**Oracle® Fusion Applications**

Upgrade Guide

11*g* Release 7 (11.1.7)

**E35833-18**

July 2014

Documentation for installers and system administrators that describes how to use Upgrade Orchestrator to upgrade Oracle Fusion Applications software between major releases.

**ORACLE**®

Oracle Fusion Applications Upgrade Guide, 11g Release 7 (11.1.7)

E35833-18

Primary Author:     Vickie Laughlin

Contributors: Subash Chadalavada, Lori Coleman, Rick Lotero, Jay Lu, Prashant Salgaocar, Venkatesh Sangam, Praveena Vajja

# Contents

## 3   Updating the Oracle Fusion Applications and Oracle Identity Management Databases

# 4 Upgrading to Oracle Fusion Applications Release 7

## 5 Post-Upgrade Tasks for Oracle Fusion Applications

## 6 Monitoring and Troubleshooting the Upgrade

## A    Additional Information About Upgrade Orchestrator

## B    Upgrade Orchestrator Properties Files

## C    Platform Specific Pre-Upgrade Steps

## D  Oracle Identity Manager Upgrade Properties

## E  Stopping and Starting Identity Management Related Servers

# Preface

This guide provides information about using Upgrade Orchestrator to upgrade your Oracle Fusion Applications software.

## Audience

This guide is intended for system administrators who are responsible for performing Oracle Fusion Applications upgrade tasks.

## 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 Administrator and Implementor Roadmap*

- *Oracle Fusion Applications Concepts Guide*

- *Oracle Fusion Applications Administrator's Guide*

- *Oracle Fusion Applications Installation Guide*

- *Oracle Fusion Applications Patching Guide*

- *Oracle Fusion Applications Post-Installation Guide*

- *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*

## 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

The following topics introduce the new and changed features of the Oracle Fusion Applications upgrade process and other significant changes that are described in this guide, and provide pointers to additional information.

## New and Changed Features for 11*g* Release 7 (11.1.7)

Oracle Fusion Applications 11*g* Release 7 (11.1.7) includes the following new and changed upgrade features for this document:

- Added information to describe Oracle Fusion Applications Upgrade Orchestrator. See Chapter 1, "Introduction to the Oracle Fusion Applications Upgrade".

- Removed manual pre-upgrade steps that are now performed by Oracle Fusion Applications Upgrade Orchestrator. See Chapter 2, "Preparing to Perform the Release 7 Upgrade".

- Modified the steps to perform the upgrade using Oracle Fusion Applications Upgrade Orchestrator. See Chapter 4, "Upgrading to Oracle Fusion Applications Release 7".

- Removed manual post-upgrade steps that are now performed by Oracle Fusion Applications Upgrade Orchestrator. See Chapter 5, "Post-Upgrade Tasks for Oracle Fusion Applications".

- Added troubleshooting information related to Oracle Fusion Applications Upgrade Orchestrator. See Chapter 6, "Monitoring and Troubleshooting the Upgrade".

- Updated path to the `defaults.txt` file. See Section 6.13.4, "Failure During AutoPatch Validation."

## Other Significant Changes in this Document for 11*g* Release 7 (11.1.7)

For 11*g* Release 7 (11.1.7), this guide has been updated in several ways. Following are the sections that have been added or changed.

- The steps for running the following processes have been moved to an Appendix because Oracle Fusion Applications Upgrade Orchestrator runs these processes.

  - Section A.2.1, "RUP Installer"

  - Section A.2.2, "Health Checker Utility"

  - Section A.2.3, "RUP Lite for OVM Utility"

  - Section A.2.4, "RUP Lite for OHS Utility"

- Section A.2.5, "RUP Lite for BI Utility"

- The steps for installing a language pack have been moved from this guide to the *Oracle Fusion Applications Administrator's Guide* because Oracle Fusion Applications Upgrade Orchestrator upgrades installed languages.

- Added an appendix that describes the properties files that are required by Oracle Fusion Applications Upgrade Orchestrator. See Appendix B, "Upgrade Orchestrator Properties Files".

- Updated the description for the REL6_RUPINSTALLER_UPGRADE_PARAM and REL7_RUPINSTALLER_UPGRADE_PARAM properties in Appendix B, "Upgrade Orchestrator Properties Files".

- Added an appendix that describes pre-upgrade steps for platforms other than Linux and Windows. See Appendix C, "Platform Specific Pre-Upgrade Steps."

- Added an appendix that describes Oracle Identity Manager upgrade properties. See Appendix D, "Oracle Identity Manager Upgrade Properties."

- Added an appendix that describes how to stop and start servers related to Oracle Identity Management. See Appendix E, "Stopping and Starting Identity Management Related Servers."

# 1

# Introduction to the Oracle Fusion Applications Upgrade

This chapter provides an introduction to the process of upgrading Oracle Fusion Applications to 11*g* Release 7 (11.1.7).

This chapter contains the following topics:

- Upgrade Process Overview
- Hosts, Directories, and Files Required by Upgrade Orchestrator
- Oracle Fusion Applications Upgrade Orchestrator Features
- Back Up Strategy
- Planning Your Down Time
- Directories Structure Overview

## 1.1 Upgrade Process Overview

Upgrading to Oracle Fusion Applications 11*g* Release 7 (11.1.7) requires that you run Oracle Fusion Applications Upgrade Orchestrator (Upgrade Orchestrator) on an Oracle Fusion Applications environment. If you are upgrading to Release 7 from Release 5 (11.1.5), Upgrade Orchestrator manages this chained upgrade in two hops. The first hop is the upgrade from Release 5 to Release 6 (11.1.6). The second hop of the upgrade is from Release 6 to Release 7. Note that releases of Oracle Fusion Applications are referred to as Release 5, Release 6, and Release 7 for the remainder of this Upgrade Guide.

The upgrade process flow varies, depending on whether you are running Oracle Fusion Applications on an Oracle VM environment. The following diagram depicts the upgrade process flow for non-Oracle VM environments.

*Figure 1–1   Upgrade Process Flow for non-Oracle VM Environments*
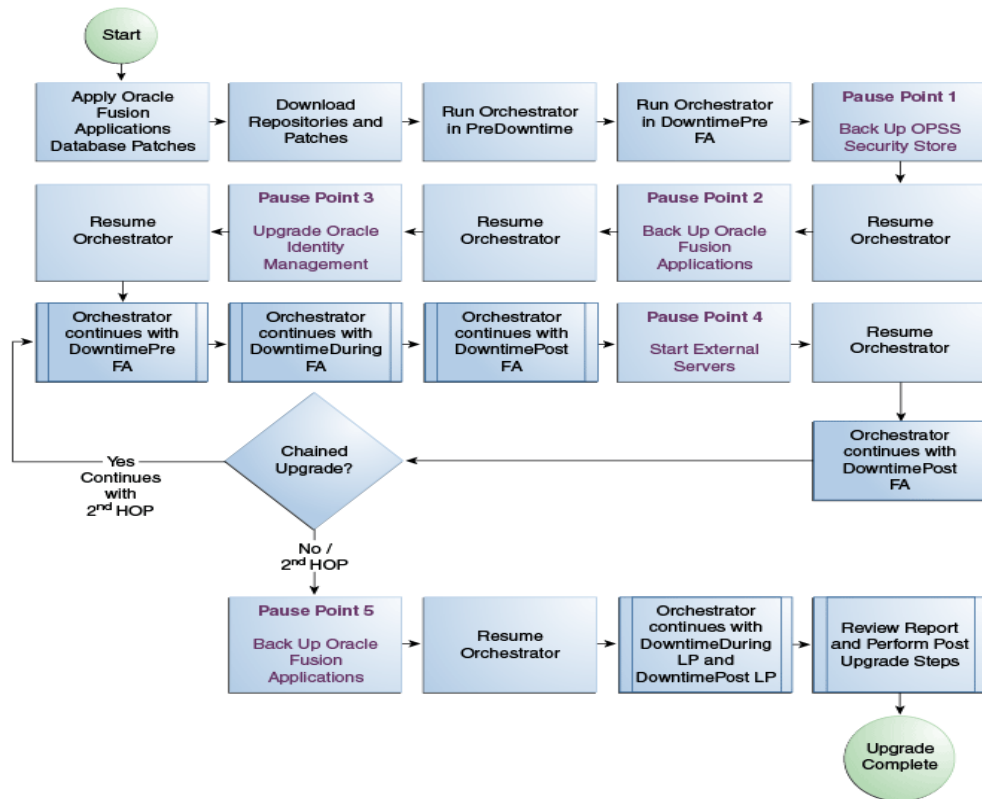


The following diagram depicts the upgrade process flow for Oracle VM environments.

*Figure 1–2   Upgrade Process Flow for Oracle VM Environments*
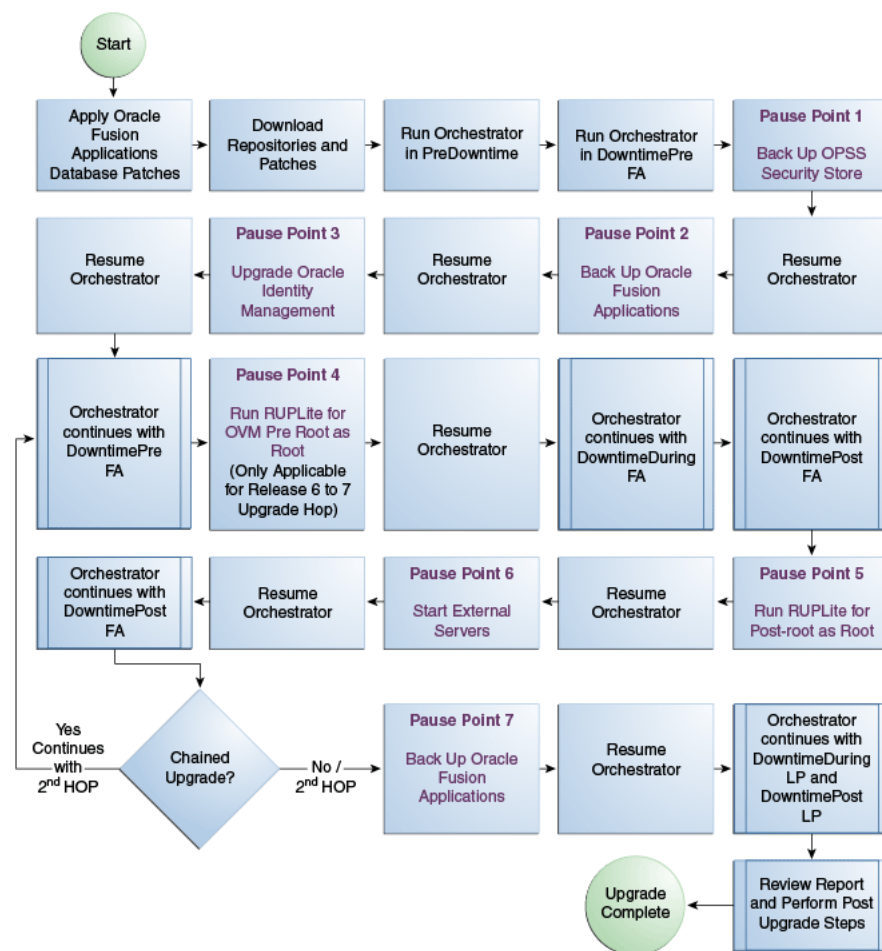


For more information about the tools and utilities called by Upgrade Orchestrator, see Appendix A, "Additional Information About Upgrade Orchestrator".

You must complete all pre-upgrade tasks before you start Upgrade Orchestrator. For more information, see Chapter 2, "Preparing to Perform the Release 7 Upgrade". You must also update your database during a separate downtime window prior to the upgrade. For more information, see Chapter 3, "Updating the Oracle Fusion Applications and Oracle Identity Management Databases." After you upgrade by following the steps in Chapter 4, "Upgrading to Oracle Fusion Applications Release 7," you must complete the post-upgrade tasks. For more information, see Chapter 5, "Post-Upgrade Tasks for Oracle Fusion Applications".

## 1.2  Hosts, Directories, and Files Required by Upgrade Orchestrator

Familiarize yourself with the information in this section before proceeding with the upgrade.

### 1.2.1  Host Types

The Release 7 upgrade must be performed on the following host types:

- **Primordial host**: The location of the Common domain (specifically the Administration Server of the Common domain). Only one primordial host exists in each environment.

- **IDM host:** A combination of hosts which hosts OID, OIM, OAM,IDM OHS, and IDM Database services.

- **OHS host:** The host where the Oracle HTTP Server (OHS) software is installed and configured.

- **DB host:** The host where the Oracle Fusion Applications database is installed and configured.

- **Midtier hosts**:

  - **Primary host**: The host on which the Administration Server of a domain runs. Only one primary host exists in a domain.

  - **Secondary host:** The 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 (do) not have the administration server is (are) called secondary host(s).

  - **BI host:** The host where the Oracle Business Intelligence (Oracle BI) software is installed and configured.

Note that all of these host types can be scaled out to multiple hosts, and Upgrade Orchestrator must be run on each scaled out host for all host types, with the exception of DB hosts. For more information, see "Scaling Out Oracle HTTP Server" in the *Oracle Fusion Applications Enterprise Deployment Guide for Customer Relationship Management*.

## 1.2.2 Directories and Files Required by Upgrade Orchestrator

The following directories and files are referenced in this guide and are required by Upgrade Orchestrator:

- SHARED_LOCATION: You create this directory in a shared location, which is accessible to all hosts in the environment, including scaled out hosts. For more information, see Section 2.3.2, "Create Directories in a Shared Location".

- ORCHESTRATION_CHECKPOINT_LOCATION and ORCHESTRATION_ CHECKPOINT_ARCHIVE_LOCATION: You create these directories in the SHARED_LOCATION, where orchestration checkpoint related files are saved. For more information, see Section 2.3.3.1, "Orchestration Checkpoint Locations". These directory locations are stored as properties in the pod.properties file. For more information, see Table B–1, " pod.properties".

- SHARED_UPGRADE_LOCATION: You create this temporary directory to copy files and perform write operations. For more information, see Section 2.3.3.2, "Shared Upgrade Location".

