encapsulated within the body of the tunneling transmission protocol.

The purpose of tunneling is to allow connectivity between Payments and external payment systems without compromising network security. Processor payment systems, for example, often require protocols, such as FTP or IP socket connectivity to receive payment files. Instead of creating breaches in your firewall to accommodate these connectivity requirements, you can instead deploy the Payments transmission servlet on a host outside your firewall and then tunnel or delegate requests to it from the Payments engine. The Payments transmission servlet does not use the applications database and can be completely isolated from the intranet of your deployment environment.

Tunneling Protocol

Payments uses a customized tunneling protocol called the Oracle Fusion Payments Tunneling Protocol. This protocol uses HTTP POST as its underlying transmission mechanism. HTTPS is also supported. When the tunneling protocol sends a request, it places an XML message header within the body of the request, which is meant to identify the tunneled or encapsulated protocol, as well as the parameters to use when invoking it, such as host name, user name, and password for FTP. The data to be delivered is sent after the XML message header is sent.

> **Important:** Payments does not support the tunneling or encapsulation of a tunneling protocol.

As a supported transmission protocol, the tunneling protocol implements the **oracle.apps.financials.payments.sharedSetup.transmissions.publicModel.util.TunnelingFunction** interface. Table 20–1 presents the parameters and descriptions of the Payments tunneling protocol.

Table 20–1 Parameters and Descriptions of the Payments Tunneling Protocol

Parameter	Description
`WEB_URL`	The HTTP/HTTPS URL of the transmission servlet executing the protocol.
`USERNAME/PASSWORD`	The user name and password used to access the servlet if its URL is secured by HTTP authentication.

Transmission Servlet

Payments transmission servlet is the module that executes tunneled or delegated transmission requests sent from the Payments engine. The servlet receives the

Payments HTTP XML delivery envelope requests and parses them into XML message header and transmission data components. The format of the XML message header is defined by an XML DTD file named DeliveryEnvelope.dtd. The message header specifies the transmission protocol, as well as the parameters to pass to the tunneled or encapsulated transmission protocol, using its Java class name and entry function name. The transmission servlet then dynamically loads the Java class implementing the tunneled protocol and initiates it by passing to it the transmission parameters parsed from the XML message header and the transmission data.

This behavior is identical to that of the Payments engine. Any protocol can be tunneled, as long as it implements the **oracle.apps.financials.payments.sharedSetup.transmissions.publicModel.util.TransmitFunction** interface. Therefore, any custom-defined protocol can be tunneled or encapsulated to the servlet, provided the Java class which implements it is in the CLASSPATH of the servlet's application container. To deploy the servlet to a different host, such as the one in a DMZ network zone, you must copy **FinPmtTransmitServlet.war** to the transmission servlet's new servlet container. If you want the servlet to support any new transmission protocol that you develop, its Java code must be deployed to the transmission servlet's web application domain.

Configuring Tunneling

Tunneling is configured on the Create Transmission Configuration page. A tunneling transmission configuration is specified as any other transmission configuration, but the protocol is always Payments HTTP XML Delivery Envelope protocol. Once the tunneling protocol is configured, it can use or encapsulate any regular, non-tunneling transmission configuration by specifying a value from the Tunneling Configuration choice list on the Create Transmission Configuration page. Once that is done, ensure that you set up your payment system to support the tunneling protocol and that your corresponding funds capture process profiles and payment process profiles specify the tunneling configuration.

20.5.2 Setting Up SSL Security to Communicate with the Payment System Servlet

When Payments communicates with the payment system servlets, the information exchanged may be sensitive information such as credit card numbers. If the communication is not secure, it poses a security risk.

The security risk is higher under the following circumstances:

- When Payments and the payment system servlets are installed on separate machines
- When Payments is deployed and operates outside your firewall

To set up a payment system servlet with a secured sockets layer, enable HTTPS on the middle-tier server where the servlet resides. If funds-capture-process profiles are not defined for the payment system, change the BASE URL parameter of the payment system to use the https: protocol. Otherwise, change the URLs on any transmission configurations set up to be used with that payment system to contain HTTPS.

20.6 Configuring Oracle B2B Inbound Flow to Receive Supplier Invoices in XML

Oracle B2B Server is an Oracle SOA Suite component that manages interactions between deploying companies and trading partners such as suppliers. Oracle Fusion Payables supports an inbound Oracle B2B flow using Oracle B2B Server for receiving invoices from suppliers in XML format.

Note: This task is not applicable to Oracle Cloud implementations.This task is not applicable to Oracle Cloud implementations.

Trading partners can use this B2B feature to communicate electronically by sending documents in XML format. The B2B XML invoices use the same XML standard 171_ Process_Invoice_002 (version 7.2.1) developed by the Open Applications Group (OAG). For more information on B2B XML Invoices, see the Oracle Fusion Applications Procurement, Payables, Payments, and Cash Guide.

Customers or deploying companies who want to receive and process invoices in XML format (complying to OAG standards) that are provided by the suppliers, need to perform the following post-installation configurations.

- Host Company Configuration
- Supplier Configuration

Note: These configurations are required only if customers or deploying companies want to use the B2B XML invoice feature.

20.6.1 Configuring the Host Company

Perform the following steps to complete Host Company configuration.

1. Set up the Oracle B2B Server.
2. Set up Oracle Supplier Network for the Host Company

Note: This step is required only if customers use Oracle Supplier Network as the communication channel.

3. To set up the Oracle B2B Server, do the following:
   a. Create a supplier trading partner.

Note: The Oracle B2B Server is preloaded with the supported OAG document schemas and sample trading partners such as MyCompany which is the host company trading partner, and ApSampleTradingPartner which is the supplier trading partner. However, you can create your own supplier trading partners as instructed here.

- Log in to the Oracle B2B Server.

- On the left, click **Add** on the Partner toolbar. The Partner Name dialog box appears.

- Enter the name of the trading partner and click **OK**. A confirmation message appears. The new supplier trading partner is listed in the Partner region.

- On the Documents tab, click **Add** to add a document definition for the supplier trading partner. The Select Document Definition dialog box appears.

- Select OAG - 7.2.1 - PROCESS_INVOICE_002 - OAG_DEF and click **Add**. The document definition is added to the supplier and is displayed under Documents.

- For the document definition, clear the checkbox under Receiver.

- In the Partner region, select the new supplier trading partner, and on the Agreement toolbar, click **Add** to add a new agreement between the host company and the new supplier trading partner.

- Enter the name of the agreement.

- On the process train, click the **Select Document Definition** train stop. The Select Document Definition dialog box appears.

- Select the PROCESS_INVOICE_002 document definition mapped to the supplier trading partner and click **OK**.

- Under Agreement Parameters, ensure that the Functional Ack checkbox is clear, and click **Save**.

- To validate the agreement, click **Validate**.

- Click **Deploy**. An information message appears, indicating successful deployment of the agreement.

b. Set up a listening channel.

Note: Oracle B2B Server supports multiple protocols for sending/receiving messages between trading partners. You can choose a protocol that is best suited for your company. Refer to the Oracle B2B Server documentation or online help to learn about each protocol and which parameters need to be set up. Listening channel can be set up at the global level (applicable to all trading partners) or at the trading partner level.

Do one of the following:

- Click **Administration** to set up a global listening channel and click the Listening Channel tab.

- Click **Partners** to set up a trading partner listening channel and click the Channels tab.

- Do not set up a listening channel if Oracle Supplier Network is used by the suppliers to send the B2B invoice payload.

Note: When Oracle Supplier Network is used, the only required setup to communicate with the supplier trading partner is to add a Generic Identifier on the B2B Server, using the Trading Partner Alias of the supplier as the value of the identifier. The Trading Partner Alias of suppliers is defined on the Trading Partners tab of the host company trading partner in the Oracle Supplier Network. The Generic Identifier entry is added to the Identifiers table on the Profile tab of the trading partner page.

Save the changes to complete the set up.

4. Set up Oracle Supplier Network for the Host Company if the supplier uses Oracle Supplier Network to send the B2B invoice payload. To complete the setup, perform the following:

   a. Log in to the Oracle Supplier Network using the registered account.

   b. Access Messaging - Communication Parameters and select HTTPS URL Connection as the Delivery Method.

   c. Click **Modify** to update the delivery method parameter values.

   d. Enter the URL of the B2B HTTP receiver. Consult your system administrator if you do not know the value.

   e. Enter the User ID and password for Oracle Supplier Network.

   Note: You can specify different values for the Test and Production environments.

   f. Access Messaging - Transaction Management.

   g. Add the OAG PROCESS_INVOICE_002 document from the list of available documents if it is not already added.

   h. From the Action drop down list, select Receive.

   i. From each Delivery Method drop down list (OSN Test Delivery Method and OSN Production Delivery Method), select HTTPS URL Connection and click **Submit**.

   j. On the Trading Partners tab, in the Add Trading Partners region, click **Add** to add supplier trading partners. You can add all the supplier trading partners who send invoice payloads to the host company.

5. Set up the B2B Site Code.

   For each supplier site that is enabled for B2B communication, the host company assigns a B2B Site Code to the site and communicates it to the supplier. Supplier has to provide this B2B Site Code in the invoice payload in the <PARTNER><PARTNRIDX> element, with <PARTNER><PARTNRTYPE> = Supplier within the <INVHEADER> element. To assign a B2B Site Code to a supplier site, navigate to the Manage Suppliers UI in the Fusion application. Search for the supplier and then open the supplier site. Enter a value into the B2B Supplier Site Code. Click **Save**. This code needs to be communicated to the suppliers manually so that they can include it in their invoice payloads.

   To assign a B2B Site Code to a supplier site, do the following:

   a. In Oracle Fusion Applications, access Suppliers - Manage Suppliers.

   b. Search for the specific supplier and open the relevant supplier site.

   c. On the Edit Site tab, in the B2B Trading Partner Information region, enter the site code (the site code set by the host company in Oracle B2B Server) in the B2B Supplier Site Code field.

   d. Click **Save**.

   Communicate the same site code to the suppliers.