- ORCH_LOCATION: This directory is created when you unzip orchestration.zip and is referred to as the orchestration directory. For more information, see Section 2.3.7, "Unzip Orchestration.zip".

- POD_NAME: You can create this directory under ORCH_LOCATION. The name of the directory created is referred to as *POD_NAME* throughout this guide.

- Manifest files: These files are .xml type distribution files that are required by both Health Checker and Upgrade Orchestrator. They are used throughout this guide to define specific tasks performed during the upgrade process.

## 1.3  Oracle Fusion Applications Upgrade Orchestrator Features

Upgrade Orchestrator includes the following features:

- Upgrade Phases
- Pause Points
- Upgrade Orchestration Properties
- Oracle Fusion Applications Orchestrator Upgrade Report
- Health Checker
- Language Upgrade

### 1.3.1  Upgrade Phases

You run Upgrade Orchestrator on all host types except for the DB host. The upgrade is performed in phases, during which sets of tasks run. Upgrade Orchestrator waits to ensure that the current set of tasks run to successful completion on all hosts before proceeding to the next set of tasks. If there is a participating host which is not reporting its status, an email alert is sent with corrective action.

Upgrade Orchestrator performs the upgrade in two primary phases:

- Pre-Down Time: Upgrade Orchestrator provides the option to run pre-down time steps using the command line option, `-phase PreDowntime`, allowing you run some steps before your down time. This phase can be run at any time prior to your upgrade maintenance window and can be run any number of times, until all validations and health checks are successful. Issues reported by the tools during this phase can be fixed ahead of time, before entering the maintenance window.

  For more information on the steps that are included in the `PreDowntime` phase and how to run this phase of the upgrade, see Section 4.1.1, "Run Upgrade Orchestrator in Pre-Down Time Mode".

- Down Time: This phase is executed during the maintenance window. Upgrade Orchestrator exits and pauses during this phase to allow you to perform required tasks outside of orchestration, after which you must relaunch orchestration on one or more hosts to resume the upgrade.

### 1.3.2  Pause Points

Upgrade Orchestrator pauses when it reaches a task that must be performed outside of orchestration. You perform the required steps and then direct Upgrade Orchestrator to continue with the upgrade. If multiple environments are sharing the orchestration software location, a **pause point** that is created on a host type is common across all environments for that host type.

Default pause points are predefined by Upgrade Orchestrator to allow you to perform the following actions:

- Perform required backups
- Upgrade the Oracle Identity Management domain
- Run RUP Lite for OVM in pre- and post-root modes
- Start external servers

You cannot edit or remove default pause points. For more information, see Section 4.4, "Pause Point Steps".

### 1.3.3 Upgrade Orchestration Properties

Orchestration uses the properties defined in five properties files: `pod.properties`, `PRIMORDIAL.properties`, `OHS.properties`, `MIDTIER.properties`, and `IDM.properties`. The properties are set to specific values as part of your preparation to begin the upgrade. For more information, see Appendix B, "Upgrade Orchestrator Properties Files".

### 1.3.4 Oracle Fusion Applications Orchestrator Upgrade Report

The Oracle Fusion Applications Upgrade Orchestrator report is generated for each pod and its location is defined in the mandatory *ORCH_REPORT_LOCATION* property in the `pod.properties` file. When you run the report, you can override the default value for the location, if needed. In the event of a failure during the upgrade, this report is generated and emailed to the user who is running the upgrade. The report name is `FAOrchestrationUpgradeReport_`*release_hosttype_hostname_timestamp*`.html`. Reports are archived at *ORCH_LOCATION*`/ARCHIVE/`*release*/*hosttype*/*hostname*/*timestamp* for troubleshooting purposes after the failure or completion of each task.

The report displays the task that failed, including the phase and host type. This report also displays the following information:

- **Upgrade from Release**: The starting release on the pod, which is either release 11.1.5.0.0 or release 11.1.6.0.0.

- **Upgrade to Release:** The ending release, which in this case is "FA version 11.1.7.0.0".

- **Upgrade Status:** The cumulative status of the upgrade. The following states are possible:

  - Success: All tasks were successful.

  - Error: One or more tasks failed.

  - Running: At least one task is still running and there are no failures.

  - NotApplicable: The task is not applicable on the host.

  - Pending: A task is waiting for a dependent task to complete.

  - PausePoint: A task must be performed manually. Orchestrator needs to be restarted after the manual process completion.

- **Report Time:** The time stamp in the format of yyyy-MM-dd HH:mm:ss.SSS.

- **Status Table:** Contains the following columns:

  - Task: Tasks are listed in the order of execution.

  - Phase: Phase during which the task runs.

  - Host type: Host type on which the task runs.

  - HostNames: All scaled out hosts for the host type.

  - Status: Status of the task for each host, including scaled out hosts.

  - Start Time: The start time for the task on a specific host.

  - End Time: The end time for the task on a specific host.

  - Duration: The duration of the task on a specific host.

  - More details: The path and file name for the HTML report that is generated on each host.

### 1.3.5 Health Checker

Upgrade Orchestrator runs the Health Checker utility to run system checks before, during, and after the upgrade to ensure that the environment meets recommended standards. For more information, see Section A.2.2, "Health Checker Utility."

### 1.3.6 Language Upgrade

If you previously installed any languages in addition to US English, Upgrade Orchestrator performs the upgrade of each installed language. For information about installing a new language, see "Installing and Maintaining Oracle Fusion Applications Languages" in the *Oracle Fusion Applications Administrator's Guide*.

Orchestration allows you to skip one or more installed language pack upgrades by using a property called `SKIP_UPGRADE_FOR_LANGUAGE` in the `PRIMORDIAL.properties` file. If you choose to skip any languages, you upgrade them manually after the completion of Upgrade Orchestration. For more information, see "Installing and Maintaining Oracle Fusion Applications Languages" in the *Oracle Fusion Applications Administrator's Guide*.

## 1.4 Back Up Strategy

Before you start the upgrade process, you should have a clear understanding of the backup requirements, as there are multiple components involved in an Oracle Fusion Applications environment. An effective and accurate backup strategy helps to restore from the point of failure without having to restart from the beginning.

Note that backups are manual steps and can be automated outside of Upgrade Orchestrator based on your IT requirements and processes. For detailed information about required backups, see Section 4.4.1, "Back Up the OPSS Security Store" and Section 4.4.2, "Back Up Oracle Fusion Applications".

The following components must be backed up:

- Oracle Fusion Applications, including:
  - Oracle Fusion Applications database
  - `APPLICATIONS_BASE`, as defined in Section 1.6.3, "Relationship of Home Directories"
  - `APPLICATIONS_CONFIG`, as defined in Section 1.6.3, "Relationship of Home Directories"
  - Oracle Identity Management database
  - Upgrade Orchestration directories
  - OHS and /etc/hosts files
  - Central Inventory
- OPSS Security Store

You must back up your Oracle Fusion Applications upgrade at multiple stages during the upgrade process. It is recommended to back up your entire Oracle Fusion Applications environment, including your databases, at the following points:

- Before the upgrade
- Between the two hops, if you are performing a multi-hop upgrade
- After the upgrade

- Before the language pack upgrade starts, if you have languages installed

For additional backup steps that are specific to Windows, refer to Section 4.4.3, "Back Up Oracle Fusion Applications on a Windows Platform".

Upgrade Orchestrator provides default pause points to perform these backup steps, depending on your upgrade path. For more information, see Section 4.1.6, "Pause Point 2 - Back Up Oracle Fusion Applications".

## 1.5 Planning Your Down Time

Consider the following suggestions when planning your down time for the upgrade:

- Perform pre-down time steps ahead of time. For more information, see Chapter 2, "Preparing to Perform the Release 7 Upgrade".

- Perform your database patching in a separate maintenance window. For more information, see Chapter 3, "Updating the Oracle Fusion Applications and Oracle Identity Management Databases".

- Run Upgrade Orchestrator in pre-down time mode after all prerequisites are met. For more information, see Section 4.1.1, "Run Upgrade Orchestrator in Pre-Down Time Mode".

## 1.6 Directories Structure Overview

Upgrade Orchestrator references and uses the following directories:

- Directories Used by Upgrade Orchestrator

- Download Directories

- Relationship of Home Directories

### 1.6.1 Directories Used by Upgrade Orchestrator

The following diagram shows the directory structure that is created when the Orchestration.zip file is unzipped and is referred to as ORCH_LOCATION. For more information, see Section 2.3.7, "Unzip Orchestration.zip".

*Figure 1–3   Directory Structure of Upgrade Orchestrator*
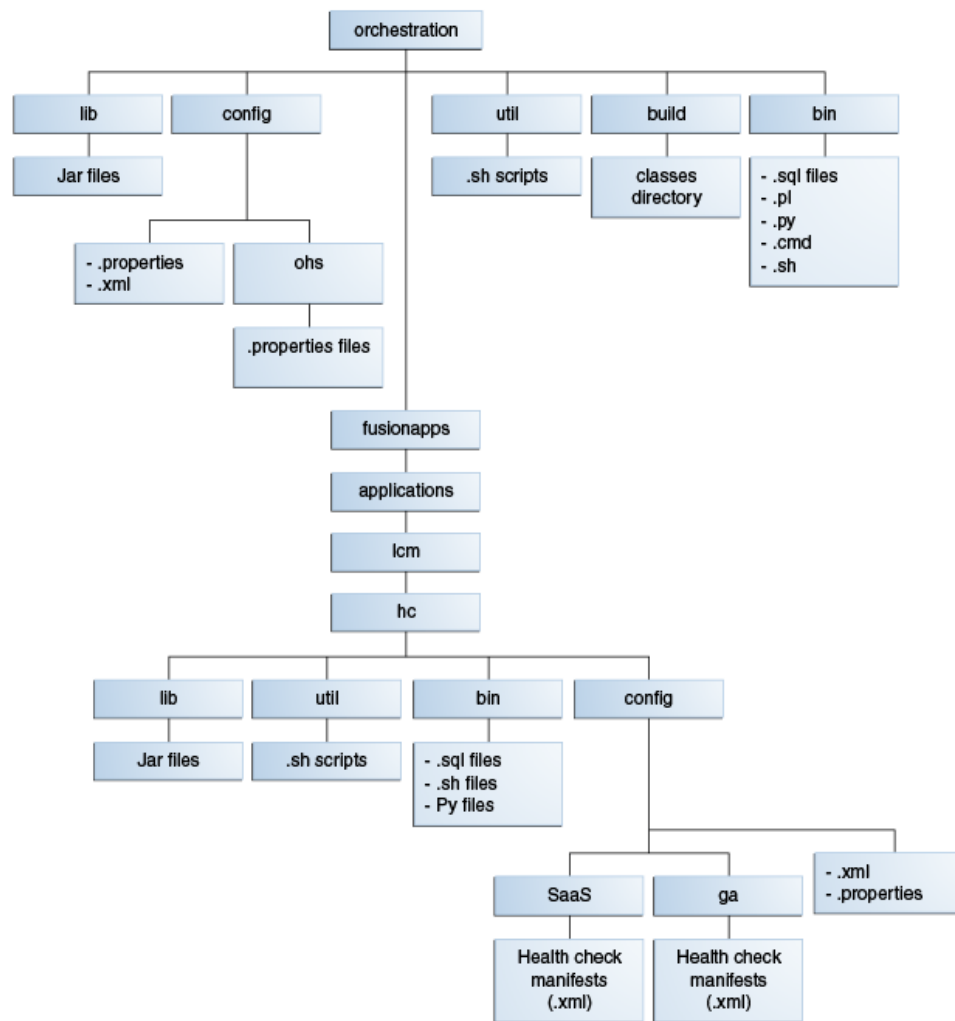


## 1.6.2  Download Directories

The following diagram shows the directory structure that you create during the preparation of your environment for the upgrade. There are specific files that must be downloaded into each of these directories. For more information, see Section 2.3.2, "Create Directories in a Shared Location".

*Figure 1–4   Directory Structure of Downloaded Patches and Repositories*
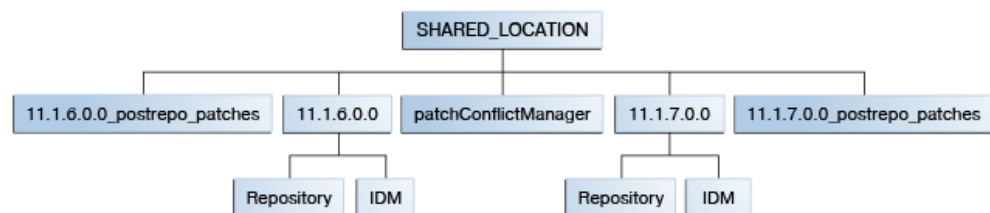


## 1.6.3  Relationship of Home Directories

The following home directories are referenced during the upgrade steps:

■ *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*: The directory named `applications`, located under the Oracle Fusion Applications Middleware home `fusionapps` directory.

The following figure shows the relationship of the home directories using the Oracle Fusion Financials product family on a UNIX environment as an example. This figure does not show all subdirectories under `APPLICATIONS_BASE` and `APPLICATIONS_CONFIG`. For example, the `APPLICATIONS_CONFIG` directory contains several more directories for component-specific configuration files. Also, Oracle Database and Oracle Identity Management are not represented in this figure, as they are installed separately. For more information, see "Provisioned Oracle Fusion Applications Home Directories" in the *Oracle Fusion Applications Administrator's Guide*.