20.6.2 Configuring the Supplier

The following configuration steps must be performed by suppliers if they are using Oracle Supplier Network to send the invoice payload.

1. Log in to the Oracle Supplier Network using the registered account.
2. Navigate to Messaging - Communication Parameters and select HTTPS URL Connection as the Delivery Method.
3. Click **Modify** to update the delivery method parameter values.
4. Enter the URL of the B2B HTTP receiver.
5. Enter the User ID and password for Oracle Supplier Network.

> **Note:** You can specify different values for the Test and Production environments.

6. Navigate to Messaging - Transaction Management.
7. Add the OAG PROCESS_INVOICE_002 document from the list of available documents if it is not already added.
8. From the Action drop down list, select Send.
9. From each Delivery Method drop down list (OSN Test Delivery Method and OSN Production Delivery Method), select HTTPS URL Connection and click **Submit**.
10. On the Trading Partners tab, in the Add Trading Partners region, click **Add** to add host company trading partner.

20.7 Setting Up Oracle B2B to Send Receivables Transactions in XML

Oracle B2B Server is an Oracle SOA Suite component that manages interactions between deploying companies and trading partners. Oracle Fusion Receivables supports an outbound Oracle B2B flow using Oracle B2B Server to send transactions to customer trading partners in XML format.

The setup of the Oracle B2B flow for Receivables makes use of these existing elements:

- XML Schema document guideline
- OAG-7.2.1-PROCESS_INVOICE_002-OAG_DEF document definition
- Host trading partner MyCompany

To set up Oracle B2B to send Receivables transactions in XML:

- Configure the host and remote trading partners
- Configure agreements between the host and remote trading partners

20.7.1 Configuring Trading Partners

Configure your enterprise as the host trading partner, and all of your customers that receive XML documents as remote trading partners.

To configure trading partners:

1. Log in to the Oracle B2B Server.
2. Navigate to the Administration page.

3. Click the Document tab.
4. Load the OAG-7.2.1-PROCESS_INVOICE_002-OAG_DEF document definition file.
5. Click the Types tab.
6. Add a new Internal Identifier with the name B2B Trading Partner Code.

   This name matches the field name on the customer account profile.
7. Navigate to the Partners page.
8. In the Partner regional area, select the default host partner MyCompany.
9. If necessary, update the default host partner name to reflect your enterprise.
10. Click the Documents tab.
11. Verify that the OAG-7.2.1-PROCESS_INVOICE_002-OAG_DEF document definition is assigned to the host trading partner.
12. Ensure that the Sender option is enabled.
13. In the Partner regional area, click the Add icon.
14. Enter the name of a remote trading partner.
15. Select the Internal Identifier Type B2B Trading Partner Code that you previously created and enter the Value for the identifier.

    This is the value that you will enter in the B2B Trading Partner Code field on the customer account profile of this remote trading partner.
16. Click the Documents tab.
17. Click the Add icon to associate the OAG-7.2.1-PROCESS_INVOICE_002-OAG_DEF document definition with the remote trading partner.
18. Enable the Receiver option.
19. Click the Channel tab.
20. Define a channel for the remote trading partner.

    The channel determines how the XML transaction is delivered to the remote trading partner from B2B: directly; via the Oracle Supplier Network (OSN), or via a third party.

    If you are communicating using Oracle Supplier Network (OSN), select the Generic Identifier and enter the IP Address of the OSN machine.
21. Repeat steps 13 to 20 for each remote trading partner.

20.7.2 Configuring Agreements

A trading partner agreement defines the terms that enable two trading partners, the sender and the receiver, to exchange business documents. The agreement identifies the trading partners, trading partner identifiers, document definitions and channels.

An agreement consists of two trading partners, the host trading partner and one remote trading partner, and represents one type of business transaction between these partners. For example, if the host trading partner MyCompany and the remote trading partner ABC Solutions regularly exchange both purchase orders and invoices, then two separate agreements are needed for each document definition.

To configure agreements between the host and remote trading partners:

1. Log in to the Oracle B2B Server.
2. Navigate to the Partners page.
3. In the Agreement regional area, click the Add icon to open a new agreement for the host trading partner MyCompany.
4. Enter the agreement ID and Name.
5. Enter the agreement parameters.
6. Select the Document Definition OAG-7.2.1-PROCESS_INVOICE_002-OAG_DEF for this agreement.
7. Select the remote trading partner to include in this agreement.
8. Select the channel for the remote trading partner.
9. Add identifiers for the remote trading partner.
10. Click **Save** to save the agreement.
11. Click **Validate** to validate the agreement.
12. Click **Deploy** to deploy the agreement.

    Deployment is the process of activating an agreement from the design-time repository to the run-time repository.
13. Repeat steps 3 to 12 for each agreement between the host trading partner and this remote trading partner.

20.8 What To Do Next

If you have installed the Fusion Accounting Hub product offering, go to Chapter 21. Otherwise, go to the chapter that corresponds to the product offering that is installed.

21

Completing Oracle Fusion Applications Accounting Hub Post-Installation Tasks

This chapter describes the Oracle Fusion Applications Accounting Hub post-installation tasks you should review and complete before you can start working with your Oracle Fusion Applications Fusion Accounting Hub implementation.

This chapter contains the following section:

21.1 Setting Up the Financial Reporting Center

To setup the Financial Reporting Center, follow the steps detailed in Section 20.1, "Setting Up the Financial Reporting Center."

21.2 Integrating with Other Products

Oracle Fusion Applications provides a coexistence strategy that allows you to continue to use your Oracle E-Business Suite or Oracle PeopleSoft General Ledgers and subledgers while using Oracle Fusion Applications Accounting Hub for financial reporting.

21.2.1 Integrating with Oracle E-Business Suite and Oracle PeopleSoft: Overview

Coexistence includes the ability to transfer balances from the Oracle E-Business Suite General Ledger and journal entries from Oracle PeopleSoft General Ledger to the Oracle Fusion Applications Accounting Hub.

For more information on completing the post-installation setup for coexistence with Oracle E-Business Suite General Ledger see:

- *Configuring Oracle Golden Gate to Integrate the E-Business Suite Ledger with Fusion Accounting Hub* on My Oracle Support.
- *Oracle Fusion Accounting Hub Implementation Guide*
- *Oracle General Ledger Implementation Guide Release 12.2*: This guide contains information about loading and transferring data from Oracle E-Business Suite to the Oracle Fusion Applications Accounting Hub.

For more information on completing the post-installation setup for coexistence with Oracle PeopleSoft General Ledger, see:

- *Oracle Fusion Accounting Hub Implementation Guide*
- *PeopleSoft General Ledger 9.1 Documentation Update: Integrating PeopleSoft General Ledger with Oracle Fusion Accounting Hub*
- *PeopleSoft General Ledger 9.1 Integration to Oracle Fusion Accounting Hub Implementation Guide*

> **Note:** The Oracle Data Integrator (ODI) component (extract file for manual import) is currently available via My Oracle Support only in note id: 1365971.1.

21.2.1.1 Registering Applications Coexistence Instances

Register applications coexistence instances to indicate in Oracle Fusion General Ledger which Oracle E-Business Suite and Oracle PeopleSoft instances are integrated with the Oracle Fusion Applications Accounting Hub. A user interface enables you to perform this registration. For each E-Business Suite or PeopleSoft instance, provide a unique system identifier. This identifier must also be registered in the corresponding Oracle E-Business Suite or Oracle PeopleSoft instance.

You can specify a unique journal source per instance. For Oracle E-Business Suite, you can limit which instance and balancing segments may post to a particular Oracle Fusion General Ledger.

For Oracle E-Business Suite, determine the Function ID to move data from Oracle Fusion General Ledger to Oracle E-Business Suite General Ledger. You must include the Function ID at the end of the drill down URL that is provided during the registration of the Oracle E-Business Suite instance.

To find the Oracle E-Business Suite Function ID:

1. Login as a System Administrator and navigate to the Function page.
2. Query for the function name: GL_FUSION_EBS_DRILL.
3. From the Help menu, click **Diagnostics > Examine**.
4. Select the **FUNCTION_ID** field. The value box shows the value of the Function ID.

For Oracle E-Business Suite: The URL format for the non-dynamic portion needs to be in the following format: `http://<domain>:<port>/OAA_HTML/RF.jsp?function_id=<function_id>`.

In the above URL format, the `domain`, `port`, and `function_id` are for the Oracle E-Business Suite Instance.

For Oracle PeopleSoft: The URL format for the non-dynamic portion needs to be in the following format: `http://server/servlet_name/SiteName/PortalName/NodeName/c/PROCESS_JOURNALS.FUS_DRILLBACK_JRNL.GBL`

In the above URL format:

- `http://server/`: Scheme (http or https) and the web server name.
- `servlet_name/`: Name of the physical servlet that the web server invokes to handle the request.
- `SiteName/`: Site name specified during Oracle PeopleSoft Pure Internet Architecture setup.

- `PortalName/`: Name of the portal to use for this request.
- `NodeName/`: Name of the node that contains the content for this request.

21.2.2 How to Integrate with Data Relationship Management: Overview

Oracle Fusion Applications provides integration between Oracle Fusion Applications Accounting Hub and Oracle Hyperion Data Relationship Management. The integration is included with Oracle Fusion Applications Accounting Hub, Oracle Hyperion Data Relationship Management to store corporate charts of accounts values and hierarchies, and then update this information to both Oracle Fusion Applications Accounting Hub and the Oracle E-Business Suite General Ledger.

For more information on completing the post-installation setup for Data Relationship Management, see the *Oracle Hyperion Data Relationship Management Oracle General Ledger Integration Guide Release 11.1.2.2* on My Oracle Support.

21.2.3 How to Integrate with Hyperion Planning: Overview

For Oracle Cloud implementations, integrate with on-premise Oracle Hyperion Planning for advanced budgeting by loading actual balances from Oracle Fusion Applications Accounting Hub to Oracle Hyperion Planning so you can use the actual data in the budgeting process. You can also load budget data from Oracle Hyperion Planning to Oracle Fusion Applications Accounting Hub through the Budget Interface to perform budget variance reporting within Oracle Fusion Applications Accounting Hub.