*Figure 1–5   Relationship of Home Directories*

# 2
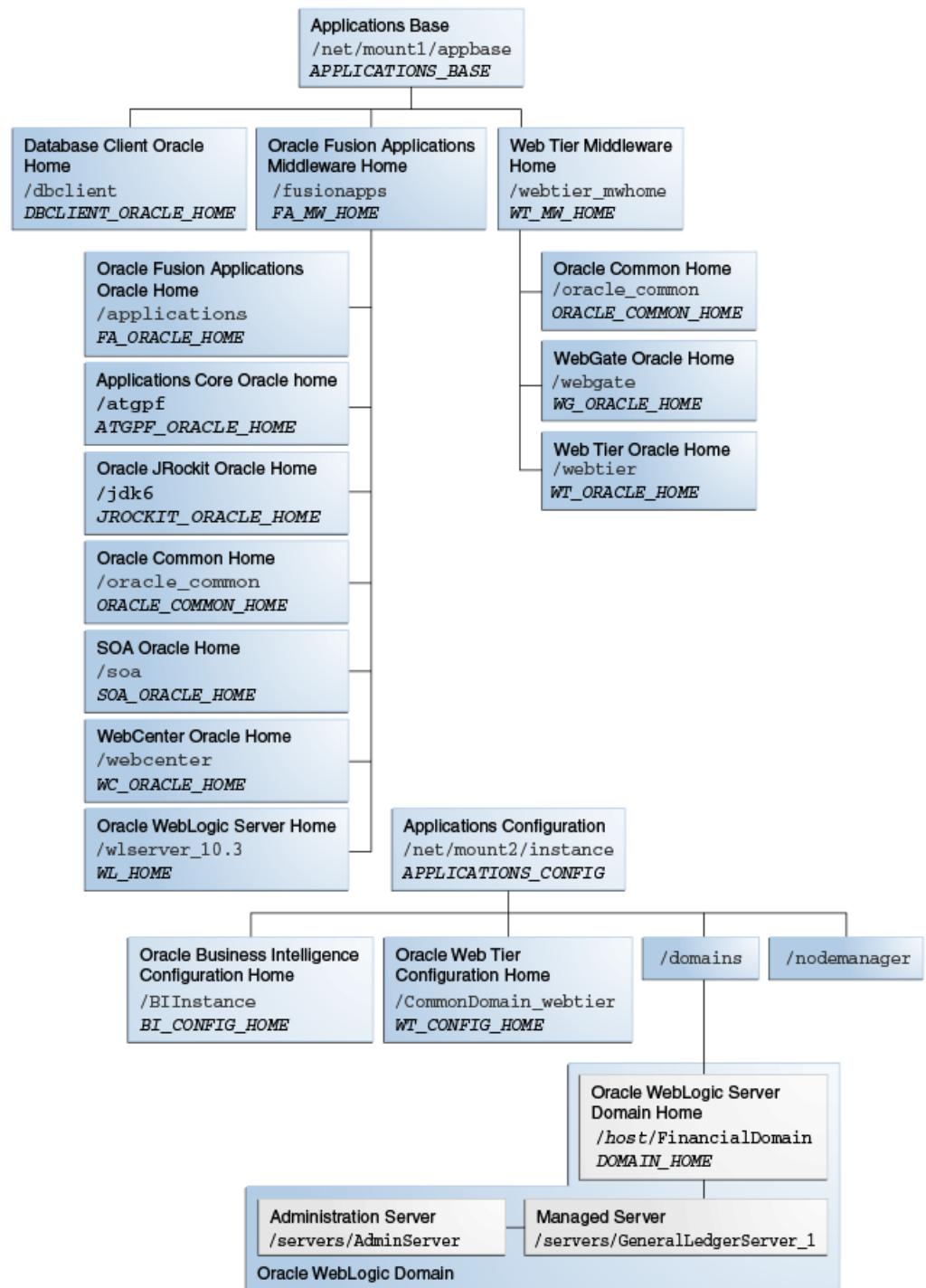
# Preparing to Perform the Release 7 Upgrade

This chapter describes the preparation steps for upgrading to Release 7, all of which can be performed before your scheduled down time. This chapter includes preparation steps for upgrading from Release 5 to Release 6 and from Release 6 to Release 7, depending on whether you are performing a chained upgrade from Release 5 to Release 6 to Release 7, or a single hop upgrade from Release 6 to Release 7.

This chapter contains the following topics:

- Before You Begin
- System Requirements
- Set Up Upgrade Directories and Obtain Software
- Set Up Upgrade Orchestrator
- Verify Your Environment Before Proceeding to Down Time
- What To Do Next

## 2.1 Before You Begin

Follow the steps in this section before you begin the upgrade.

1. Ensure you have access to the following documentation:

   - Upgrade documentation from Release 5 and/or Release 6
   - Oracle Fusion Applications release notes from Release 5 and/or Release 6
   - Oracle Fusion Applications release notes for Release 7

2. Ensure you have performed all Release 5 post upgrade tasks from Release 5 documentation and Release 5 release notes, if your starting point is Release 5.

3. Ensure you have applied the following high watermark patch bundles on your Release 5 environment prior to upgrading to the next release:

   - Fusion Middleware Patch Bundles for Oracle Fusion Applications
   - Oracle Fusion Application Patch Bundles

   Contact Oracle Support for information about high watermark patch bundles.

4. Ensure you perform all Release 6 Pre-upgrade steps from Release 6 release notes.

5. Ensure `sendmail` is configured and working on all hosts where Upgrade Orchestrator will run by sending a test mail from the hosts. Sendmail must be working properly before running the upgrade so you can effectively monitor the upgrade status.

## 2.2 System Requirements

Ensure that your environment meets the following system requirements:

- Memory Requirements
- Free Disk Space Requirements
- Ports Requirements
- Configure JVM Memory Settings for ESS Cluster and SCM Common
- Set LBR_PRESENT to True on the Primordial Host
- Webtier Instance Directory Mount (Oracle VM Only)

### 2.2.1 Memory Requirements

During the pre-down time phase, Upgrade Orchestrator reports an error if your environment does not meet the following memory requirements:

*Table 2–1    Memory Requirements for Non-Oracle VM Environments*

| Memory Requirements | Chained Upgrade | Single Hop Upgrade |
|---|---|---|
| Swap Space | 4GB | 4GB |
| Memory for RUP Installer/OUI | 7GB | 1GB |
| Memory per Managed Servers | 2GB multiplied by the number of managed servers in your environment, plus 4GB | 2GB multiplied by the number of managed servers in your environment, plus 4GB |
| Memory Per Administration Servers | 1GB multiplied by the number of administration servers in your environment | 1GB multiplied by the number of administration servers in your environment |
| Memory for BI Domain | 6GB | 6GB |
| Memory for APP OHS | 1 GB Free, 2GB Total | 1 GB Free, 2GB Total |

*Table 2–2    Memory Requirements for Oracle VM Environments in OVM Memory (MB)*

| Topology | IDM3OID | IDM3MW | IDM3OHS | FA | Primary | Secondary | OSN | BI | AppOHS |
|---|---|---|---|---|---|---|---|---|---|
| HCM | 2048 Free, 4096 Total | 3072 Free, 12288 Total | 256 Free, 1536 Total | 14336 | 32768 | 62464 | 3584 | 6144 | 2048 Free, 3072 Total |
| CRM | 2048 Free, 6144 Total | 3072 Free, 12288 Total | 256 Free, 1536 Total | 19456 | 33792 | 55296 | 3584 | 6144 | 2048 Free, 3072 Total |
| FSCM-H | 2048 Free, 4096 Total | 3072 Free, 12288 Total | 256 Free, 1536 Total | 17920 | 31744 | 65536 | 3584 | 6144 | 2048 Free, 3072 Total |

All free memory for IDM nodes is the recommended memory requirement when no IDM processes are running. To check for free memory availability, first shut down the servers and then measure the free memory.

In addition to memory requirements, ensure you meet the swap requirements on all topologies, as depicted in the following table.

*Table 2–3 Memory Swap Requirements for All Oracle VM Topologies (MB)*

| IDM3OID | IDM3MW | IDM3OHS | FA | Primary | Secondary | OSN | BI | AppOHS |
|---------|--------|---------|------|---------|-----------|------|------|--------|
| 4000 | 4000 | 4000 | 4000 | 4000 | 4000 | 4000 | 4000 | 4000 |

## 2.2.2 Free Disk Space Requirements

The disk space requirements in the following table are recommendations for how much disk space should be added on each host type. During the pre-down time phase, Upgrade Orchestrator reports an error if your environment does not meet these requirements. The disk space check is not checking for total space. It is checking only for usable disk space, which is defined as free space, with respect to quotas and permissions. All recommendations and requirements assume non-shared access to the disk space. Therefore, if you have multiple hosts or processes running against the same physical disk, the size of this disk needs to be determined with respect to all sharing tenants. The requirements in the following table do not consider disk sharing scenarios.

*Table 2–4 Free Disk Space Requirements*

| Host | Single Hop (Release 6 to Release 7) | Chained Upgrade (Release 5 to 6 to 7) |
|------|-------------------------------------|----------------------------------------|
| Primordial | 100GB + 5GB for /tmp | 150GB + 8GB for /tmp |
| DB | 36GB + 5GB for /tmp + 4GB for flash recovery area (if configured) | 72GB + 5GB for /tmp + 12GB for flash recovery area (if configured) |
| OHS | 8GB + 5GB for /tmp | 13GB + 5GB for /tmp |
| Midtier | 5GB + 5GB for /tmp | 8GB + 5GB for /tmp |

## 2.2.3 Ports Requirements

Ensure that the following firewall ports are open to run the context URI health check on the OHS host source host and the LBR/Routing tier.

| Source | http Protocol | https Protocol |
|--------|---------------|----------------|
| fs | 10613 | 10614 |
| BI | 10621 | 10622 |
| crm | 10615 | 10616 |
| fin | 10603 | 10604 |
| hcm | 10619 | 10620 |
| prc | 10607 | not applicable |
| prj | 10605 | 10606 |
| scm | 10617 | 10618 |
| ic | 10611 | 10612 |
| prc-supplierportal | not applicable | 10610 |

### 2.2.4 Configure JVM Memory Settings for ESS Cluster and SCM Common

Perform the following steps to configure JVM memory settings.

1.  Open the following file in Edit mode to configure JVM settings for the `SCMCommonCluster`:

    *APPLICATIONS_ BASE*/instance/domains/admin-apps.oracleoutsourcing.com/SCMDomain/config/fusiona pps_start_params.properties

2.  Change the values of the following property to the new values in bold:

    fusion.SCMDomain.SCMCommonCluster.default.minmaxmemory.nonmain=-**Xms512m** -**Xmx1024m**

3.  Open the following file in Edit mode to configure JVM settings for the `ESSCluster` in the `CommonDomain`:

    *APPLICATIONS_ BASE*/instance/domains/admin-apps.oracleoutsourcing.com/CommonDomain/config/fusi onapps_start_params.properties

4.  Change the values of the following property to the new values in bold:

    fusion.CommonDomain.ESSCluster.default.minmaxmemory.main=-**Xms256m** -**Xmx1024m**

### 2.2.5 Set LBR_PRESENT to True on the Primordial Host

If you have LBR configured, ensure that the following `LBR_PRESENT` properties are set to true on all Administration Servers on the primordial host:

```
APPLICATIONS_BASE/instance/fapatch/ATGPF_env.properties:LBR_PRESENT=true
APPLICATIONS_BASE/instance/fapatch/FUSION_env.properties:LBR_PRESENT=true
APPLICATIONS_BASE/instance/fapatch/FUSION_prov.properties:LBR_PRESENT=true
```

### 2.2.6 Webtier Instance Directory Mount (Oracle VM Only)

Confirm whether `/u02/instance/CommonDomain_webtier_local` is mounted on the OHS host. If it is already mounted, you can skip this section and proceed to Section 2.3, "Set Up Upgrade Directories and Obtain Software."

If `/u02/instance/CommonDomain_webtier_local` is not mounted and it is a local directory, perform the steps in Section 2.2.6.1, "Steps for Local Directory That is not Mounted". If the environment is scaled out, perform the steps in Section 2.2.6.2, "Steps for Scaled Out Environment". These steps must be performed before running RUP Lite for OVM in pre-root mode.

#### 2.2.6.1 Steps for Local Directory That is not Mounted

If `/u02/instance/CommonDomain_webtier_local` is not mounted and it is a local directory, perform the following steps to mount the `webtier` instance directory to the OHS host.

1.  Create a `u02` directory under `/u01`, if it does not already exist.

2.  Stop OHS by using `opmnctl`.

3.  Move or copy `/u02/instance` to `/u01/u02`.

4.  Move `/u02` to `/u02_OHS_Old`.

5. Create a `/u02/instance/CommonDomain_webtier_local` directory using the root user.

6. Change the owner and group of `/u02`:.

   `chown -R user:group /u02`

   Example: `chown -R oracle:dba /u02`

7. To find the device where the `/u01` directory exists, run `mount | grep u01`.

   Example output for this command follows:

   `server01-nfs.mycompany.com:/export/fusion/appohs/u01 on /u01 type nfs (rw,address=ip_address)`

8. Using the device name from the step 7, run the following command: `mount -t nfs device_name`

   An example command follows:

   `mount -t nfs server01-nfs.mycompany.com/export/fusion_imf/appohs_ imf/u02/instance/CommonDomain_webtier_local /u02/instance/CommonDomain_ webtier_local`

### 2.2.6.2 Steps for Scaled Out Environment

If your environment is scaled out, on each scaled out host, if `/u02/instance/CommonDomain_webtier_local` is not mounted and it is a local directory, perform the following steps to mount the `webtier` instance directory to the OHS host.

1. Create a `u02_hostname` directory under `/u01`, if it does not already exist.

2. Stop OHS by using `opmnctl`.

3. Move or copy `/u02/instance` to `/u01/u02_hostname`.

4. Move `/u02` to `/u02_OHS_Old`.

5. As the root user, create a `/u02/instance/CommonDomain_webtier_local` directory.

6. Change the owner and group of `/u02`, using the following command:

   `chown -R user:group /u02`

   Example command:

   `chown -R oracle:dba /u02`

7. To find the device where the `/u01` directory exists, run `mount | grep u01`.

   Example output from this command follows:

   `server01-nfs.mycompany.com:/export/fusion/appohs/u01 on /u01 type nfs (rw,address=ip_address)`

8. Using the device name from the previous step, run the following command:

   ` mount -t nfs device_name`

   Example command:

   ` mount -t nfs server01-nfs.mycompany.com/export/fusion_imf/appohs_imf/u02_ hostname/instance/CommonDomain_webtier_local /u02/instance/CommonDomain_ webtier_local`

## 2.3 Set Up Upgrade Directories and Obtain Software

Perform the following steps to set up upgrade directories and obtain software required for the upgrade:

- Create a Common User Group and Permissions for Shared Directories

- Create Directories in a Shared Location

- Create Directories Common to One Environment

- Download and Unzip the Patch Conflict Manager Utility

- Download and Unzip Repository and Patches for the Upgrade from Release 5 to Release 6

- Download and Unzip Repository and Patches for Release 6 to Release 7 Upgrade

- Unzip Orchestration.zip

### 2.3.1 Create a Common User Group and Permissions for Shared Directories

The following steps outline the process for setting up permissions on directories that are shared across multiple hosts and are used by Oracle Fusion Applications Upgrade Orchestrator. These steps are required if you use different operating system (OS) users and groups to own Oracle Fusion Applications components (FA, FMW, and IDM) on the hosts in the Oracle Fusion Applications environment (Primordial, OHS, and IDM). An OS user and group is considered to be the same across all hosts only if the corresponding IDs (User ID and Group ID) are also the same across the hosts. The minimum requirement for Upgrade Orchestrator is that the files in the *SHARED_LOCATION* must be owned by the same group. All OS users that own Oracle Fusion Applications components on various hosts must belong to the common group, in addition to other groups to which they already belong. Note that the *SHARED_LOCATION* must be exported with the `no_root_squash` option, or its equivalent, to allow root user access to files in the *SHARED_LOCATION* that are owned by the applications user. For more information about the *SHARED_LOCATION*, see Section 2.3.2, "Create Directories in a Shared Location". For Windows, see Section 2.3.1.1, "Set Up Shared Folders and Permissions on Windows".

1. Determine the OS group and Group ID that you want to use for owning the shared directories. As an example, you can use `orch` as the common group to be used across the hosts.

2. The following steps must be executed as a privileged OS user, such as `root`, on all hosts that participate in orchestration.

   a. Create the common group, if needed.

   ```
   (Linux) /usr/sbin/groupadd -g group_ID -f group_name

   (Solaris) /usr/sbin/groupadd -g group_ID group_name

   (AIX) /usr/bin/mkgroup id=group_ID group_name
   ```

   b. Add each distinct Oracle Fusion Applications component (FA, FMW, DB, IDM) OS owner on each host to the common group.

   ```
   (Linux) /usr/sbin/usermod -a -G group_name component_OS_owner

   (Solaris)  EXISTING_GROUPS=$(grep -w component_OS_owner /etc/group |awk -F:
   '{print $1}' |xargs echo | sed 's/ /,/g')
   /usr/sbin/usermod -G ${EXISTING_GROUPS},group_name component_OS_owner
   ```

```
(AIX) lsgroup -a users group_name
/usr/bin/chgroup users=list_of_existing_users,component_OS_owner group_name
```

You must log out of any sessions that were open prior to this change for OS users being modified, and then log in again so the changes take effect.

**c.** Mount the file system to be used for the shared directories on all hosts.

**d.** Perform the following steps on one of the hosts, such as the primordial host.

■ Create a top-level directory that is passed to orchestration under which additional directories and files are created during orchestration. This directory is referred to as *SHARED_LOCATION* and is further described in Section 2.3.2, "Create Directories in a Shared Location".

■ Perform the following steps before any additional content is created in the shared directories. These steps are applicable to Linux and UNIX platforms, such as AIX, Solaris Sparc and Solaris X64.

– Change the group ownership of the top-level directory to the common group, such as `orch`.

```
(Linux and UNIX) chgrp common_group SHARED_LOCATION
```

– Set permissions on the directory so that the group has read, write, and access privileges.

```
(Linux and UNIX) chmod g+r,g+w,g+x SHARED_LOCATION
```

– Set the Directory group ID bit for the top-level shared directory. This allows for any subdirectories and files created under this shared directory to be owned by the same group, regardless of the host from where they are created.

```
(Linux and UNIX) chmod g+s SHARED_LOCATION
```

**3.** Perform the following steps on all hosts that participate in orchestration. You must be logged in as the OS user that owns the Oracle Fusion Applications content on the host when you run these steps.

**a.** Set the default mask for files so that the group has sufficient privileges on the files.

```
umask 0007
```

**b.** Confirm that the group changes are effective. The `groups` command displays all groups that the current OS user belongs to. You must confirm that the common group, `orch`, is one of them.

```
(Linux and UNIX) groups
```

**c.** Confirm that the permissions are set up correctly on each host. To do this, you can create a temporary file in the shared directory and confirm that the file is owned by the common group and that its permissions are correct. For directories, the group should have read, write, and execute privilege. For files, the group should have at least read and write privileges. Run the following commands after you create the temporary file.

The following command should show that the file is owned by the common group:

```
(Linux and Unix)) ls -ls file_name
```

The following command prints the group and group ID ownership for the file.

```
(Linux) stat --printf="%G %g\n" file_name

(Solaris) echo "group: `ls -ld file_name|awk '{print $4}'" "`"; echo
"groupid:`ls -dn file_name | awk '{print $4}'" "`"

(AIX) istat file_name | grep Group
```

Then remove the temporary file.

---

**Note:** When you unzip the contents of a ZIP archive into the shared folder, the group ownership can be lost on some folders and files. This issue is specific to the unzip utility. To work around the issue, run the following commands when you extract contents to the shared folder:

```
jar -xvf ZIP_archive
unzip -q -o ZIP_archive
```

---

4. Ensure file permissions are correct by performing the following steps, as a prerequisite to starting orchestration.

   a. Change directory to *FA_ORACLE_HOME*/hcm/hrc/bin.

   b. Run `chmod -R 755 *`.

   c. During the running of RUP Installer, `patch_stage` directories are created in a location which is parallel to the *APPLICATIONS_BASE* directory. If the user ID who is running the upgrade does not have write permissions, the **Consolidating Repository and Downloaded Patches** configuration assistant will report a failure. To avoid this failure during the upgrade, ensure that the user who runs Upgrade Orchestrator has write permissions on the top level directory parallel to the *APPLICATIONS_BASE* directory, which is typically `/net/mount1`.

### 2.3.1.1 Set Up Shared Folders and Permissions on Windows

Perform the following steps for Windows on one of the hosts, for example, Host1

1. Create a top-level folder, such as C:\Shared on Host1, that will be passed to orchestration, and under which additional folders and files are created during orchestration.

2. Perform the following steps before any additional content is created in the top-level folder. Repeat these steps to share the top-level folder to one or more Windows Domain users who will be accessing this top-level folder from the hosts in the Oracle Fusion Applications environment (Primordial, OHS, RDBMS, and IDM).

   a. In Windows Explorer, right click on the top-level folder and select Properties from the context menu.

   b. In the Properties window, click the Sharing tab, then click Share.

   c. In the File Sharing window, enter the domain user name using the format *DomainName\userid*.

   d. Click **Add**. This adds the given domain user name to the list of users whom the folder is shared with.

  **e.** Select the domain user name that has been added and change the permission level to Read/Write.

  **f.** Click Share and then click Done to save and close the File Sharing window.

  **g.** Click Close to close the Properties window.

This shared folder can be accessed via the path `\\Host1\Shared`.

**3.** Perform the following steps on all the hosts that participate in orchestration.

  **a.** Log in to the host using the `DomainName\userid` you used in Step c.

  **b.** Create a symlink (C:\Shared) using following command:

```
mklink /D C:\Shared  \\Host1\Shared
```

## 2.3.2 Create Directories in a Shared Location

Create the directories required for the upgrade in a shared location that is accessible to all host types, including scaled out hosts, in your Oracle Fusion Applications environment. This location is referred to as *SHARED_LOCATION* in this Upgrade Guide.

> **Note:** If you are upgrading more than one environment, those environments can be configured to access this *SHARED_LOCATION* to avoid duplicating the software downloads. These directories must also be available to all users and if different users create any of the directories, the users must belong to the same shared group.

The directory names in this section are suggested names and are referenced throughout the upgrade steps. You can choose to use your own naming conventions. See Figure 1–4, "Directory Structure of Downloaded Patches and Repositories" for more information.

> **Note:** Avoid creating any repository in a deeply nested directory on Windows. The Windows PATH variable has a limited size, and long directory names may cause it to overflow. For example, `c:\work\my_repository` is a better choice than `c:\Work\WorkInProgress\FusionApps\FusionAppsv1\Nov2012\tempfiles\my_repository`.

### 2.3.2.1 Patch Conflict Manager Directory

Create the following directory for the Patch Conflict Manager utility:

- *SHARED_LOCATION/*patchConflictManager

### 2.3.2.2 Release 6 Repository Directories

Create the following directories for Release 6 if you are upgrading from Release 5:

- *SHARED_LOCATION/*11.1.6.0.0/Repository

- *SHARED_LOCATION/*11.1.6.0.0_post_repo_patches

- *SHARED_LOCATION/*11.1.6.0.0/IDM

### 2.3.2.3 Release 7 Repository Directories

Create the following directories for Release 7:

- *SHARED_LOCATION*/11.1.7.0.0/Repository

- *SHARED_LOCATION*/11.1.7.0.0_post_repo_patches

- *SHARED_LOCATION*/11.1.7.0.0/IDM

- *SHARED_LOCATION*/11.1.7.0.0/LanguagePacks (required only if you have installed languages other than US English)

#### 2.3.2.4  HCM Workforce Reputation Directory

This section is applicable only if you plan to use the Human Capital Management (HCM) Workforce Reputation Management product packaged with the Workforce Deployment, or Workforce Development product offerings.

Create the following directory or confirm that it exists for HCM Workforce Reputation if you use HCM. Also update the permissions on this directory. The directory should be created and should be accessible from the host where HWR app is provisioned. In an Oracle VM environment, WorkforceReputationServer_1 is allocated to the secondary node in the OVM template for Release 7, therefore this directory needs to be created only on the secondary node.

- (Unix) mkdir /mnt/hwrrepo

  (Windows) mkdir \mnt\hwrrepo

- Use the following command to grant directory permission to the user and group who own the Oracle Fusion Applications WLS domains.

  chown *user_id*:*group_name* /mnt/hwrrepo

- Use the following command to set the correct read and write permission to the directory.

  chmod 750 /mnt/hwrrepo

### 2.3.3  Create Directories Common to One Environment

Create the directories described in this section in shared storage that is available to all users and all host types within the environment that is getting upgraded. Although not mandatory, these directories can also be configured to be shared across other environments.

#### 2.3.3.1  Orchestration Checkpoint Locations

Create the following directories for storing checkpoint information:

- ORCHESTRATION_CHECKPOINT_LOCATION

  This is a shared location available to all hosts in the environment where orchestration checkpoint related files are saved. Ensure that you select a shared mount point that has high disk I/O performance, especially for writing. Orchestration framework automatically creates *POD_NAME* under the directory you specify. This location is stored in the ORCHESTRATION_CHECKPOINT_LOCATION property in the pod.properties file. It is a best practice not to use *ORCH_LOCATION*/config as a value for this property.

- ORCHESTRATION_CHECKPOINT_ARCHIVE_LOCATION

  This is a shared location available to all hosts in the environment where orchestration checkpoint related files are saved. Ensure that you select a shared mount point that has high disk I/O performance, especially for writing. Orchestration framework automatically archives the checkpoint file stored under

the *POD_NAME* directory in the directory specified by the `ORCHESTRATION_`
`CHECKPOINT_LOCATION` property. This location is stored in the `ORCHESTRATION_`
`CHECKPOINT_ARCHIVE_LOCATION` property in the `pod.properties` file. It is a best
practice not to use *ORCH_LOCATION*`/config` as a value for this property.

### 2.3.3.2 Shared Upgrade Location

Create a directory referred to as *SHARED_UPGRADE_LOCATION*. This is a temporary
directory required by the upgrade to copy files and perform write operations. Ensure
that you select a shared mount point that is shared across all hosts for a given
environment that has high disk I/O performance, especially for writing. This area can
be cleaned up after all of your environments have been successfully upgraded to
Release 7.

Also create the following directory:

*SHARED_UPGRADE_LOCATION*`/healthchecker/common`

Grant the group that you created in Section 2.3.1, "Create a Common User Group and
Permissions for Shared Directories" write access on the checkpoint location and shared
upgrade directories that you created in this section.

## 2.3.4 Download and Unzip the Patch Conflict Manager Utility

Download and unzip the latest version of patch 16572470 from My Oracle Support
into the *SHARED_LOCATION*`/patchConflictManager` directory. Ensure that you unzip
this patch as the same user that runs the upgrade.

## 2.3.5 Download and Unzip Repository and Patches for the Upgrade from Release 5 to Release 6

If you are upgrading from Release 6, proceed to Section 2.3.6, "Download and Unzip
Repository and Patches for Release 6 to Release 7 Upgrade". Download the following
repositories and patches for upgrading from Release 5 to Release 6 if you are
performing a chained upgrade from Release 5 to Release 6 to Release 7:

### 2.3.5.1 Download and Unzip the Release 6 Repository

Perform the following steps to download the Release 6 repository from the Oracle
Fusion Applications Product Media Package.

1. Go to http://edelivery.oracle.com.

2. Complete the Export Validation process by entering basic identification
   information using the online form.

3. On the Media Pack Search page, select Oracle Fusion Applications as the product
   pack and then select your platform to identify the media pack you want to
   download.

4. Choose the appropriate media pack from the search results, such as Release 6
   (11.1.6.0.0) for your platform, and download the Release repository (in zipped
   format) to *SHARED_LOCATION*`/11.1.6.0.0/Repository`.

5. Extract the contents of all zipped files to the same target directory, *SHARED_*
   *LOCATION*`/11.1.6.0.0/Repository`.

For more information, see "Obtaining the Software" in the *Oracle Fusion Applications
Installation Guide*.

### 2.3.5.2 Download and Unzip Mandatory Post-Release 6 Patches

> **Note:** If there are no post-release patches in Release 6 Oracle Fusion Applications release notes when you upgrade, there is no action required for this step and you can proceed to Section 2.3.6, "Download and Unzip Repository and Patches for Release 6 to Release 7 Upgrade".