For other implementations, Oracle Fusion Applications provides integration between Oracle Fusion Applications Accounting Hub and Oracle Hyperion Planning through Oracle Financial Data Quality Management ERP Integrator adapter. To complete the post-installation setup for the ERP Integrator adapter, see *Oracle Hyperion Financial Data Quality Management ERP Integrator Adapter for Oracle Applications Administrator's Guide*.

21.3 What To Do Next

If you have installed the Oracle Fusion Human Capital Management product offering, go to Chapter 22. Otherwise, go to the chapter that corresponds to the product offering that is installed.

22

Completing Oracle Fusion Human Capital Management Post-Installation Tasks

This chapter describes the Oracle Fusion Human Capital Management (Oracle Fusion HCM) post-installation tasks you should review and complete before you can start working with your Oracle Fusion HCM implementation.

This chapter contains the following sections:

22.1 Recommended Memory Requirement for Oracle Fusion Human Capital Management Workforce Reputation Management Product

This section is only applicable if you plan to use the Oracle Fusion HCM Workforce Reputation Management product packaged with the Workforce Deployment, or Workforce Development product offerings. To provision an environment with these two product offerings, see Section 12.1.2, "Selecting Product Offerings."

The physical machine hosting Oracle Fusion HCM Workforce Reputation Management (WorkforceReputationServer_1) Managed Server must have a minimum of 24 GB of memory. You need to allocate 8 GB of memory to the Oracle Fusion HCM Workforce Reputation Management (WorkforceReputationServer_1) Managed Server. The Oracle Fusion HCM Workforce Reputation Management externalization process may use up to 16 GB of memory.

To specify memory allocation for the Oracle Fusion HCM Workforce Reputation Management (WorkforceReputationServer_1) Managed Server:

1. Edit the `fusionapps_start_params.properties` file located under *`APPLICATIONS_CONFIG`*`/domains/<host>/HCMDomain/config`, by replacing the line:

   ```
   fusion.HCMDomain.WorkforceReputationCluster.default.minmaxmemory.main=-Xms512m -Xmx2048
   ```

   with

   ```
   fusion.HCMDomain.WorkforceReputationCluster.default.minmaxmemory.main=-Xms4096m -Xmx8192m
   ```

2. Save the `fusionapps_start_params.properties` file.

3. Restart Oracle Fusion HCM Workforce Reputation Management (WorkforceReputationServer_1) managed server either from the WebLogic console or Enterprise Management for the Oracle Fusion HCM domain. For more information, see "Chapter 4, Performing Routine Administrative Tasks" in the *Oracle Fusion Applications Administrator's Guide*.

22.2 Setting Up Oracle Fusion Human Capital Management Coexistence

Oracle Fusion HCM Coexistence functionality enables you to integrate your existing Oracle Human Resource applications with a hosted Oracle Fusion HCM implementation. As a result of the integration, you can use Oracle Fusion Workforce Compensation and Talent Management functionality alongside your existing setup.

Using Oracle Fusion HCM Coexistence, you can extract, transform, and transport files from PeopleSoft Enterprise or Oracle E-Business Suite and intelligently synchronize selected business object data between your source application and Oracle Fusion HCM applications. For more information, refer to HCM Coexistence: Explained.

Setting up an implementation of Oracle Fusion HCM for Coexistence with an existing application involves the following procedures.

1. Ensuring that tokens are correctly replaced during Oracle Enterprise Scheduler Service deployment.
2. Setting up an FTP Server.
3. Setting up FTP Accounts.
4. Setting up SOA FTP Adapter.
5. Setting up Oracle Data Integrator.
6. Configuring the Oracle Web Services Manager for Interaction with the Source Application Web Services.
7. Setting up the HCM Configuration for Coexistence Parameters.

These procedures set up the connections in the Oracle Fusion environment to work with the source application. Therefore, you need to set up the connections in the source application as well. The instructions for configuring the source application are in the following documents, which are available on My Oracle Support (MOS):

- Integrating PeopleSoft HRMS 8.9 with Fusion Talent Management and Fusion Workforce Compensation (Document ID 1480967.1)
- Integrating PeopleSoft HRMS 9.0 with Fusion Talent Management and Fusion Workforce Compensation (Document ID 1480995.1)
- Integrating PeopleSoft HRMS 9.1 with Fusion Talent Management and Fusion Workforce Compensation (Document ID 1480996.1)
- HCM Coexistence - Integrating EBS HCM 11i and Fusion Talent Management and Workforce Compensation (Document ID 1460869.1)
- HCM Coexistence - Integrating EBS HCM R12.1 and Fusion Talent Management and Workforce Compensation (Document ID 1460868.1)

22.2.1 Prerequisites

Use Oracle Fusion Applications Provisioning to provision a new Oracle Fusion Applications environment.

In addition to the components installed using Oracle Fusion Applications Provisioning, Oracle Fusion HCM Coexistence requires the following products to be installed.

- Adobe Reader
- Oracle Application Development Framework Desktop Integration (ADFDi)
- Microsoft Office 2007

For more details, see the topic Coexistence for HCM Offering: Overview.

22.2.2 Ensuring Correct Token Replacement During Oracle Enterprise Scheduler Service Deployment

Ensure that Oracle Fusion HCM invokes the following services defined in the Oracle Enterprise Scheduler Service `connections.xml` file for `HcmEssApp`:

- `BulkLoadOdiInvoke` - ODI Agent
- `OdiAgentURLForHCM` - ODI Agent via ODI-ESS bridge
- All entries with the prefix BulkLoad* - HCM product services

Ensure that the service URLs of the entries above are replaced correctly during deployment. Ensure that the Protocol, Host and Port tokens are assigned valid values for the application domain.

22.2.3 Setting Up an FTP Server

Oracle Fusion Applications Provisioning creates an FTP server and installs Oracle WebCenter. Ensure that the server is configured on port 20 and 21 and start the server.

22.2.4 Setting Up FTP Accounts

Create two user accounts with read and write access, a generic user account to configure the FTP adapter and a user specific account for Oracle Fusion Applications.

For example, create user accounts with directory structure and permissions as shown in the following table.

User/ Usage	User Name (OS User)	Password	User Home Directory	Permissions	Comments
BPEL /SOA	`<bpel_username>`	`<bpel_password>`	/fusion	Read and write for current directory and child levels only	User account used with Oracle Fusion SOA FTP Adapter configuration.

User/ Usage	User Name (OS User)	Password	User Home Directory	Permissions	Comments
Customer 1	<customer1_username>	<customer 1-pswd>	/fusion/E_<ENTERPRISE_ID>	Read and write for current directory and child levels only	The <ENTERPRISE_ID> corresponds to the Oracle Fusion Applications ID of Customer 1. The user account is used by the PeopleSoft Enterprise application interaction with the Oracle Fusion SOA/BPEL process.

22.2.5 Setting Up SOA FTP Adapter

Set up the following parameters of the SOA FTP adapter.

- Set the FTP server `hostname` in the FTP adapter connections properties file `weblogic-ra.xml`
- Set the FTP server operating system user name and password

To set the FTP server `hostname` and set the FTP server operating system user name and password in the FTP adapter connections property file, do the following:

1. Access `FtpAdapter.rar` which is available in the **Oracle_SOA1** directory structure on Oracle Weblogic Server (WLS) HcmDomain server file system.
2. Extract and save the `META-INF/weblogic-ra.xml` file to a temporary location.
3. Update the `META-INF/weblogic-ra.xml` file with appropriate values for the following connection properties:
   - `<wls:jndi-name>eis/Ftp/FtpAdapter</wls:jndi-name>`
   - `<wls:name>host</wls:name>`

     `<wls:value>ftpServerHostName</wls:value>`
   - `<wls:name>username</wls:name>`

     `<wls:value>ftpUserName</wls:value>`
   - `<wls:name>password</wls:name>`

     `<wls:value>ftpUserPswd</wls:value>`
4. Create an additional copy of `FtpAdapter.rar`.
5. Update `FtpAdapter.rar` with the updated `META-INF/weblogic-ra.xml` file. Run the following command:

   ```
   zip -ur  /<path>/Oracle_SOA1/soa/connectors/FtpAdapter.rar
   META-INF/weblogic-ra.xml
   ```
6. Bounce the WLS HcmDomain.

22.2.6 Setting Up Oracle Data Integrator

This section describes the prerequisites and steps required for setting up Oracle Data Integrator.

22.2.6.1 Prerequisites

Before setting up Oracle Data Integrator, ensure that you complete the following are set up:

- Oracle Data Integrator code is loaded using XML Import into a copy of the central template repository (id:500) using the FUSION_ODI schema.
- Topology entries are coming from the central template repository.
- Work repository (jdbc) is configured automatically to match the installation.
- Topology Java DataBase Connectivity (JDBC) entries for the database are configured automatically to match the installation.
- Installation uses the default FUSION and FUSION_ODI_STAGE schemas.
- Schemas FUSION and FUSION_ODI_STAGE are installed in the same database.
- The Oracle Data Integrator repository is in the same database as FUSION (schema: FUSION_ODI).
- Default context **Development** is used.
- Oracle Data Integrator console is available for configuration of the topology.

22.2.6.2 Setting Up Oracle Data Integrator for Oracle Fusion Human Capital Management Coexistence

To set up Oracle Data Integrator for Oracle Fusion HCM Coexistence, complete the following procedures.

1. Create Oracle Data Integrator directories.
2. Validate Oracle Data Integrator topology settings.
3. Verify the configuration of the work repository.
4. Verify database connections.
5. Configure file technology connections.

22.2.7 Creating Oracle Data Integrator Directories

You must manually create and specify the directories and files to which Oracle Data Integrator has read and write access.

- For each enterprise, create an enterprise folder in the work directory.
- For the operating system user of the Oracle Data Integrator agent, create or specify directories for the items listed in the following table for Oracle Data Integrator use. The users must have full read and write access to the directories.

Oracle Data Integrator Directory Name	Item Description	Example Values
FILE_ROOT_HCM	Oracle Data Integrator base work directory	/home/ODI_ROOT_DIRECTORY
FILE_OUTPUT_HCM	Oracle Data Integrator export work directory	/home/ODI_ROOT_DIRECTORY/export
N/A	Enterprise directory name, where <eid> is the numeric enterprise id	/home/ODI_ROOT_DIRECTORY/E_<eid>

Note: While creating the directory, ensure that the owner of the directory and the operating user of the Oracle Data Integrator agent are the same. The directory should be accessible from the Oracle WebLogic Server domain that runs the Oracle Data Integrator agent and the SOA process.

22.2.8 Validating the Topology Settings

After you have created the directories, use either Oracle Data Integrator Studio or Oracle Data Integrator Repository Explorer to validate the Oracle Data Integrator topology settings.

Configure or validate the following:

- Work repository connection
- Oracle technology (database) connections
- File technology connections

Note: Use JDBC connection and credentials to validate and ensure that the connections refer to the correct database.

22.2.9 Verifying the Configuration of the Work Repository

Use Oracle Data Integrator Studio to verify the work directories and repository configuration.

1. Navigate to **Topology** > **Repositories** > **Work Repositories**.
2. Double-click **FUSIONAPPS_WREP**.
3. Verify that the work repository (jdbc URL) points to your Oracle Fusion Applications database.

22.2.10 Verifying Database Connections

Verify that the JDBC data server URLs point to the Oracle Fusion Applications database.

1. Navigate to **Topology** > **Physical Architecture** - **Oracle**.
2. Double-click the **ORACLE_FUSION** data server.
3. On the Definitions page, verify that the **Connection User** is FUSION_ODI_STAGE.
4. Enter the password.
5. In the **Instance/db link (Data Server)** field, enter the instance for the Oracle Fusion Applications database.

   Use the following format if the instance name is not registered with the Transparent Network Substrate (TNS) service: `<host>:<port>/<instance_name>`. If the instance name is registered with the TNS service, specify only the instance name.
6. Click **JDBC**.
7. Ensure that the URL in the **JDBC URL** field points to the Oracle Fusion Applications database.

8. Expand and open the child schema: **ORACLE_FUSION.FUSION**.
9. Ensure that the **Default** box is selected.
10. Verify that FUSION is entered as the value in the **Schema** field.
11. Verify that FUSION_ODI_STAGE is entered as the value in the **Work Schema** field.

> **Note:** Perform the same steps for the ORACLE_WORK_HCM data server. However, ensure that the value of both the schema and the work schema is FUSION_ODI_STAGE.

22.2.11 Configuring File Technology Connections

The ODI work directories that you defined now need to be configured in the topology so that ODI can make use of them.

Using ODI Studio, configure files in topology.

1. Navigate to **Topology** > **Physical Architecture** - **File**.
2. Double-click FILE_ROOT_HCM.
3. Verify that the value of **JDBC Driver** is com.sunopsis.jdbc.driver.file.FileDriver.
4. Verify that the value of **JDBC URL** is jdbc:snps:dbfile.
5. Expand and open the child physical schema.
6. For **Directory (Schema)**, provide the directory path that you defined for FILE_ROOT_HCM.
7. Provide the same value for **Directory (Work Schema)**.
8. Ensure that the **Default** box is selected.

Use the same steps to configure FILE_OUTPUT_HCM using the directory path for FILE_OUTPUT_HCM instead of FILE_ROOT_HCM.

22.2.12 Enabling SQL*Loader for Oracle Data Integrator

Oracle Fusion HCM Coexistence Oracle Data Integrator uses SQL*Loader to import file data. Use the SQL*Loader in Oracle Data Integrator from the Oracle Weblogic Server environment to perform the following steps.

1. Determine the directory where the Oracle client software is installed for your deployment. The default name is `DBCLIENT` and it is placed in the parent directory of *MW_HOME*. You can refer to this directory as `DBCLIENT ORACLE_HOME`.
2. Verify the existence of `DBCLIENT ORACLE_HOME/bin/sqlldr`.
3. Change the directory to *ODI ORACLE_HOME*`/bin`.
4. Create a script named `sqlldr` that contains the following:

```
#!/bin/sh
ORACLE_HOME=<DBCLIENT ORACLE_HOME>
export ORACLE_HOME
$ORACLE_HOME/bin/sqlldr $*
#
```

5. Make the script executable using the following command.

```
chmod +x sqlldr
```

22.2.13 Configuring the Oracle Web Services Manager for Interaction with the Source Application Web Services

Configure the Oracle Web Services Manager certificate key with the user credentials for a Simple Object Access Protocol (SOAP) interaction with the source application Web services.

The user credentials correspond to the source application user with entitlement to invoke the source application Web service.

1. Log in to the Enterprise Manager Console as a Weblogic_Administrator user.
2. Access **HcmDomain** under the Weblogic Domain.
3. Open **Security** - **Credentials**.
4. Access and expand the key map oracle.wsm.security.
5. Click **Credential Key** to search for the key `FUSION_APPS_HCM_HR2HR_APPLOGIN-KEY`.
6. Click **Edit** to update the credentials.
7. Set the user name and password of the source application user.

22.2.14 Setting up the HCM Configuration for Coexistence Parameters

After you have created the FTP and Oracle Data Integrator directory paths, you need to set up the related parameters in Oracle Fusion HCM.

1. Log in to Oracle Fusion Applications.

   Note: The Oracle Fusion Applications user must have the appropriate roles to set up and configure Oracle Fusion applications. At least, ensure that the user is assigned the **View All** data role for the **HCM Application Administrator** job role. For details on setting up implementation users, refer to the HCM Coexistence Implementation Guide.

2. Go to **Navigator** - **Tools** - **Setup and Maintenance** and perform the following tasks:
   1. Find and initiate the **Manage HCM Configuration for Coexistence** task to bring up the **Manage HCM Configuration for Coexistence** parameters page.
   2. Set up the following parameters.

Parameter	Description
On Demand FTP Root Directory	Mounted root directory of the server
ODI Context	The logical name for the group containing logical-to-physical mappings for connections in Oracle Data Integrator. The default value in Oracle Data Integrator is DEVELOPMENT. This value is case sensitive. Therefore, ensure that it is completely uppercase.
ODI User	The Oracle Data Integrator user name

Parameter	Description
ODI Password	The password associated with the Oracle Data Integrator user name
ODI Work Repository	The repository that contains the Oracle Data Integrator related code definitions. The default value in Oracle Data Integrator is FUSIONAPPS_WREP.
ODI Root Directory	The local directory where Oracle Data Integrator processes files and creates work and log files. It is the directory path defined for FILE_ROOT_HCM, when creating the Oracle Data Integrator directories.

You are now ready to implement Oracle Fusion Talent and Oracle Fusion Workforce Compensation using the Coexistence for HCM offering, available from the Setup and Maintenance work area of Oracle Fusion Applications.

22.3 Creating an ISAM Vertex Database

To successfully run the US Payroll, you need to create an Indexed Sequential Access Method (ISAM) database using the data file provided by Vertex. Once the ISAM database is created, you need to process the data file each month to maintain accurate payroll results. Vertex makes the data file available on a monthly basis.

22.3.1 Creating an ISAM Database for Microsoft Windows

To create the ISAM database for Applications running on Windows, follow these instructions.

1. In the `environment.properties` file, ensure that the *$VERTEX_TOP* variable is set for the appropriate environment.
2. Copy the utility and library files under *$VERTEX_TOP*`/utils` and *$VERTEX_TOP*`/lib` and place them in a Windows local directory, such as `C:\Vertex_Util-Lib`.
3. Copy the latest Vertex data file (`qfpt.dat`) to the local directory where you want to create the ISAM database, such as `C:\Vertex_Data`.
4. From the local directory containing the utilities and library files (in this case `C:\Vertex_Util-Lib`), run `cbmaint`.
5. On the installer screen, select **Create Database** and **Payroll Tax Database**.
6. Provide the local directory path where you want to created the ISAM database (in this case, `C:\Vertex_Data`). The ISAM database files get created in this directory.
7. From the local directory containing the utilities and library files (in this case `C:\Vertex_Util-Lib`), run `vprtmupd` to populate the ISAM database files.
8. On the Installer screen, select **Update Payroll Tax Database**.
9. Provide the local directory path where the Vertex data file `qfpt.dat` is available (in this case `C:\Vertex_Data`).
10. Provide the directory path where ISAM database was created (in this case `C:\Vertex_Data`). The ISAM database files residing in this directory get updated. The update process takes some time.
11. Backup the database file and the related files under *$VERTEX_TOP*`/data`, if any, in case there is a need to revert to the earlier ISAM database.

12. Copy the ISAM database files and all related files from the local directory (in this case `C:\Vertex_Data`), and place then under *$VERTEX_TOP*`/data`.
13. Provide users with complete permissions to all files under *$VERTEX_TOP*`/data`.

The ISAM database is available for use by the US Payroll application.

22.3.2 Creating an ISAM Database for UNIX

To create the ISAM database for application running on UNIX, follow these instructions.

1. Set the appropriate environment variable (for the given platform) as the value of *$VERTEX_TOP*`/lib`, as per the following specification:

Table 22–1 ISAM Environmental Variables for UNIX Systems

UNIX System	Environment Variable
AIX	LBPATH
HP-UX 11.11	SHLIB_PATH
Others	LD_LIBRARY_PATH

2. Backup the database file and the related files under `$VERTEX_TOP/data`, if any, in case there is a need to revert to the earlier ISAM database.
3. Copy the latest Vertex data file (`qfpt.dat`) to `$VERTEX_TOP/data`.
4. From *$VERTEX_TOP*`/utils`, run `cbmaint`.
5. On the installer screen, select **Create Database** and **Payroll Tax Database**.
6. Provide the directory path where you want to create the ISAM database (in this case *$VERTEX_TOP*`/data`). The ISAM database files get created in this directory.
7. From the *$VERTEX_TOP*`/utils`, run `vptmupd` to populate the ISAM database files.
8. On the Installer screen, select **Update Payroll Tax Database**.
9. Provide the directory path where the Vertex Data file `qfpt.dat` is available (in this case *$VERTEX_TOP*`/data`).
10. Provide the directory path where ISAM database was created (in this case *$VERTEX_TOP*`/data`). The ISAM database files residing in this directory get updated. The update process takes some time.
11. Provide users with complete permissions ot all files under *$VERTEX_TOP*`/data`.