Upgrade Orchestrator can apply mandatory post-release patches that are required by Oracle Fusion Applications if you download the patches from My Oracle Support before you start the upgrade. Note that this feature relates only to patches that are documented in Oracle Fusion Applications release notes and that are specifically required for 11*g* Release 6 (11.1.6).

Perform the following steps to download patches for Release 6:

1. Unzip `SHARED_LOCATION/11.1.7.0.0/Repository/installers/pre_install/PostRepoPatchDirs.zip` in the `11.1.6.0.0_post_repo_patches` directory, which is part of the repository you downloaded in Section 2.3.6.1, "Download and Unzip the Release 7 Repository", to create the directory structure for the patches you download.

2. Review the README file that was created when you unzipped `PostRepoPatchDirs.zip,` to learn how the subdirectories under the `11.1.6.0.0_post_repo_patches` directory map to the corresponding components, such as Oracle Fusion Middleware, database client, and database server components.

3. Refer to the section titled "Upgrade Known Issues, Pre-Upgrade Known Issues, Mandatory Patches to be Downloaded" in Oracle Fusion Applications release notes for Release 6 to find any additional patches to be downloaded from My Oracle Support.

   The following table describes the types of patches that you download and where to find the list of patches in Oracle Fusion Applications release notes.

*Table 2–5    Mandatory Post-Release Patches to be Downloaded*

| Type of Patches | Location in Oracle Fusion Applications release notes | Orchestrator Step or Utility That Applies the Patches |
|---|---|---|
| Oracle Database | Upgrade Known Issues, Pre-Upgrade Known Issues, Mandatory Patches to be Downloaded, Oracle Database | RUP Lite for RDBMS |
| Oracle Fusion Middleware | Upgrade Known Issues, Pre-Upgrade Known Issues, Mandatory Patches to be Downloaded, Oracle Fusion Middleware | Apply Pre-PSA Middleware Patches and Apply Post-PSA Middleware Patches |
| Oracle HTTP Server (OHS) | Upgrade Known Issues, Pre-Upgrade Known Issues, Mandatory Patches to be Downloaded, Oracle HTTP Server (OHS) | Upgrade Oracle Fusion Applications WebTier (RUP Lite for OHS) |
| Oracle Fusion Applications | Upgrade Known Issues, Pre-Upgrade Known Issues, Mandatory Patches to be Downloaded, Oracle Fusion Applications | Apply Downloaded Patches |
| Oracle Fusion Applications LCM Tools | Upgrade Known Issues, Pre-Upgrade Known Issues, Mandatory Patches to be Downloaded, Oracle Fusion Applications Patch Manager | Update LCM Tools |

*Table 2–5   (Cont.)  Mandatory Post-Release Patches to be Downloaded*

| Type of Patches | Location in Oracle Fusion Applications release notes | Orchestrator Step or Utility That Applies the Patches |
| --- | --- | --- |
| Oracle Fusion Applications LCM Tools for Oracle VM | Upgrade Known Issues, Pre-Upgrade Known Issues, Mandatory Patches to be Downloaded, Oracle Fusion Applications Patch Manager | Install Oracle Fusion Applications LCM Tools for Oracle VM |

4. Download and unzip the patches listed in the Release Notes for Oracle Fusion Applications 11g Release 6 (11.1.6), into the appropriate subdirectory under the `11.1.6.0.0_post_repo_patches` directory, based on the mapping information in the README file described in Step 2. Downloading a patch to the incorrect directory could result in failure.

   If your database tier runs on a different platform from Oracle Fusion Applications or Oracle Fusion Middleware, you must download RUP Lite for RDBMS specifically for the platform on which your database tier runs.

5. This step assumes that you have downloaded the patches as described in Step 4. Create a patch plan by running the Perl script, `adCreateMosPlan.pl` for Oracle Fusion Applications patches.

   > **Note:**   This step is only applicable for Oracle Fusion Applications patches using Oracle Fusion Applications Patch Manager.

   The `adCreateMosPlan.pl` script is typically located in *SHARED_LOCATION*`/11.1.6.0.0/Repository/installers/farup/Disk1/upgrade/bin`. If the latest LCM patch bundle is included in the downloaded LCM Tools patches, then `adCreateMosPlan.pl` is located in `download_location_for_lcm_patches_only/`*patch_bundle_patch_number/* `files/lcm/ad/bin`.

   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 PATH /u01/APPLTOP/dbclient/perl/bin:$PATH
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
SHARED_
LOCATION/11.1.6.0.0/Repository/installers/farup/Disk1/upgrade/bin/adCreateMosPl
an.pl 11.1.6.0.0_post_repo_patches

(Windows)
set PATH /u01/APPLTOP/dbclient/perl/bin;PATH
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
%SHARED_
LOCATION/11.1.6.0.0/Repository%\installers\farup\Disk1\upgrade\bin\adCreateMosP
lan.pl 11.1.6.0.0_post_repo_patches
```

An excerpt from a sample patch plan follows:

```
- <fapatchexecplan>
  <generated_date>20130531</generated_date>
  <fapatchutilversion>1.1</fapatchutilversion>
- <group_list>
- <group>
- <patch>
  <id>33001</id>
  <description />
  <artifact_type>BIP</artifact_type>
  <language>US</language>
  </patch>
  </group>
- <group>
- <patch>
  <id>9912345</id>
  <description />
  <artifact_type>SOA</artifact_type>
  <language>US</language>
  </patch>
  </group>
  </group_list>
  </fapatchexecplan>
```

## 2.3.6 Download and Unzip Repository and Patches for Release 6 to Release 7 Upgrade

Download the following repositories and patches for upgrading to Release 7:

### 2.3.6.1 Download and Unzip the Release 7 Repository

The Release repository contains all patches that are required to upgrade to Release 7 in an existing Oracle Fusion Applications environment. Perform the following steps to download the repository from the Oracle Fusion Applications Product Media Package:

1. Go to http://edelivery.oracle.com.

2. Complete the Export Validation process by entering basic identification information using the online form.

3. On the Media Pack Search page, select Oracle Fusion Applications as the product pack and then select your platform to identify the media pack you want to download.

4. Choose the appropriate media pack from the search results, such as Release 7 (11.1.7) for your platform, and download the Release repository (in zipped format) to *SHARED_LOCATION*/11.1.7.0.0/Repository.

5. Extract the contents of all zipped files to the same target directory, *SHARED_ LOCATION*/11.1.7.0.0/Repository.

For more information, see "Obtaining the Software" in the *Oracle Fusion Applications Installation Guide*.

### 2.3.6.2 Download and Unzip Release 7 Language Packs

For each language installed in your environment, download the Release 7 language pack from http://edelivery.oracle.com to the *SHARED_ LOCATION*/11.1.7.0.0/LanguagePacks directory. The location of where you download the language packs is recorded in the REL7_LP_REPOSITORY_LOCATION property in the Primordial host properties file, as described in Table B–2, " PRIMORDIAL.properties".

You can run the following SQL*Plus query to find all installed languages in your environment:

```
select LANGUAGE_TAG, ISO_LANGUAGE, ISO_TERRITORY from FND_LANGUAGES where
INSTALLED_FLAG in ('I', 'B')
```

Note that if you are running the chained upgrade from Release 5 to Release 6 to Release 7, you download language packs only for Release 7 and not for Release 6.

### 2.3.6.3 Download and Unzip Mandatory Post-Release 7 Patches

> **Note:** If there are no post-release patches in Release 7 Oracle Fusion Applications release notes when you upgrade, there is no action required for this step and you can proceed to Section 2.3.7, "Unzip Orchestration.zip".

Upgrade Orchestrator can apply mandatory post-release patches that are required by Oracle Fusion Applications if you download the patches from My Oracle Support before you start the upgrade. Note that this feature relates only to patches that are documented in Oracle Fusion Applications release notes and that are specifically required for 11*g* Release 7 (11.1.7).

Perform the following steps to download patches for Release 7:

1. Unzip *SHARED_LOCATION*/11.1.7.0.0/Repository/installers/pre_
   install/PostRepoPatchDirs.zip, which is part of the repository you downloaded
   in Section 2.3.6.1, "Download and Unzip the Release 7 Repository", in the
   11.1.7.0.0_post_repo_patches directory to create the directory structure for the
   patches you download.

2. Review the README file that was created when you unzipped
   PostRepoPatchDirs.zip, to learn how the subdirectories under the 11.1.7.0.0_
   post_repo_patches directory map to the corresponding components, such as
   Oracle Fusion Middleware, database client, and database server components.

3. Refer to the section titled "Upgrade Known Issues, Pre-Upgrade Known Issues,
   Mandatory Patches to be Downloaded" in Oracle Fusion Applications release
   notes for Release 7 to find any additional patches to be downloaded from My
   Oracle Support. Note that if you stage a patch which contains translated content
   and is translatable, you will also need to stage the corresponding translated
   patches for the active languages.

   The following table describes the types of patches that you download and where
   to find the list of patches in Oracle Fusion Applications release notes.

*Table 2–6    Mandatory Post-Release Patches to be Downloaded*

| Type of Patches | Location in Oracle Fusion Applications release notes | Orchestrator Step or Utility That Applies the Patches |
|---|---|---|
| Oracle Database | Upgrade Known Issues, Pre-Upgrade Known Issues, Mandatory Patches to be Downloaded, Oracle Database | RUP Lite for RDBMS |
| Oracle Fusion Middleware | Upgrade Known Issues, Pre-Upgrade Known Issues, Mandatory Patches to be Downloaded, Oracle Fusion Middleware | Apply Pre-PSA Middleware Patches and Apply Post-PSA Middleware Patches |

*Table 2–6   (Cont.) Mandatory Post-Release Patches to be Downloaded*

| Type of Patches | Location in Oracle Fusion Applications release notes | Orchestrator Step or Utility That Applies the Patches |
|---|---|---|
| Oracle HTTP Server (OHS) | Upgrade Known Issues, Pre-Upgrade Known Issues, Mandatory Patches to be Downloaded, Oracle HTTP Server (OHS) | Upgrade Oracle Fusion Applications WebTier (RUP Lite for OHS) |
| Oracle Fusion Applications | Upgrade Known Issues, Pre-Upgrade Known Issues, Mandatory Patches to be Downloaded, Oracle Fusion Applications | Apply Downloaded Patches |
| Oracle Fusion Applications Release 7 Installer | Upgrade Known Issues, Pre-Upgrade Known Issues, Mandatory Patches to be Downloaded, Installer | Oracle Fusion Applications Upgrade Installer |
| Oracle Fusion Applications LCM Tools | Upgrade Known Issues, Pre-Upgrade Known Issues, Mandatory Patches to be Downloaded, Oracle Fusion Applications Patch Manager | Update LCM Tools |
| Oracle Fusion Applications LCM Tools for Oracle VM | Upgrade Known Issues, Pre-Upgrade Known Issues, Mandatory Patches to be Downloaded, Oracle Fusion Applications Patch Manager | Install Oracle Fusion Applications LCM Tools for Oracle VM |

4. Download and unzip the patches listed in the Release Notes for Oracle Fusion Applications 11*g* Release 7 (11.1.7), into the appropriate subdirectory under the `11.1.7.0.0_post_repo_patches` directory, based on the mapping information in the README file described in Step 2. Downloading a patch to the incorrect directory could result in failure.

   If your database tier runs on a different platform from Oracle Fusion Applications or Oracle Fusion Middleware, you must download RUP Lite for RDBMS specifically for the platform on which your database tier runs.

5. This step assumes that you have downloaded the patches as described in Step 4. Create a patch plan by running the Perl script, `adCreateMosPlan.pl`, for Oracle Fusion Applications patches.

   > **Note:** This step is only applicable for Oracle Fusion Applications patches using Oracle Fusion Applications Patch Manager.

   The `adCreateMosPlan.pl` script is typically located in *SHARED_LOCATION*/`11.1.7.0.0/Repository/installers/farup/Disk1/upgrade/bin`. If the latest LCM patch bundle is included in the downloaded LCM Tools patches, then `adCreateMosPlan.pl` is located in `download_location_for_lcm_patches_only/`*patch_bundle_patch_number*/ `files/lcm/ad/bin`.

   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 PATH /u01/APPLTOP/dbclient/perl/bin:$PATH
   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
SHARED_
LOCATION/11.1.7.0.0/Repository/installers/farup/Disk1/upgrade/bin/adCreateMosPl
an.pl 11.1.7.0.0_post_repo_patches

(Windows)
set PATH /u01/APPLTOP/dbclient/perl/bin;PATH
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
%SHARED_
LOCATION%/11.1.7.0.0/Repository\installers\farup\Disk1\upgrade\bin\adCreateMosP
lan.pl 11.1.7.0.0_post_repo_patches
```

An excerpt from a sample patch plan follows:

```
- <fapatchexecplan>
  <generated_date>20130531</generated_date>
  <fapatchutilversion>1.1</fapatchutilversion>
- <group_list>
- <group>
- <patch>
  <id>33001</id>
  <description />
  <artifact_type>BIP</artifact_type>
  <language>US</language>
  </patch>
  </group>
- <group>
- <patch>
  <id>9912345</id>
  <description />
  <artifact_type>SOA</artifact_type>
  <language>US</language>
  </patch>
  </group>
  </group_list>
  </fapatchexecplan>
```

### 2.3.6.4 Download the Invalid Objects Patch for Exclusion List

Sets of validations are performed at various stages of the upgrade. One such validation is the check for database objects in an invalid state. In certain scenarios, a set of objects gets into an invalid state during intermediate stages of an upgrade and can be safely ignored. The list of objects to be ignored is delivered as a file through a downloadable patch.

Download patch 17051994 from My Oracle Support and copy all files named as FA*overrides.xml, from the patch to the *SHARED_UPGRADE_ LOCATION/*healthchecker/common directory. You may need to create this directory if it does not already exist.

## 2.3.7 Unzip Orchestration.zip

Perform the following steps to download and unzip the latest versions of Orchestration.zip and the Health Checker framework.

1. The latest version of the `Orchestration.zip` file will be uploaded to patch 16979658 on My Oracle Support after Release 7 is released. To ensure you have the latest version of `Orchestration.zip`, download patch 16979658 from My Oracle Support. The patch contains `Orchestration.zip`, `readme.txt`, and the `validateOrchVersion.sh` script. Extract the patch contents to a temporary location.

   > **Note:** Do not download the patch while Orchestration is running or while upgrade orchestration exits due to a pause point or a failure. This patch can be downloaded and used only in case of restoring the environments to the original state. For this case, the upgrade must be started from the beginning.

   If you do not find patch 16979658, no new version of `Orchestration.zip` was released yet, so use the `Orchestration.zip` file that is delivered in the Release 7 Repository, located at *SHARED_LOCATION*`/11.1.7.0.0/Repository/installers/farup/Disk1/upgrade/orchestration`.

2. Unzip the `Orchestration.zip` file from the appropriate location, as described in Step 1, to *SHARED_LOCATION*. Unzip the `Orchestration.zip` file as the same operating system user that was used to set up the Oracle Fusion Applications environment. If you unzip the file as a different user, refer to Section 2.3.1, "Create a Common User Group and Permissions for Shared Directories".

   When you unzip `Orchestration.zip`, a directory named `orchestration` is created. This directory is referred to as *ORCH_LOCATION*. For more information, see Section 1.6.1, "Directories Used by Upgrade Orchestrator".

3. If you downloaded the latest `Orchestration.zip` file from the patch in Step 1, run the `validateOrchVersion.sh` script to validate the version of `Orchestration.zip`. This will confirm that the correct `Orchestration.zip` file has been unzipped to the shared storage location:

   `validateOrchVersion.sh` *ORCH_LOCATION*

   If the script finishes with errors, ensure that the *ORCH_LOCATION* argument passed to the command is correct and that it points to the location where the latest `Orchestration.zip` file was unzipped. If the argument is correct, contact Oracle Support for further assistance.

4. `Orchestration.zip` contains the Health Checker framework. After unzipping `Orchestration.zip`, ensure you have the latest version of Health Checker by downloading patch 16979832 from My Oracle Support. If this patch is not available, use the Health Checker packaged with `Orchestration.zip`.

5. If the patch is available, unzip patch 16979832. Then copy the contents of the `lcm/hc` directory in this patch, to the *ORCH_LOCATION*`/fusionapps/applications/lcm/hc` directory. Overwrite the contents in this directory. If this patch is not available, there are no newer versions of Health Checker.

## 2.4 Set Up Upgrade Orchestrator

Perform the steps in this section to set up Upgrade Orchestrator.

### 2.4.1 Set Up Upgrade Orchestrator on a Shared Location

Perform the following steps to set up Upgrade Orchestrator on a shared location.

1. Perform this step only if you are on Windows.

   - Install python from
     http://www.python.org/ftp/python/2.7.3/python-2.7.3.msi

   - Edit registry HKEY_CLASSES_ROOT/py_auto_file/shell/open/command

     ```
     "C:\Python27\python.exe" "%1" %*
     ```

2. Run the `orchsetup` script on the primordial host. (Ensure that you run this script only on an environment that is Release 5 or higher.)

   ```
   (UNIX)
   cd ORCH_LOCATION/bin
   ./orchsetup.py -r SHARED_LOCATION/11.1.7.0.0/Repository --appbase APPLICATIONS_
   BASE

   (Windows)
   cd ORCH_LOCATION\bin
   orchsetup.py -r SHARED_LOCATION\11.1.7.0.0\Repository --appbase APPLICATIONS_
   BASE
   ```

3. Create a subdirectory to contain setup files for the machine or environment that you are upgrading, using a name that you define, in the *ORCH_LOCATION*/config directory.

   This location can be configured to be shared across multiple environments that are being upgraded. In this case, this location is referred to as *POD_NAME*. For example, you could use this location for your test, production, and development environments, if you are upgrading all three environments to Release 7.

   ```
   cd ORCH_LOCATION/config
   mkdir POD_NAME
   ```

4. Copy the following template files to the directory you created in Step 3, without using the template extension, as shown in the following examples:

   ```
   cd ORCH_LOCATION/config/
   cp MIDTIER.properties.template POD_NAME/MIDTIER.properties
   cp PRIMORDIAL.properties.template POD_NAME/PRIMORDIAL.properties
   cp IDM.properties.template POD_NAME/IDM.properties
   cp OHS.properties.template POD_NAME/OHS.properties
   cp pod.properties.template POD_NAME/pod.properties
   cp silent.rsp.template POD_NAME/silent.rsp
   ```

### 2.4.2 Bootstrap Upgrade Orchestrator

Perform the following steps to prepare Upgrade Orchestrator to upgrade your environment.

- Select a Master Orchestration Password

- Prepare RUP Lite for OVM

- Prepare to Register Database Schema Information

- Prepare to Register System User Information

- Update Orchestrator Properties Files

### 2.4.2.1 Select a Master Orchestration Password

The next three steps require a master orchestration password. Select a password at this time, which is referred to as the "Master Orchestration Password" in this documentation. Note that this password must be a minimum of 8 characters long and it must contain at least one alphabetic character and at least one numeric or special character.

### 2.4.2.2 Prepare RUP Lite for OVM

---

**Note:** Perform the steps in this section only if you are running Oracle Fusion Applications in an Oracle VM environment that was created from the official releases of Oracle VM templates for Oracle Fusion Applications Release 2 (11.1.2) and higher. This content is not applicable for any Oracle VM environments that are created using other methods.

To determine if the Oracle VM environment was created from official releases of Oracle VM templates for Oracle Fusion applications Release 2 and higher, you can verify if the `/assemblybuilder` directory is present in the Oracle VM environment. This confirms that the environment is an OVAB. To confirm the release version, you must review the `.labelinfo.txt` and `.misclabels.txt` files in the `u01/APPLTOP/ovabext` directory to check the rehydration labels that correlate to the release version.

---

Perform the steps for both Release 6 and Release 7 if you are upgrading from Release 5. Otherwise, perform only the steps for Release 7.

- Prepare RUP Lite for OVM for Release 6

- Prepare RUP Lite for OVM for Release 7

Refer to Section A.2.3, "RUP Lite for OVM Utility" to see the overall flow of running RUP Lite for OVM during the upgrade.

**2.4.2.2.1 Prepare RUP Lite for OVM for Release 6** Perform the following steps to install the Oracle Fusion Applications 11.1.6.0.0 Lifecycle Management Tools for Oracle VM Installer repository on the Oracle VM hosts. This repository includes RUP Lite for OVM.

1. The latest version of the `fasaaslcmtools.zip` file will be uploaded to patch 17451957 on My Oracle Support. To ensure that you have the latest version of `fasaaslcmtools.zip`, download patch 17451957 from My Oracle Support. The patch contains `fasaaslcmtools.zip`, `readme.txt`, `validate.py`, and `validate.label`. Extract the contents of the patch to a temporary location.

2. If you do not find patch 17451957, no new version of `fasaaslcmtools.zip` was released yet, and you can obtain `fasaaslcmtools.zip` from the Release 6 *OVAB_HOME*. *OVAB_HOME* is the top-level directory for the Oracle Virtual Assembly Builder that contains all software needed to deploy Oracle Fusion Applications as an Oracle VM instance.

3. Unzip `fasaaslcmtools.zip` to a temporary location and ensure that you specify this *temporary_location*/`fasaaslcmtools` location in the `REL6_SAAS_LCM_INSTALLER_DIR` property in the `pod.properties` file. For more information, see Table B–1, "pod.properties".

4. Copy the entire contents of the *REL6_SAAS_LCM_INSTALLER_ DIR*/Disk1/preupg/rupliteovm directory to *SHARED_LOCATION/ORCH_ LOCATION/config/POD_NAME*/11.1.6.0.0/rupliteovm.

5. Run validate.py, from the location where the patch was downloaded in step 1, to ensure that the correct fasaaslcmtools is used for the upgrade, using the following command syntax:

```
validate.py fasaaslcmtools_SHIPHOME_LOCATION
```

The value for *SHIPHOME_LOCATION* is the value for the REL6_SAAS_LCM_INSTALLER_ DIR property from Step 3. If the script finishes with errors, confirm that the command and the argument passed to it are correct. If both values are correct, contact Oracle Support for further assistance.

6. Update the env.properties file under the *SHARED_LOCATION/ORCH_ LOCATION/config/POD_NAME*/11.1.6.0.0/rupliteovm/metadata directory with the required property values for the following plug-ins:

- **PreUpgradeCredentials** (runs in wallet mode)

  The first property enables the validation of passwords by prompting twice for the required credentials. Do not set the ovm.plugin.PreUpgradeCredentials.enable_password_update property to true before running Upgrade Orchestrator, because orchestration will hang while waiting for a response.

  ```
  ovm.plugin.PreUpgradeCredentials.enable_password_validation=true
  ovm.plugin.PreUpgradeCredentials.enable_password_update=false
  ```

- **SetupCredentials** (runs in offline and online mode)

  The first property enables the validation of passwords by prompting twice for the required credentials. If you need to change the password in the wallet, set the second property to true. This allows you to overwrite the existing password for a specific plug-in the wallet.

  ```
  ovm.plugin.SetupCredentials.enable_password_validation=true
  ovm.plugin.SetupCredentials.enable_password_update=false
  ```

- **ApplyMemorySettings** (runs in offline mode)

  ```
  ovm.plugin.ApplyMemorySettings.enabled=true
  ```

- **SetServerPassphrase** (runs in offline mode)

  ```
  ovm.plugin.SetServerPassphrase.enabled=true
  ```

- **GenerateOptimizedQueryPlans** (runs in offline mode)

  ```
  ovm.plugin.GenerateOptimizedQueryPlans.enabled=true
  ```

- **UpdateHTTPProxySettings** (runs in offline mode)

  ```
  ovm.plugin.UpdateHTTPProxySettings.enabled=true
  ```

- **UpdateWLSUmask** (runs in offline mode)

  ```
  ovm.plugin.UpdateWLSUmask.enabled=true
  ```

- **ConfigureODIAgent** (runs in offline mode)

  ```
  ovm.plugin.ConfigureODIAgent.enabled=true
  ```

- **UpdateSESDBConnection** (runs in online mode)

  ```
  ovm.plugin.UpdateSESDBConnection.enabled=true
  ```

  If your environment originated from Oracle Fusion Applications Release 2 (11.1.2), you must also add the following values:

  ```
  faovm.ha.fusiondb.new.port
  faovm.ha.fusiondb.new.rac.port1
  faovm.ha.fusiondb.new.rac.port2
  ```

- **DeployECSF** (runs in online mode)

  ```
  ovm.plugin.DeployECSF.enabled=true
  ovm.plugin.DeployECSF.connection_timeout_seconds=300
  ```

- **DisableWebchatConnections** (runs in online mode)

  ```
  ovm.plugin.DisableWebchatConnections.enabled=true
  ```

  Note that although this plugin disables the WebChat connections for Oracle Fusion Applications, the CRM Managed Server requires a bounce after the upgrade, before WebChat connections are fully removed.

- **UpdateResolvConf** (runs in post-root mode)

  If you have additional DNS servers, search domains, or want to set options such as time-out and attempt, set the following properties and run this plug-in.

  If no additional DNS servers, search domains or options are needed, disable this plug-in so it does not run.

  ```
  ovm.plugin.UpdateResolvConf.enabled=true

  # Optional additional dns name server IP addresses (comma delimited)
  #example: ovm.plugin.UpdateResolvConf.dns_servers=ip_address,ip_address
  ovm.plugin.UpdateResolvConf.dns_servers=

  # Optional additional resolv.conf options (comma delimited)
  #example: ovm.plugin.UpdateResolvConf.options=timeout:1,attempts:2
  ovm.plugin.UpdateResolvConf.options=

  # Optional additional resolv.conf search domains (comma delimited)
  #example: ovm.plugin.UpdateResolvConf.search=example.com,x.example.com
  ovm.plugin.UpdateResolvConf.search=
  ```

  The `dns_servers property` is a comma separated list of IP addresses of the DNS servers to add to the /etc/resolv.conf file.

- **EnableEMRemoteMonitoring** (runs in post-root mode)

  ```
  ovm.plugin.EnableEMRemoteMonitoring.enabled=true
  ```

- Confirm that the `OVM_STORAGE_MOUNT` and `APPLTOP` properties in the `env.properties` file are set correctly, for example, `OVM_STORAGE_MOUNT=/u01` and `APPLTOP=/u01/APPLTOP`.

7. Create a custom wallet directory under *SHARED_LOCATION/ORCH_LOCATION/config/POD_NAME*/11.1.6.0.0, using a name of your choice.

8. Update the `CUSTOM_WALLET_DIR` property in the *SHARED_LOCATION/ORCH_LOCATION/config/POD_NAME*/11.1.6.0.0/rupliteovm/metadata/env.properties

file so that it contains the absolute path of the directory name you created in Step 7.

9. Run RUP Lite for OVM in wallet mode:

```
setenv JAVA_HOME java_home_directory
cd SHARED_LOCATION/ORCH_LOCATION/config/POD_NAME/11.1.6.0.0/rupliteovm
bin/ruplite.sh wallet
```

Enter the credentials for active plug-ins. Use the Master Orchestration Password that you selected in Section 2.4.2.1, "Select a Master Orchestration Password".

10. Verify that the wallet was created under the custom wallet directory you created in Step 7. If no credentials were required then the wallet will not be created.

**2.4.2.2.2  Prepare RUP Lite for OVM for Release 7**  Perform the following steps to install the Oracle Fusion Applications 11.1.7.0.0 Lifecycle Management Tools for Oracle VM Installer repository on the Oracle VM hosts. This repository includes RUP Lite for OVM.

1. The latest version of the `fasaaslcmtools.zip` file, after Release 7 is released, will be uploaded to patch 17291862  on My Oracle Support. To ensure that you have the latest version of `fasaaslcmtools.zip`, download patch 17291862  from My Oracle Support. The patch contains `fasaaslcmtools.zip`, `readme.txt`, `validate.py`, and `validate.label`. Extract the contents of the patch to a temporary location.

2. If you do not find patch 17291862, no new version of `fasaaslcmtools.zip` was released yet, and you can obtain `fasaaslcmtools.zip` from the Release 7 *OVAB_HOME*. *OVAB_HOME* is the top-level directory for the Oracle Virtual Assembly Builder that contains all software needed to deploy Oracle Fusion Applications as an Oracle VM instance.