The ISAM databse is available for use by the US Payroll application.

22.3.3 Updating the Vertex Data File for US Tax Information

In order for your installation to successfully run Oracle Fusion Payroll for the US, you must process the Vertex `qfpt.dat` data file to create an Indexed Sequential Access Method (ISAM) database. Vertex publishes and delivers this data file on a monthly basis to its customers, so you must perform the database creation regularly.

You can perform this operation in a Windows or UNIX environment.

22.3.3.1 Generating the Vertex ISAM Database for Windows

1. Set the *$VERTEX_TOP* enviornmental variable in the `environment.properties` file.

2. Copy the files in *$VERTEX_TOP*/utils and *$VERTEX_TOP*/lib into a local directory. Perform this step only after applying an Oracle update that includes a new version of Vertex.
3. Execute cbmaint.exe from the Vertex local directory.
4. Select **Create Database**.
5. Select **Payroll Tax Database**.
6. Type the directory path where you want to create the ISAM database (*$VERTEX_TOP*/data).
7. Execute vprtmupd.exe to populate the ISAM database files.
8. Select **Update Payroll Tax Database**.
9. Enter the directory path where the Vertex data file qfpt.dat is located.
10. Enter the direcotry location you chose for your ISAM database (Step 6).
11. Copy all files of the newly created ISAM database into *$VERTEX_TOP*/data.

22.3.3.2 Generating the Vertex ISAM Database for UNIX

1. Set up the environmental variable for shared libraries to *$VERTEX_TOP*/lib. This varies according to your UNIX operating system.

Table 22–2 ISAM Environmental Variables for UNIX Systems

Operating System	System Environmental Variable
AIX	LIBPATH
HP-UX 11.11	SHLIB_PATH
All others	LD_LIBRARY_PATH

2. Execute cbmaint.exe from *$VERTEX_TOP*/utils.
3. Select **Create Database**.
4. Select **Payroll Tax Database**.
5. Type the directory path where you want to create the ISAM database (*$VERTEX_TOP*/data).
6. Run vprtmupd.exe to populate the ISAM database files.
7. Select **Update Payroll Tax Database**.
8. Enter the directory path where the Vertex data file qfpt.dat is located.
9. Enter the directory location you chose for your ISAM database (Step 5).
10. Copy all files of the newly created ISAM database *$VERTEX_TOP*/data.

22.4 What To Do Next

If you have installed the Oracle Fusion Incentive Compensation product offering, go to Chapter 23. Otherwise, go to the chapter that corresponds to the product offering that is installed.

23

Completing Oracle Fusion Incentive Compensation Post-Installation Tasks

This chapter describes the Oracle Fusion Incentive Compensation post-installation tasks you should review and complete before you can start working with your Oracle Fusion Incentive Compensation implementation.

This chapter contains the following sections:

23.1 Integrating Oracle Fusion Incentive Compensation with Geo Map Server

Oracle Fusion Incentive Compensation uses the functionality provided by the Geo Map server. Depending on the network connectivity where the application is installed and the available support for integration, you may have to modify the MapViewer and GeoMapViewer connections.

If you intend to use the map server provided by Oracle, you must connect to `http://elocation.oracle.com`.

> **Note:** If the firewall on your network blocks HTTP connections, you cannot access the map server.

If you intend to use your preferred map server or any other map server that is available on premise or on another network, you must modify certain Oracle Application Development Framework (Oracle ADF) connection properties for MapViewer and GeoMapViewer.

1. Log in to Oracle Enterprise Manager Fusion Applications Control.
2. In the left pane, navigate to **Oracle Fusion Incentive Compensation** > **Fusion Applications** > **IncentiveCompensationApp** and click the server for which you want to modify the ADF connection properties.
3. At the top of the page, from the **Fusion J2EE Application** context menu, select **ADF** > **Configure ADF Connections**.
4. On the ADF Connections Configuration page, go to the **URL Connections** section.
5. Select the **MapViewerURL** connection name and click **Edit**.

6. In the URL field, replace the default URL with the URL or location information of your preferred map server and click **OK**.
7. Repeat the steps to modify the URL for the **GeoMapViewer** connection name.

23.2 What to Do Next

If you have installed an Oracle Fusion Project Portfolio Management product offering, go to Chapter 24. Otherwise, go to the chapter that corresponds to the product offering that is installed.

24

Completing Oracle Fusion Project Portfolio Management Post-Installation Tasks

This chapter describes the Oracle Fusion Project Portfolio Management post-installation tasks you should review and complete before you can start working with your Oracle Fusion Project Portfolio Management implementation.

This chapter contains the following sections:

24.1 Configuring Oracle Fusion Project Portfolio Management Integration with Primavera P6 Enterprise Project Portfolio Management

Use Oracle Fusion Project Integration Gateway to integrate Oracle Fusion Project Portfolio Management with Primavera P6 Enterprise Project Portfolio Management. The integration enables project accountants, project billing specialists, and executives to centrally perform project costing, billing, accounting, and executive reporting tasks in Oracle Fusion Project Portfolio Management while enabling each project manager to perform detailed project planning and scheduling in Primavera P6 Enterprise Project Portfolio Management.

24.1.1 Configuring Oracle Fusion Project Portfolio Management Integration With P6 Enterprise Project Portfolio Management

To configure Oracle Fusion Project Portfolio Management Integration with Primavera P6 Enterprise Project Portfolio Management, complete the following tasks:

1. Install Primavera P6 Enterprise Project Portfolio Management and configure Oracle Fusion Project Portfolio Management Bridge.

   For more information on installing Primavera P6 integration with Oracle Fusion Project Portfolio Management and working with Oracle Fusion Project Portfolio Management Bridge, see *Primavera P6 EPPM Administrator's Guide for an Oracle Database*.

2. Configure the Oracle Fusion Project Portfolio Management environment.

   a. Verify that a `FUSION_APPS_PRJ_P6INT_ADMIN-KEYoracle.wsm.security` credential key is defined for the `ProjectsDomain` in Oracle Fusion Project Portfolio Management.

For the FUSION_APPS_PRJ_P6INT_ADMIN-KEY key, ensure that the user name and password match the user name and password of the P6 administration super user designated for use with the integration between Oracle Fusion Project Portfolio Management and Primavera P6 Enterprise Project Portfolio Management.

b. Create a user named FUSION_P6_PROJECT_INTEGRATION_USER.

c. Register the Primavera P6 Endpoint address details in Oracle Fusion Functional Setup Manager.

a. Navigate to **Topology Registration > Register Enterprise Applications** and add the following enterprise application:

Enterprise Application: PJGP6 Primavera Application

Name: PJGP6_Primavera1

b. Enter the host and port server details where the P6 integration service is deployed:

Server Protocol: http

External Server host: <host of the P6 integration service>

External Server port: <port of the P6 integration service>

24.2 What to Do Next

If you have installed the Oracle Fusion Supply Chain Management product offering, go to Chapter 25. Otherwise go to Chapter 26 to complete the required functional and implementation tasks before you can start using your Oracle Fusion Applications setup.

25

Completing Oracle Fusion Supply Chain Management Post-Installation Tasks

This chapter describes the Oracle Fusion Supply Chain Management post-installation tasks you should review and complete before you can start working with your Oracle Fusion Supply Chain Management implementation.

This chapter contains the following sections:

25.1 Installing Oracle Enterprise Data Quality for Product Data Oracle DataLens Server

Oracle Enterprise Data Quality for Product Data is built on industry-leading DataLens Technology to standardize, match, enrich, classify, and correct product data from different sources and systems. For Oracle Fusion Product Hub to use Oracle Enterprise Data Quality for Product Data features, you must establish a connection between them.

For more information on installing and using Oracle Enterprise Data Quality for Product Data Oracle DataLens Server, see the *Oracle Enterprise Data Quality for Product Data Oracle DataLens Server Installation Guide*. For more information on implementation, see *Oracle Enterprise Data Quality for Product Data R12 PIM Connector Installation Guide*.

25.1.1 Establishing a Connection

After installation, use the Oracle Enterprise Manager to establish or modify the connection with the Oracle DataLens Server.

1. Log in to an Oracle Fusion Middleware farm using Oracle Enterprise Manager Fusion Applications Control.
2. Expand the Fusion Applications node under Oracle Fusion Supply Chain Management.
3. Right-click the application for which a connection will be established, for example, **ProductManagementApp**.
4. Select **ADF** > **Configure ADF Connections** from the menu.
5. On the ADF Connections Configuration page, set the connection type as `URL` and the connection name as `DSAServerURL`.

6. Click **Create Connection**. The added connection appears under URL Connections.
7. Under URL Connections, select **Edit** `DSAServerURL` and provide the **URL** for Oracle DataLens Server.

   For example, the SOA Common Properties Server URL with `/datalens` appended to the URL such as `http://<host name>:port/datalens`.
8. Click **OK**.
9. Click **Apply**.
10. Set connections for **ProductManagementCommonApp** and **ScmEssApp** applications using Step 3 to Step 10.
11. For the changes to take effect, restart the Product Management, SCM Common, and ESS servers from the Weblogic Admin Console.

25.2 What to Do Next

Go to Chapter 26 which describes the next steps to be completed.

26

What To Do Next

This chapter describes implementation and functional tasks you must complete before you can start using your Oracle Fusion Applications setup.

This chapter contains the following sections:

26.1 Introduction

Your new Oracle Fusion Applications environment is complete and operational. You must now perform the necessary implementation and functional setup tasks.

26.2 Managing User Passwords for Login Access to Applications Components

For complete information about setting up and managing passwords for your new environment, see "Securing Oracle Fusion Applications" and "Provisioning Identities" in *Oracle Fusion Applications Administrator's Guide*.

26.3 Completing Common User Setup Tasks

For complete information about completing common user setup tasks needed to create an implementation project, optionally create initial implementation users, and set up the basic enterprise structure needed for implementing any and all Oracle Fusion Applications offerings see the *Getting Started with Oracle Fusion Applications: Common Implementation* posted on My Oracle Support (Doc ID 1387777.1).

26.4 Enabling Product Offering Functionality

Before you can start using any of the product offerings you have installed, you must complete some common implementation tasks and enable the functionality of the offerings in your environment.

A large library of product-related documentation is available for use after provisioning. Some of the guides that you will find useful are listed here:

- *Oracle Fusion Functional Setup Manager User's Guide*
- Product-specific Oracle Fusion Applications implementation guides

26.5 Troubleshooting Tips for Runtime Issues

Follow the instructions detailed in this section for resolving known runtime issues.

26.5.1 OutOfMemory Error Due to PermGen Space (Solaris)

Problem: An OutOfMemoryError due to PermGen space is reported on the SCMCommon WebLogic Managed Server in the Oracle Fusion Supply Chain Management domain for the Solaris x64 or Solaris Sparc platform.

Solution for Solaris x64

Perform the following steps to resolve this issue on the Solaris x64 platform.

1. Check the cluster name for the managed server where the PermGen exception is reported. The cluster name can be found from the Administration Server console for the Oracle Fusion Supply Chain Management domain.
2. Edit the *$DOMAIN_HOME*`/config/fusionapps_start_params.properties` file by performing the following steps.
   a. Identify the key/value pair which is `fusion.SCMCommonCluster.SunOS-i386.memoryargs` in `fusionapps_start_params.properties`.
   b. Duplicate the entire line containing the key/value pair of `fusion.SCMCommonCluster.SunOS-i386.memoryargs` and add this as a new line in `fusionapps_start_params.properties`.
   c. Comment the original line by adding a '#' at the beginning of the line.
   d. For the line added in **Step b**, change the default value in `fusion.SCMCommonCluster.SunOS-i386.memoryargs` by replacing 512m with 756m. This is what it should look like:

```
fusion.SCMCommonCluster.SunOS-i386.memoryargs=-XX:PermSize=256m
-XX:MaxPermSize=756m -XX:+UseParallelGC
-XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=@HEAP_DUMP_PATH@
-XX:+ParallelGCVerbose -XX:ReservedCodeCacheSize=128m
-XX:+UseParallelOldGC -XX:ParallelGCThreads=4
```

   e. Bounce the Managed Server.

An example for `SCMCommonServer_1` for Solaris x64 follows.

1. `SCMCommonCluster` is the cluster name for `SCMCommonServer_1`.
2. Add the following entry:

```
fusion.SCMCommonCluster.SunOS-i386.memoryargs=-XX:PermSize=256m
-XX:MaxPermSize756m -XX:+UseParallelGC
 -XX:+HeapDumpOnOutOfMemoryError
-XX:HeapDumpPath=path_for_heap_dump -XX:+ParallelGCVerbose
-XX:ReservedCodeCacheSize=128m -XX:+UseParallelOldGC
```

```
-XX:ParallelGCThreads=4
```

In this example, the entry for `fusion.default.SunOS-i386.memoryargs` is already correct.

Solution for Solaris Sparc

Perform the following steps to resolve this issue on the Solaris Sparc platform.

1. Check the cluster name for the managed server where the `PermGen` exception is reported. The cluster name can be found from the Administration Server console for the Oracle Fusion Supply Chain Management domain.
2. Edit the *$DOMAIN_HOME*`/config/fusionapps_start_params.properties` file by performimg the following steps.
   a. Identify the key/value pair which is `fusion.SCMCommonCluster.SunOS-sparc.memoryargs` in `fusionapps_start_params.properties`.
   b. Duplicate the entire line containing the key/value pair of `fusion.SCMCommonCluster.SunOS-sparc.memoryargs` and add this as a new line in `fusionapps_start_params.properties`.
   c. Comment the original line by adding a '#' at the beginning of the line.
   d. For the line added in **Step b**, change the default value in `fusion.SCMCommonCluster.SunOS-sparc.memoryargs` by replacing 512m with 756m. This is what it should look like:

```
fusion.SCMCommonCluster.SunOS-sparc.memoryargs=-XX:PermSize=256m
-XX:MaxPermSize=756m -XX:+UseParallelGC
-XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=@HEAP_DUMP_PATH@
-XX:+ParallelGCVerbose -XX:ReservedCodeCacheSize=128m
-XX:+UseParallelOldGC -XX:ParallelGCThreads=4
```

   e. Bounce the Managed Server.

An example for `SCMCommonServer_1` for Solaris Sparc follows.

1. `SCMCommonCluster` is the cluster name for `SCMCommonServer_1`.
2. Add the following entry:

```
fusion.SCMCommonCluster.SunOS-sparc.memoryargs=-XX:PermSize=256m

-XX:MaxPermSize756m -XX:+UseParallelGC

-XX:+HeapDumpOnOutOfMemoryError

-XX:HeapDumpPath=path_for_heap_dump -XX:+ParallelGCVerbose

-XX:ReservedCodeCacheSize=128m -XX:+UseParallelOldGC

-XX:ParallelGCThreads=4
```

In this example, the entry for `fusion.default.SunOS-sparc.memoryargs` is already correct.

26.6 (Optional) Installing Oracle Enterprise Manager Cloud Control

Oracle Enterprise Manager Cloud Control (Cloud Control) is a system management software that delivers centralized monitoring, administration, and life cycle management functionality for the complete Oracle Fusion Applications IT

infrastructure from one single console. For example, you can monitor all the Oracle WebLogic Server domains for all the product families from one console.

See the following documentation to install Cloud Control:

- *Oracle Enterprise Manager Cloud Control Basic Installation Guide*
- *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*

Part VIII

Uninstalling Oracle Fusion Applications

This part describes uninstalling Oracle Fusion Applications.

Part VIII contains the following chapters:

27

Uninstalling an Oracle Fusion Applications Environment

This chapter describes the actions necessary to remove an existing Oracle Fusion Applications environment from your system. It includes step-by-step instructions and provides important information about the ramifications of taking this action.

This chapter includes the following sections:

27.1 Introduction to Uninstalling an Oracle Fusion Applications Environment

During the uninstallation process, components that were installed using the Provisioning Wizard are removed. The Oracle Fusion Applications database and the Oracle Identity Management components are not removed. To remove the Oracle Fusion Applications database, see Section 27.7, "Deleting the Database". The Oracle Identity Management environment, including the Oracle Identity Management databases is not removed.

Note the following characteristics of the uninstallation process:

- You must run the `deinstall` process on *all* hosts. Use the Provisioning Wizard `deinstall` option for the Primordial host, and the command line option for the Primary host and Secondary host. *Products installed from the command line must be deinstalled from the command line.*
- Start the Provisioning Wizard on the same host (primordial) where you started it at the time of installation. You can monitor the process on all hosts using the primordial host interface.
- All binaries, regardless of patch level, are removed.

Note: You cannot partially uninstall an environment by selecting specific components to uninstall.

27.2 Prerequisites to Uninstalling an Oracle Fusion Applications Environment

Always use the provisioning `deinstall` option (the Provisioning Wizard option or the command line) rather than simply deleting the *`APPLICATIONS_BASE`*, *`APPLICATIONS_CONFIG`*, and the `oraInventory` directories manually. This is especially important for the web tier. Two of its instances share the same `oraInventory` location.

Before you begin the uninstallation process, complete these tasks:

1. Stop any processes that are running in the environment.
2. Shut down all Managed Servers, the Administration Server, and the Node Manager on all hosts. If the servers are configured as Windows services, stop the services before deinstalling the software. See "Stopping an Oracle Fusion Applications Environment" in *Oracle Fusion Applications Administrator's Guide*.
3. Stop Oracle HTTP Server with this command: *`APPLICATIONS_CONFIG`*`/CommonDomain_webtier/bin/opmnctl shutdown`.
4. Stop the Oracle Business Intelligence components that are controlled by Oracle Process Manager and Notification Server with this command: *`APPLICATIONS_CONFIG`*`/BIInstance/bin/opmnctl shutdown`. See "Using the OPMN Command Line to Start, Stop, Restart, and View the Status of System Components" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* for more information.
5. Shut down Global Order Promising (GOP) (if provisioned):

   UNIX: *`APPLICATIONS_CONFIG`*`/gop_1/bin/opmnctl shutdown`. To remove the Windows service, run: `sc delete GlobalOrderPromisingServer1`.
6. Stop the Java EE components using Oracle Enterprise Manager Fusion Middleware Control. See "Starting and Stopping Java EE Applications Using WLST" in *Oracle Fusion Applications Administrator's Guide*.
7. Shut down Informatica Identity Resolution (IIR) (if provisioned) by running these commands *in the order listed*:

   a. *`APPLICATIONS_BASE`*`/informaticaIR/bin/idsdown`

   b. *`APPLICATIONS_BASE`*`/informaticaIR/bin/lidown`

See "Starting and Stopping Components in the Oracle Fusion Applications Environment" in the *Oracle Fusion Applications Administrator's Guide* for more information.

27.3 Uninstalling Oracle Fusion Applications Using the Provisioning Wizard

To perform an uninstallation using the Provisioning Wizard, start the wizard from the primordial host and complete the uninstallation interview screens.