3. Unzip `fasaaslcmtools.zip` to a temporary location and ensure that you specify this *temporary_location*/`fasaaslcmtools` location in the `REL7_SAAS_LCM_INSTALLER_DIR` property in the `pod.properties` file. For more information, see Table B–1, " pod.properties".

4. Copy the entire contents of the *REL7_SAAS_LCM_INSTALLER_DIR*/Disk1/preupg/rupliteovm directory to *SHARED_LOCATION/ORCH_LOCATION*/config/*POD_NAME*/11.1.7.0.0/rupliteovm.

5. Run `validate.py`, from the location where the patch was downloaded in step 1, to ensure that the correct `fasaaslcmtools` is used for the upgrade, using the following command syntax:

```
validate.py fasaaslcmtools_SHIPHOME_LOCATION
```

The value for *SHIPHOME_LOCATION* is the value for the `REL7_SAAS_LCM_INSTALLER_DIR` property from Step 3. If the script finishes with errors, confirm that the command and the argument passed to it are correct. If both values are correct, contact Oracle Support for further assistance.

6. Update the `env.properties` file under the *SHARED_LOCATION/ORCH_LOCATION*/config/*POD_NAME*/11.1.7.0.0/rupliteovm/metadata directory with the required property values for the following plug-ins:

   - **PreUpgradeCredentials** (Runs in wallet mode. If no credentials are required, a wallet will not be created.)

     This plug-in prompts for all secure properties that are required by all RUP Lite for OVM plug-ins. It stores these properties in a wallet file, which is encrypted

using a key that you provide. If a wallet already exists, you must provide a key that is valid for the wallet. If the wallet does not exist, a new wallet is created using the key you provide. If a secure property already exists in the wallet, you are not prompted for it again. Update the following properties for this plug-in:

```
ovm.plugin.PreUpgradeCredentials.enable_password_validation=true
ovm.plugin.PreUpgradeCredentials.enable_password_update=false
```

The first property enables the validation of passwords by prompting twice for the required credentials.

This plug-in also has a secure property, RUP Lite Wallet Key, which is requested if the wallet must be created or accessed.

- **SetupCredentials** (runs in offline, pre-root, online, and post-root mode)

  The first property enables the validation of passwords by prompting twice for the required credentials. If you need to change the password in the wallet, set the second property to true. This allows you to overwrite the existing password for a specific plug-in the wallet.

---

**Note:** Do not set the `ovm.plugin.PreUpgradeCredentials.enable_password_update` property to true before running Upgrade Orchestrator, because orchestration will hang while waiting for a response.

---

```
ovm.plugin.SetupCredentials.enable_password_validation=true
ovm.plugin.SetupCredentials.enable_password_update=false
```

- **ApplyMemorySettings** (runs in offline mode)

  ```
  ovm.plugin.ApplyMemorySettings.enabled=true
  ```

- **GenerateOptimizedQueryPlans** (runs in offline mode)

  ```
  ovm.plugin.GenerateOptimizedQueryPlans.enabled=true
  ```

- **DisableSearchUI** (runs in offline mode)

  ```
  ovm.plugin.DisableSearchUI.enabled=true
  ```

- **UpdateFusionIIRDiag** (runs in offline mode)

  ```
  ovm.plugin.UpdateFusionIIRDiag.enabled=true
  ```

- **DisableWebchat** (runs in offline mode)

  ```
  ovm.plugin.DisableWebchat.enabled=true
  #password for root login to webchat OVM
  ```

- **RemoveNetAppJar** (runs in offline mode)

  ```
  ovm.plugin.RemoveNetAppJar.enabled=true
  ```

- **UpdateSOAUnicastConfiguration** (runs in offline mode)

  ```
  ovm.plugin.UpdateSOAUnicastConfiguration.enabled=true
  ```

- **FixEPMRegistry** (runs in offline mode)

  ```
  ovm.plugin.FixEPMRegistry.enabled=true
  ```

- **FixEMDProperties** (runs in offline mode)

  ```
  ovm.plugin.FixEMDProperties.enabled=true
  ```

- **UpdateTopologyManagerInternalHosts** (runs in offline mode)

  ```
  ovm.plugin.UpdateTopologyManagerInternalHosts.enabled=true
  ```

- **FixEtcHosts** (runs in pre-root mode)

  ```
  ovm.plugin.FixEtcHosts.enabled=true
  ```

- **SetupOHSInstanceHome** (runs in pre-root mode)

  ```
  ovm.plugin.SetupOHSInstanceHome.enabled=true
  ```

- **DeployECSF** (runs in online mode)

  ```
  ovm.plugin.DeployECSF.enabled=true
  ovm.plugin.DeployECSF.connection_timeout_seconds=300
  ```

- **DisableWebchatConnections** (runs in online mode)

  ```
  ovm.plugin.DisableWebchatConnections.enabled=true
  ```

  Note that although this plugin disables the WebChat connections for Oracle Fusion Applications, the CRM Managed Server requires a bounce after the upgrade, before WebChat connections are fully removed.

- **ConfigureBIEmailDelivery** (runs in online mode)

  ```
  ovm.plugin.ConfigureBIEmailDelivery.enabled=true

  # BI Delivers Email Specific Properties
  #Sender display name for email From: field
  ovm.plugin.ConfigureBIEmailDelivery.email_senderdisplayname=
  #Sender email address for Reply-To: field - REQUIRED
  ovm.plugin.ConfigureBIEmailDelivery.email_senderemailaddress=
  #Email SMTP host - REQUIRED
  ovm.plugin.ConfigureBIEmailDelivery.bemail_smtpserver=localhost
  #Email SMPT port - REQUIRED
  ovm.plugin.ConfigureBIEmailDelivery.email_smtpserverport=port_number
  ```

- **UpdateResolvConf** (runs in post-root mode)

  If you have additional DNS servers, search domains, or want to set options such as time-out and attempt, set the properties below and run this plugin.

  If no additional DNS servers, search domains or options are needed, disable this plugin so it does not run.

  ```
  ovm.plugin.UpdateResolvConf.enabled=true

  # Optional additional dns name server IP addresses (comma delimited)
  #example: ovm.plugin.UpdateResolvConf.dns_servers=ip_address,ip_address
  ovm.plugin.UpdateResolvConf.dns_servers=

  # Optional additional resolv.conf options (comma delimited)
  #example: ovm.plugin.UpdateResolvConf.options=timeout:1,attempts:2
  ovm.plugin.UpdateResolvConf.options=

  # Optional additional resolv.conf search domains (comma delimited)
  #example: ovm.plugin.UpdateResolvConf.search=example.com,x.example.com
  ```

```
ovm.plugin.UpdateResolvConf.search=
```

The `dns_servers property` is a comma separated list of IP addresses of the DNS servers to add to the `/etc/resolv.conf` file.

- **DisableWebchatRoot** (runs in post-root mode)

  ```
  ovm.plugin.DisableWebchatRoot.enabled=true
  ```

- **PostHostRehydrate** (runs in post-root mode)

  ```
  ovm.plugin.PostHostRehydrate.enabled=true
  ```

- Confirm that the `OVM_STORAGE_MOUNT` and `APPLTOP` properties the `env.properties` file are set correctly, for example, `OVM_STORAGE_MOUNT=/u01` and `APPLTOP=/u01/APPLTOP`.

7. Create a custom wallet directory under *SHARED_LOCATION/ORCH_LOCATION/config/POD_NAME*/11.1.7.0.0, using a name of your choice.

8. Update the `CUSTOM_WALLET_DIR` property in the *SHARED_LOCATION/ORCH_LOCATION/config/POD_NAME*/11.1.7.0.0/rupliteovm/metadata/env.properties file so that it contains the absolute path of the directory you created in Step 7.

9. Run RUP Lite for OVM in wallet mode.

   ```
   setenv JAVA_HOME java_home_directory
   cd SHARED_LOCATION/ORCH_LOCATION/config/POD_NAME/11.1.7.0.0/rupliteovm
   bin/ruplite.sh wallet
   ```

   Enter the credentials for active plug-ins. Use the Master Orchestration Password that you selected in

10. Verify that the wallet was created under the custom wallet directory you created in Step 7. If no credentials were required then the wallet will not be created.

### 2.4.2.3 Prepare to Register Database Schema Information

Some new Release 7 features require that all database schemas be registered in the credential store. Perform the following steps to ensure that all database schemas are registered in the credential store. Note that this step needs to be run only once, even if you are performing a chained upgrade from Release 5 to Release 6 to Release 7, and this step must be run on the primordial host.

1. Apply patches related to the credential store to *FA_ORACLE_HOME*, depending on whether your upgrade is from Release 5 to Release 6 to Release 7, or if your upgrade is from Release 6 to Release 7.

   a. Unzip the contents of *SHARED_LOCATION*/11.1.7.0.0/Repository/installers/pre_install/credstorepatches.zip and *SHARED_LOCATION*/11.1.7.0.0/Repository/installers/pre_install/pcupatches.zip to a temporary location, referred to as *temp_location*.

   b. If you are performing the chained upgrade from Release 5 to Release 6 to Release 7, unzip and apply the following patches using `opatch`. If you are starting your upgrade to Release 7 from Release 6, proceed to Step c:

   ```
   temp_location/p16699884_Generic.zip
   temp_location/p16605586_Generic.zip
   ```

   **c.** Unzip and apply the following patches using `opatch` when upgrading from Release 6 to Release 7:

```
temp_location/p16699893_Generic.zip
temp_location/p16605596_Generic.zip
```

**2.** Ensure the files in the *FA_ORACLE_HOME*/lcm/util/bin directory have read, write, and execute permissions.

**3.** Set the JAVA_HOME environment variable before running any commands in this section.

```
(UNIX)
cd APPLICATIONS_BASE/fusionapps/applications/lcm/util/bin
setenv JAVA_HOME java_home_location

(Windows)
cd APPLICATIONS_BASE\fusionapps\applications\lcm\util\bin
set JAVA_HOME=java_home_location
```

> **Note:** You must run all commands in this section from *APPLICATIONS_BASE*/fusionapps/applications/lcm/util/bin.

**4.** Run the templateGen utility to create the csf_template.ini template file.

```
(UNIX)
./templateGen.sh -appbase APPLICATIONS_BASE

(Windows)
templateGen.cmd -appbase APPLICATIONS_BASE
```

For the -appbase argument, specify the complete directory path to the APPLICATIONS_BASE directory.

The templateGen utility generates the following template files in the *APPLICATIONS_CONFIG*/lcm/admin/pcu directory:

- standard_template.ini
- csf_template.ini
- validation_template.ini
- system_user_template.ini
- standard_template.properties
- csf_template.properties

The command also generates the pcu_output.xml file in the same directory.

**5.** Make a copy of csf_template.ini from the *APPLICATIONS_CONFIG*/lcm/admin/pcu directory. In this example, the copy is named csf_plain.ini.

**6.** Manually edit csf_plain.ini as follows:

- Set the master_password property to the Master Orchestration Password you selected in Section 2.4.2.1, "Select a Master Orchestration Password".

- For each line that contains #text# or #password#, replace #text# or #password# with the correct value for your environment. Note that this password must be a minimum of 8 characters long and it must contain at least one alphabetic character and at least one numeric or special character.

> **Note:**  To prevent incorrect results, do not alter `csf_plain.ini` beyond these changes.

**7.** Create an encrypted version of `csf_plain.ini` and delete the clear-text input file. This step requires an encryption tool, such as the `lcmcrypt` tool or the Linux `gpg` tool, that takes an encrypted file and a passphrase and writes the decrypted contents to the standard output. In the following example, using `lcmcrypt`, the command reads the passphrase from the standard input and produces an encrypted output file, `csf_plain.ini.enc`.

```
(UNIX)
echo password | ./lcmcrypt.sh -nonInteractive -encrypt -inputfile complete_
directory_path/csf_plain.ini
```

```
(Windows)
echo password | lcmcrypt.cmd -nonInteractive -encrypt -inputfile complete_
directory_path\csf_plain.ini
```

**8.** Run `iniGen.sh` in non-interactive mode, which also requires a decryption tool, to take an encrypted file and a passphrase and write the decrypted contents to the standard output. The following example uses `lcmcrypt`:

```
(UNIX)
echo password | ./lcmcrypt.sh -nonInteractive -decrypt -inputfile complete_
directory_path/csf_plain.ini.enc | ./iniGen.sh -nonInteractive -templatefile
APPLICATIONS_CONFIG/lcm/admin/pcu/csf_template.ini -outputfile APPLICATIONS_
CONFIG/lcm/admin/pcu/csf_encrypted.ini -appbase APPLICATIONS_BASE
```

```
(Windows)
echo password | lcmcrypt.cmd -nonInteractive -decrypt -inputfile complete_
directory_path\csf_plain.ini.enc | .\iniGen.cmd -nonInteractive -templatefile
APPLICATIONS_CONFIG\lcm\admin\pcu\csf_template.ini -outputfile APPLICATIONS_
CONFIG\lcm\admin\pcu\csf_encrypted.ini -appbase APPLICATIONS_BASE
```

The call to `lcmcrypt` reads the passphrase from the standard input and writes the clear text version of `csf_plain.ini.enc` to the standard output, which is then piped to the standard input of `iniGen.sh`.

`iniGen.sh` uses the value of the `master_password` property to encrypt all other passwords in the generated input file. It also alters the value of the `master_password` property back to `master_password=ignore_me` in the generated input file.

**9.** Update the `CSF_ENCRYPTED_FILE` property in `PRIMORDIAL.properties` with the full directory path and file name for `APPLICATIONS_CONFIG/lcm/admin/pcu/csf_encrypted.ini`. For more information, see Table B–2, " PRIMORDIAL.properties".

For more information about the utilities used in this process, see "Changing Oracle Fusion Applications Passwords in the Oracle Database" in the *Oracle Fusion Applications Administrator's Guide*.

### 2.4.2.4  Prepare to Register System User Information

Perform the following steps to prepare passwords for system users. Note that this step needs to be run only once, even if you are performing the chained upgrade from Release 5 to Release 6 to Release 7.