27.3.1 Starting the Provisioning Wizard

To start the Provisioning Wizard, do the following from the primordial host:

1. Set the *JAVA_HOME* environment variable to point to the JDK location in the provisioning repository, for example:

   UNIX:

   ```
   export JAVA_HOME=REPOSITORY_LOCATION/jdk6
   export PATH=$JAVA_HOME/bin:$PATH
   ```

   AIX:

   ```
   export JAVA_HOME=REPOSITORY_LOCATION/jdk6
   export PATH=$JAVA_HOME/bin:$PATH
   export SKIP_ROOTPRE=TRUE
   ```

   Windows:

   ```
   set JAVA_HOME=REPOSITORY_LOCATION\jdk6
   set PATH=%JAVA_HOME%\bin;%PATH%
   ```

2. Verify that the LIBPATH value is null.
3. Run the following command on the primordial host:

   UNIX:

   ```
   cd FAPROV_HOME/provisioning/bin
   ./provisioningWizard.sh
   ```

   On Solaris, use `bash provisioningWizard.sh` instead of `./provisioningWizard.sh`.

   Windows:

   ```
   cd FAPROV_HOME\provisioning\bin
   provisioningWizard.bat
   ```

27.3.2 Wizard Interview Screens and Instructions

Table 27–1 shows the steps necessary to uninstall an Oracle Fusion Applications environment with the Provisioning Wizard. For help with any of the interview screens, click **Help** on any Provisioning Wizard interview screen.

Note: If you do not input the correct values required, the error and warning messages are displayed at the bottom of the screen.

Table 27–1 Deinstalling an Oracle Fusion Applications Applications Environment

Screen	Description and Action Required
Welcome	No action is required on this read-only screen. Click **Next** to continue.
Specify Central Inventory Location	This screen displays only if one or more of the following conditions are not met: ■ The `-invPtrLoc` option is used to specify the central inventory location on non-Windows platforms, so the default value for your platform is not used. Note that the default for Linux and AIX platforms is `/etc/oraInst.loc` and for Solaris and HP, it is `/var/opt/oracle/oraInst.loc`. ■ The Central Inventory Pointer File is readable. ■ The Central Inventory Pointer File contains a value for `inventory_loc`. ■ The `inventory_loc` directory is writable. ■ The `inventory_loc` directory has at least 150K of space. ■ `inventory_loc` is not a file. Specify the location of the **Central Inventory Directory** that meets the previous criteria. The `inventory_loc` directory can be created by the `createCentralInventory.sh` script and does not have to exist at the time you specify its location. For non-Windows platforms, in the **Operating System Group ID** field, select or enter the group whose members will be granted access to the inventory directory. All members of this group can install products on this host. Click **OK** to continue. The **Inventory Location Confirmation** dialog prompts you to run the *`inventory_directory`*`/createCentralInventory.sh` script as root, to confirm that all conditions are met and to create the default inventory location file, such as `/etc/oraInst.loc`. After this script runs successfully, return to the interview and click **OK** to proceed with the installation. If you do not have root access on this host but want to continue with the installation, select **Continue installation with local inventory** and click **OK** to proceed with the installation. For Windows platforms, this screen displays if the inventory directory does not meet requirements. For more information about inventory location files, see "Oracle Universal Installer Inventory" in the *Oracle Universal Installer and OPatch User's Guide*. Click **Next** to continue.
Installation Options	Presents a list of valid installation actions that you can perform using the Provisioning Wizard. Select **Deinstall an Applications Environment**. Enter the directory path in the **Response File** field to the response file associated with the environment you want to deinstall. Or click **Browse** to navigate to the response file location. Click **Next** to continue.

Table 27–1 (Cont.) Deinstalling an Oracle Fusion Applications Applications Environment

Screen	Description and Action Required
Summary	Displays the application and middleware components to be uninstalled. The processes associated with these components must be shut down manually. See Section 27.2 for details. Click **Deinstall** to begin uninstalling the applications and middleware components.
Deinstallation Progress	The uninstallation process runs on the primordial host. You must uninstall from the command line on any primary or secondary hosts provisioned in your environment. See Section 27.4 for more details. The following symbols help track the deinstall progress: ■ **Block**: Processing has not yet started on this host for the named phase. ■ **Clock**: Performing the build for a phase. ■ **Check mark**: The build was completed successfully. ■ **x** mark: The build has failed for this phase. You must correct the errors before you can continue. ■ **Restricted** symbol: The validation process has stopped due to a failure within another process. Click an **x** or a **Restricted** symbol to display information about failures. Select the icon in the **Log** column to view host-level details. If there is a **Log** file icon beside a build message, you can select that file to see the details of that build. If the uninstallation fails, a **Retry** button is enabled, allowing you to try the uninstall again. See Section 14.4, "Recovery After Failure" for information about retry, cleanup, and restore actions. Click **Next** to continue.
Deinstallation Complete	Review the list of components removed from this environment. Click **Save** to create a text file that contains the details. See Section 27.5 for information about manual tasks necessary to complete the uninstallation process. Click **Finish** to dismiss the screen.

27.4 Uninstalling Oracle Fusion Applications From the Command Line

If you have provisioned a primary or secondary host, you must run the `deinstall` command on those hosts from the command line, using the same procedure that you used during provisioning. If the primordial host is no longer available, the entire uninstall process must be run from the command line.

Run the `deinstall` command as `root` (with administration privileges) as follows:

UNIX: `runProvisioning.sh -responseFile` *`response_file_location`* `-target deinstall`

Windows: `runProvisioning.bat -responseFile` *`response_file_location`* `-target deinstall`

If the web tier has been deployed in a DMZ, you must run the Oracle Universal Installer (OUI) manually on that host to deinstall. See *Oracle Universal Installer and OPatch User's Guide*.

27.5 Cleaning Up After Uninstalling Oracle Fusion Applications

The remaining cleanup tasks are as follows:

UNIX:

1. If you set up processes to run as a service, verify the */etc/services* file and remove the corresponding entries from the file.
2. If you set up processes to run as a service, verify the */etc/inetd.conf* file and remove the corresponding process entries from the file.

3. Clean up or remove the *APPLICATIONS_BASE* directory.
4. Clean up or remove the application configuration (*APPLICATIONS_CONFIG*) directory. If you enable local application configuration, you should also clean up or remove the local application configuration directories.

Windows:

1. Remove Program Groups. You must also remove Program Groups from the `Start Menu\Programs` folder.
2. Reboot your system after you have finished removing all programs.

Note: Deinstalling Oracle Fusion Applications does not remove the `beahomelist` file or the `bea` directory under:

UNIX: `user_home/bea/beahomelist`

Windows: `C:\bea\beahomelist`

For information about how this file is used, see "Backup Artifacts" and "Updating Oracle Inventory" in the *Oracle Fusion Middleware Administrator's Guide*.

27.6 Uninstalling Oracle Identity Management

Follow these instructions to clean up an Oracle Identity Management provisioned environment, before starting another round of provisioning.

Linux or UNIX:

1. On each host, kill all Oracle Identity Management processes. Restarting the host is recommended.
2. On each host, delete the contents of the directory `IDM_LOCAL_CONFIG`.
3. Delete the contents of the directories `IDM_BASE` and `IDM_CONFIG` on shared storage.
4. Drop the database schema using Oracle Fusion Middleware Repository Creation Utility. When dropping the schema, ensure that you select the ODS schema, as it is not selected by default. Oracle Identity Management Provisioning will fail during the next run if you do not perform this step correctly.
5. Rerun provisioning.

Windows:

1. Stop **all** the services started by Oracle Identity Management Provisioning by using the `stopall.bat` script located in `IDM_CONFIG/scripts` directory and execute the command:

   ```
   stopall.bat <node manager password> <weblogic password>
   ```

2. Deinstall the OPMN Instances.
   1. From the `<Product-Oracle-home>/oui/bin` directory, execute the following command:

      ```
      setup.exe -deinstall -novalidation
      ```

      An Oracle Universal Installer is launched
   2. Do the following:
      a. On the Welcome screen, click **Next**.

b. On the next screen, select **Deinstall ASinstances managed by Weblogic Domain** and click **Next**.

c. On the next screen, enter values for following fields:

Domain Host Name (i.e. Value for your hostname)

Domain Port No (i.e. Value for Admin Server Port)

UserName (i.e. Value for your Weblogic user name)

Password (ie. Value for your Oracle Identity Management Password)

d. In the next screen, select the Managed Instance you want to deinstall (The instances are named with the instance names e.g : oid1,ohs1, oif_inst,odsm).

e. Click **Next**.

f. Click **Finish**.

27.7 Deleting the Database

To delete the database, use Database Configuration Assistant (DBCA) to delete an instance of the database and then remove the database software. For more information, see "Deleting a Database Using DBCA" and "Removing Oracle Database Software" in *Oracle Database 2 Day DBA*.

27.8 Uninstalling the Oracle Identity Management Provisioning Framework

Follow the instructions described in this section to uninstall the Oracle Identity Management provisioning framework.

1. Stop all services running under *IDMLCM_HOME*. Since there is no script for killing processes under *IDMLCM_HOME*, you must manually kill all the processes running under *IDMLCM_HOME*.
2. Change directory to *IDMLCM_HOME*`/oui/bin` and execute the following command:

   UNIX:

   ```
   runInstaller -deinstall -jreLoc <JAVA_HOME>
   ```

   Windows:

   ```
   setup.exe -deinstall -jreLoc <JAVA_HOME>
   ```

3. On the Oracle Universal Installer screen, complete the following steps:
   a. On the **Welcome** page, click **Next**.
   b. On the **Deinstall Oracle Home** page, select the **Deinstall** option and click **Yes** when prompted. The **Deinstallation Progress** screen is displayed.
   c. After the deinstallation is complete, click **Finish**.

Note: If the `JAVA_HOME` environment variable is not set, you can retrieve it from *REPOSITORY_LOCATION/installers/jdk/jdk6.zip*, unzip it to any location and set the `JAVA_HOME`.

27.9 Uninstalling the Oracle Fusion Applications Provisioning Framework

Uninstalling Oracle Fusion Applications involves removing the Oracle Fusion Applications Provisioning Oracle home. The deinstaller attempts to remove the Oracle home from which it was started, and removes only the software in the Oracle home.

Before you remove the Oracle Fusion Applications Provisioning Oracle home, ensure that it is not in use. After you remove the software, you will no longer be able to provision a new Oracle Fusion Applications environment.

27.9.1 Running the Provisioning Framework Deinstaller

To start the deinstaller, navigate to:

UNIX: *FAPROV_HOME*/oui/bin or Windows: *FAPROV_HOME*\oui\bin and use this command:

UNIX: `runInstaller -deinstall -jreLoc REPOSITORY_LOCATION/jdk6`

Windows: `setup.exe -deinstall -jreLoc REPOSITORY_LOCATION\jdk6`

On Windows operating systems, you can also start the deinstaller from the Start menu by navigating to **Programs**, then **Oracle Fusion Applications Provisioning 11g-Home1**, and finally **Uninstall**.

The **Uninstall** menu is a Windows shortcut to the `setup.exe -deinstall` command. Note that you should not use the `Start -> All Programs -> Oracle - OHnnnn -> Oracle Installation Products -> Uninstall` menu option on Windows operating systems, where nnnn is a number. This **Uninstall** menu is also a shortcut to the `setup.exe` program but does not have the `-deinstall` command line option. Therefore, it will not deinstall the provisioning framework.

The deinstaller described in this section removes the provisioning framework that you can use to provision the Oracle Fusion Applications environment. It does not uninstall the Oracle Fusion Applications environment. If you want to uninstall an Oracle Fusion Applications environment, refer to Section 27.3 or Section 27.4 before removing the provisioning wizard from your system.

After removing the provisioning wizard from Windows operating systems, delete the `Oracle - OHnnnn` folder located in the `ProgramData -> Microsoft -> Windows -> Start Menu -> Programs` folder.

27.9.2 Deinstaller Screens and Instructions

Table 27–2 contains instructions for uninstalling the provisioning framework. For help with any of the interview screens, click **Help** on any interview screen.

Table 27–2 Provisioning Deinstaller Screen Flow

Screen	Description and Action Required
Welcome	No action is required on this read-only screen. Click **Next** to continue.

Deinstall Oracle Home	Verify that the directory path is correct. Click **Save** to create a text file with the details of the configuration you are deinstalling. Click **Deinstall** to continue.
	On the **Warning** screen, select whether you want the deinstaller to remove the Oracle home directory in addition to removing the software. Click **Yes** to remove the software files and the provisioning Oracle home directory. Click **No** to remove only the software files, or click **Cancel** to return to the previous screen.
	If you clicked **No**, remove the framework software files manually. For example, you would use this syntax if the directory is `/d1/oracle/provisioning`:
	`UNIX: cd /d1/oracle/provisioning`
	`Windows: rm -rf provisioning`
	If the Oracle home directory is `C:\Oracle\Provisioning`, use a file manager window and navigate to the `C:\Oracle` directory. Right-click the `Provisioning` folder and select **Delete**.

Deinstallation Progress	Monitor the progress of the deinstallation. Click **Cancel** to stop the process. Click **Next** to continue.
Deinstallation Complete	Click **Finish**.

Glossary

applications base

The top-level directory for the Oracle Fusion Applications binaries. You specify a name for this directory at the time of provisioning. This directory includes two mount points: */net/mount1/appbase* for components that will remain read-only after provisioning, and */net/mount2* (*APPLICATIONS_CONFIG*) to contain instances that are configurable after provisioning. This structure aids performance issues and accommodates a "lock-down" of binaries after provisioning. It ensures that the configurable components remain available.

BPEL

Business Process Execution Language; a standard language for defining how to send XML messages to remote services, manipulate XML data structures, receive XML messages asynchronously from remote services, manage events and exceptions, define parallel sequences of execution, and undo parts of processes when exceptions occur.

cleanup

The installation phase that shuts down processes started during a failed phase and performs the necessary cleanup actions. If the automated cleanup fails, you must manually stop all processes except the Node Manager on all hosts including OPMN and Java EE processes before you can run the restore action. Note, however, that you must stop *all* processes if you are running the cleanup action on the Configure phase

CLI

Used for starting the Provisioning Wizard and running installation phases on the Primary host, Secondary host, and DMZ host (when present).

cluster

A group of Oracle WebLogic Servers that work together to provide scalability and high availability for applications. A cluster appears as a single Oracle WebLogic Server instance. The Managed Server instances that constitute a cluster can run on the same host or be located on different hosts. Applications are deployed to the cluster, which implies deployment to every Managed Server within the cluster.

Configure

The installation phase that creates domains, Managed Servers, and clusters. Configures data sources and performs Node Manager registration of servers on the primordial host and primary host.

Configure-secondary

The installation phase that performs the configuration actions on a primary or secondary host (or both), registers Managed Servers with the Node Manager on secondary hosts, and creates a web tier instance. If there are no primary or secondary hosts, or if there are only primary hosts, this phase runs, but takes no action.

cube

A block of data that contains three or more dimensions. An Essbase database is a cube.

DMZ

Acronym for demilitarized zone. An isolated internal network used for servers that are accessed by external clients on the Internet, such as web servers, to provide a measure of security for internal networks behind the firewall.

DMZ host

A host that cannot access the shared storage within the firewall. This type of host is typically used to install the Oracle HTTP Server so that restrictions on communication with components within the firewall can be enforced.

e-mail bounce

An e-mail that is returned due to a temporary or permanent error condition.

financial reporting book

Comprised of reports and other documents such as text, PDF, PowerPoint, Excel and Word files. When run, the report data is dynamically retrieved from the database; the snapshot data remains static.

FTP

Acronym for File Transfer Protocol. A system for transferring computer files, generally by the Internet.

global area

The region across the top of the user interface. It provides access to features and tools that are relevant to any page you are on.

home directory

A directory that contains one or more Oracle Fusion Middleware homes or Oracle Fusion Applications homes. This directory has no functional significance other than as a grouping of related Oracle product offerings.

idmsetup.properties

A properties file, `idmsetup.properties`, is automatically generated during the provisioning of an Oracle Identity Management environment. This file includes some of the configuration values that you must supply to the Provisioning Wizard when you create a response file. These values must be included in your response file to integrate Oracle Identity Management components with an Oracle Fusion Applications environment.

Select the **Load IDM Configuration from IDM Properties file** option available on the **IDM Properties File** screen of the Provisioning Wizard, if you want the values on the Identity Management Configuration screen and the Access and Policy Management Configuration screen to default to the values in the IDM properties file. You must however review these screens to ensure that all values are accurate before proceeding to the next screen.

The properties file is created in:*SHARED_CONFIG_DIR*/fa/idmsetup.properties, where SHARED_CONFIG_DIR is the shared configuration location that you selected in the **Install Location Configuration** page of the Oracle Identity Management Provisioning Wizard.

For more information about the IDM properties file, see Section 10.7.2, "Passing Configuration Properties File to Oracle Fusion Applications".

Install

The installation phase that installs middleware and applications components and applies database patches shipped with provisioning (for databases created with the wizard).

Managed Server

A server which hosts components and associated resources that constitute each product configuration. The domains are predefined to ensure that product offerings and their dependencies are always stored in a standardized arrangement.

MTA

Acronym for mail transfer agent. A software program that transfers electronic mail messages from one computer to another.

offering

A comprehensive grouping of business functions, such as Sales or Product Management, that is delivered as a unit to support one or more business processes.

Oracle Fusion Applications Search

A special type of search based on technology that differs from that of most other searches in Oracle Fusion Applications. Oracle Fusion Applications Search is available in the global area and other places.

point of view

User selected dimensions that are not included in the grids at the row, column or page levels for a particular report. Only these dimensions can be overridden at run time, unless user also specifically defined Prompt for the dimensions on the grid.

Postconfigure

Installation phase which configures Oracle SOA Suite composite deployment and Oracle HTTP Server, and populates policies and grants. Configures middleware and applications that require servers to be online.

Preconfigure

The installation phase that updates the Oracle Application Development Framework (Oracle ADF) configuration.

Preverify

The installation phase that checks to see that the prerequisites for an installation are met.

Primary host

The host on which the Administration Server of a domain runs.

Primordial host

The host that contains the Common domain (and specifically the Administration Server of the Common domain). There is one, and only one, primordial host per shared drive.

product offerings

Groups of features within an installation of Oracle Fusion Applications which represent the highest-level collection of functionality that you can license and implement.

provisioning configuration

A collection of one or more product offerings.

Provisioning Command-line Interface (CLI)

See CLI.

provisioning repository

A repository which contains all the installers required to provision a new Oracle Fusion Applications environment. You download the repository from the Oracle Fusion Applications Product Media Package and extract the files to a location of your choice, for example *repository_location*/installers. The repository must be located on a networked drive or a shared hard disk so that it is accessible to all the hosts in your new environment.

provisioning summary file

A file which contains details that describe the installation. It is automatically created by provisioning after the installation is complete and includes a link to the Oracle Fusion Applications home page.

Provisioning Wizard

A question-and-answer interview that guides you through the process of installing a database, creating or updating a response file, and installing or deinstalling the components of an Oracle Fusion Applications environment.

response file

A collection of configuration details you specify about installation locations, product offerings and middleware (technology stack) dependencies. In addition, you enter connection parameters for the database and identity management components that you set up as prerequisites. You use the Provisioning Wizard interview to create and execute the response file.

restore

The installation phase consisting of the necessary restore actions required for a given provisioning phase. This action deletes and restores the instance directory, and, if necessary (and available), restarts the Common Domain Administration Server and Oracle HTTP Server.

Secondary host

Location where the Managed Servers for any application reside when they are not on the same host as the Administration Server of the same domain. Typically used when a domain spans two physical servers.

SOA

Abbreviation for service-oriented architecture.

Startup

Installation phase that starts the Administration Server and the Managed Server on the current host. Performs online configuration, including global unique identifier (GUID) reconciliation and Financial/IPM configuration.

Validate

Installation phase that validates the deployment configuration and starts the Managed Server.

WebLogic Server Domain

A logically related group of Oracle WebLogic Server resources that is managed as a unit. It consists of an Administration Server and one or more Managed Server.

WSDL

Abbreviation for Web Services Description Language. It is an XML format that provides a model for describing Web services.