1. Make a copy of `system_user_template.ini` from the *APPLICATIONS_ CONFIG*/lcm/admin/pcu/ directory. In this example, the copy is named `system_ user_plain.ini`.

2. Manually edit `system_user_plain.ini` as follows:

   - Set the `master_password` property to the Master Orchestration Password you selected in Section 2.4.2.1, "Select a Master Orchestration Password".

   - For each line that contains `#text#` or `#password#`, replace `#text#` or `#password#` with the correct value for your environment.

   - If you are not running Oracle Fusion Applications in an Oracle VM environment, update the `FUSION_APPS_PATCH_ID_STORE_READONLY-KEY` property to the value of `IDROUser` in the `USERS` section by making the following update:

     ```
     FUSION_APPS_PATCH_ID_STORE_READONLY-KEY=IDROUser
     ```

     > **Note:** You must run all commands in this section from *APPLICATIONS_BASE*/fusionapps/applications/lcm/util/bin.

3. Create an encrypted version of `system_user_plain.ini` and delete the clear-text input file. This step requires an encryption tool, such as the `lcmcrypt` tool or the Linux `gpg` tool, that takes an encrypted file and a passphrase and writes the decrypted contents to the standard output. In the following example, using `lcmcrypt`, the command reads the passphrase from the standard input and produces an encrypted output file, `system_user_plain.ini.enc`.

   ```
   (UNIX)
   echo password | ./lcmcrypt.sh -nonInteractive -encrypt -inputfile complete_
   directory_path/system_user_plain.ini
   ```

   ```
   (Windows)
   echo password | lcmcrypt.cmd -nonInteractive -encrypt -inputfile complete_
   directory_path\system_user_plain.ini
   ```

4. Run `iniGen.sh` in non-interactive mode, which also requires a decryption tool, to take an encrypted file and a passphrase and write the decrypted contents to the standard output. The following example uses `lcmcrypt`:

   ```
   (UNIX)
   echo password | ./lcmcrypt.sh -nonInteractive -decrypt -inputfile complete_
   directory_path/system_user_plain.ini.enc | ./iniGen.sh -nonInteractive
   -templatefile APPLICATIONS_CONFIG/lcm/admin/pcu/system_user_template.ini
   -outputfile APPLICATIONS_CONFIG/lcm/admin/pcu/system_user_encrypted.ini
   -appbase APPLICATIONS_BASE
   ```

   ```
   (Windows)
   echo password | lcmcrypt.cmd -nonInteractive -decrypt -inputfile complete_
   directory_path\system_user_plain.ini.enc | iniGen.cmd -nonInteractive
   -templatefile APPLICATIONS_CONFIG\lcm\admin\pcu\system_user_template.ini
   -outputfile APPLICATIONS_CONFIG\lcm\admin\pcu\system_user_encrypted.ini
   -appbase APPLICATIONS_BASE
   ```

   The call to `lcmcrypt` reads the passphrase from the standard input and writes the clear text version of `system_user_plain.ini.enc` to the standard output, which is then piped to the standard input of `iniGen.sh`.

iniGen.sh uses the value of the `master_password` property to encrypt all other passwords in the generated input file. It also alters the value of the `master_password` property back to `master_password=ignore_me` in the generated input file.

In Section 2.4.2.5, "Update Orchestrator Properties Files", you update the `CSF_SYSTEM_USERS_ENCRYPTED_INI` property in `PRIMORDIAL.properties` with the location of the generated `system_user_encrypted.ini` file.

5. Make a note of the following information, which you will need in subsequent steps of the upgrade process.

   ■ The master orchestration password

   ■ The location and file name for the .ini file, `system_user_encrypted.ini`.

6. Perform the following steps if you are running on a Windows platform. Ensure that the Administration Server of the common domain is running for this step.

   a. Set the *JAVA_HOME* environment variable. If *APPLICATIONS_BASE* is located at `c:\AT`, set the *JAVA_HOME* as follows:

   ```
   set JAVA_HOME=c:\AT\fusionapps\jdk6
   ```

   b. Start the Administration Server of the common domain.

   c. Run the following command.

   ```
   c:\AT\fusionapps\applications\lcm\util\bin\schemaPasswordChangeTool.cmd
   -inputfile C:\AT\instance\lcm\admin\pcu\system_user_encrypted.ini -appbase
   c:\AT
   ```

### 2.4.2.5 Update Orchestrator Properties Files

Update the properties files which are located in the *ORCH_LOCATION*/config/*POD_NAME* directory. Note that if any property values are updated while orchestration is running, the new values do not take effect until you start a new orchestration session. Detailed information about each property exists in the property file. For a list of properties, see Appendix B, "Upgrade Orchestrator Properties Files".

---

> **Note:** The following HOSTNAME properties must contain a host name: HOSTNAME_PRIMORDIAL, HOSTNAME_MIDTIER, HOSTNAME_PRIMARY, HOSTNAME_SECONDARY, HOSTNAME_BIINSTANCE, HOSTNAME_OSN, HOSTNAME_OHS, HOSTNAME_IDMOID, HOSTNAME_IDMOIM, HOSTNAME_IDMOHS. When running on single-node environments, the HOSTNAME_OSN property in `pod.properties` should be blank because OSN is not supported on single-node environments. Note that on Windows, the host name is case sensitive and can be obtained from the Control Panel, under System, then Full computer name.

---

## 2.5 Verify Your Environment Before Proceeding to Down Time

Perform the following steps to verify your environment before you proceed to down time steps:

■ Confirm Database Settings

■ Confirm JDeveloper Customizations Can Be Merged

■ Maintain Versions of Customized BI Publisher Reports

- Verify the FUSION User Quota on FUSION_TS* Tablespaces

- Validate Domain Directories

- Verify the Node Manager Configuration is Correct

- Ensure the `registered` Property is Set to True on OHS Registered Domains

- Verify the Default Realm Name is myrealm

- Register Oracle Homes in Central Inventory (Windows Only)

- Run Health Checker on the Database Host

- Install the MKS Toolkit (Windows Only)

### 2.5.1 Confirm Database Settings

Refer to Release Notes for Oracle Fusion Applications 11*g* Release 7 (11.1.7) to verify that your database and Sql*Net tuning parameters are set properly to avoid time-out errors during the upgrade.

### 2.5.2 Confirm JDeveloper Customizations Can Be Merged

If you performed JDeveloper customizations to a SOA composite and then you deployed the composite to the SOA runtime, you must perform manual steps to merge your customizations during the installation. To ensure that your customizations can be merged successfully, review the recommendations in "Merging Runtime Customizations from a Previously Deployed Revision into a New Revision" in the *Oracle Fusion Applications Extensibility Guide for Developers* before you start Upgrade Orchestrator.

You will merge your customizations after the **SOA Preverification** configuration assistant fails during the upgrade. For more information, see Section 6.16.6, "Merging SOA Composite JDeveloper Customizations During SOA Preverification".

### 2.5.3 Maintain Versions of Customized BI Publisher Reports

Ensure that you have your own versions of any customized BI Publisher reports. If an upgrade 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 for Business Analysts*.

### 2.5.4 Verify the FUSION User Quota on FUSION_TS* Tablespaces

The FUSION user must have an unlimited quota on all FUSION_TS* tablespaces.

Run the following query to verify that the FUSION user has an unlimited quota on all FUSION_TS* tablespaces:

```
select tablespace_name, max_bytes from dba_ts_quotas where username = 'FUSION';
```

The FUSION user must have a value of -1 for max_bytes on all FUSION_TS* tablespaces. If any tablespace does not have the correct value or does not have an entry, you must grant the unlimited quota by running the following command:

```
alter user FUSION quota unlimited on tablespace_name;
```

## 2.5.5 Validate Domain Directories

Run the `validatedomains` script to confirm that all Administration Server domain locations are detectable.

If you followed steps to scale out hosts, you may have added the Administration Server of the scaled out host to a new machine. This section provides the steps to temporarily add the Administration Server back to the originally provisioned machine so that all domain directories can be found by Upgrade Orchestrator. During post-upgrade steps, you add the Administration Server back to the machine that was created during scaleout.

Whether are or not you have scaled out hosts, perform the following steps to run the validation for domain locations and to temporarily update the machine for Administration Servers, if needed.

1. Unzip `domainvalidate.zip` from the *SHARED_LOCATION*`/11.1.7.0.0/Repository/installers/farup/Disk1/upgrade/validate` directory into any directory on the primordial host, regardless of whether you are performing a chained upgrade from Release 5 or you are performing a single hop upgrade from Release 6.

2. For Windows, set following environment variables before running `validatedomains.bat`:

   ```
   set JAVA_HOME=c:\AT\fusionapps\jdk6
   set PATH=%PATH%;%JAVA_HOME%\bin
   ```

3. If *FA_MW_HOME* is *APPLICATIONS_BASE/*fusionapps, run the following command.

   ```
   (UNIX) ./validatedomains.sh APPLICATIONS_BASE
   (Windows) validatedomains.bat APPLICATIONS_BASE
   ```

   Example:

   ```
   validatedomains.sh /u01/APPLTOP
   ```

   If *APPLICATIONS_CONFIG* is *APPLICATIONS_BASE/*instance, run the following command.

   ```
   (UNIX) ./validatedomains.sh FA_MW_HOME APPLICATIONS_CONFIG
   (Windows) validatedomains.bat FA_MW_HOME APPLICATIONS_CONFIG
   ```

   Example:

   ```
   validatedomains.sh /u01/APPLTOP/fusionapps /u01/APPLTOP/instance
   ```

4. If the utility reports any domains that failed the validation, and if you have scaled out hosts, perform the following steps on the Administration Server of each of the reported domains:

   > **Note:** If you do not have scaled out hosts and if you have domains listed after the utility was run, contact Oracle Support for further assistance.

   a. Log in to the WebLogic console for the domain.

   b. Navigate to Environment, then Machines.

   c. Find the machine that corresponds to the host name for which the Administration Server was initially provisioned.

    **d.** Click on the machine and go to the Servers tab. Note that the Administration Server should not appear on the list of servers. If it does appear on the list, either this domain passed validation or this is not the originally provisioned machine for the Administration Server.

    **e.** Click **Lock & Edit** to make changes.

    **f.** Click **Add**.

    **g.** Select the AdminServer and click **Finish**.

    **h.** Click **Activate Changes** to apply the changes.

## 2.5.6 Verify the Node Manager Configuration is Correct

Perform the following steps on the `admin-apps/PRIMORDIAL` host to verify that the node manager configuration is correct.

**1.** Review the `config/config.xml` file in each domain directory and check the `MACHINE_NAME` entries. Ensure that for each machine entry, the `node-manager` child element has its own name element that matches the name element of the machine. Refer to the following example:

```
<machine>
  <name>MACHINE_NAME</name>
  <node-manager>
    <name>MACHINE_NAME</name>
    ...
  </node-manager>
</machine>
```

**2.** If any of the `node-manager` elements are missing child name elements, then the configuration must be fixed by using the offline WLST command as described in the following steps:

    **a.** Run the WLST utility to fix the configuration in each domain directory:

```
FMW_ORACLE_HOME/oracle_common/common/bin/wlst.sh
```

    **b.** Open the domain in offline mode:

```
readDomain('PATH_TO_DOMAIN')
```

    **c.** Run the following commands for each affected machine:

```
cd('/Machine/MACHINE_NAME/NodeManager/NodeManager')
set('Name', 'MACHINE_NAME')
```

    **d.** Save the domain and exit WLST:

```
updateDomain()
closeDomain()
exit()
```

**3.** Review the `config.xml` file for each of the affected domain directories and ensure that the name elements are now present.

## 2.5.7 Ensure the `registered` Property is Set to True on OHS Registered Domains

Ensure the `registered` property is set to the correct value on the OHS registered domain. Review the `WT_CONFIG_HOME/config/OPMN/opmn/instance.properties` file to check the value for the `registered` property. If OHS is registered to the domain,

ensure the property is set to "true". If OHS is not registered to the domain, ensure the property is set to "false".

## 2.5.8 Verify the Default Realm Name is myrealm

Upgrade Orchestrator expects the default realm name to be `myrealm` for the Common Domain. Perform the following steps to verify that you have not changed this value to any other name, because changing the name to anything other than `myrealm` causes Upgrade Orchestrator to fail.

1. Log in to the WLS Console for the Common Domain.

2. Click **Security Realms** on the domain structure pane.

3. A list of realms displays in the **Summary of Security Realms** window.

4. Verify there is an entry for `myrealm` and that "true" displays in the Default Realm column.
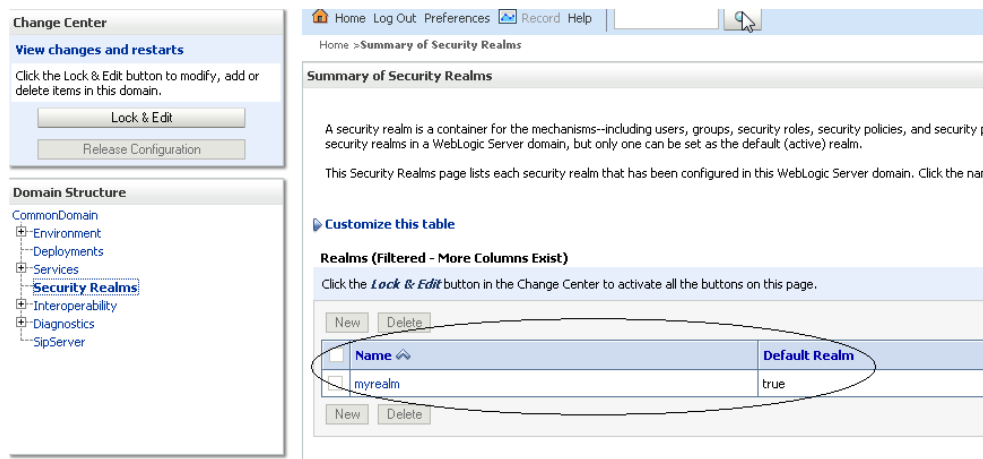


## 2.5.9 Register Oracle Homes in Central Inventory (Windows Only)

Oracle Provisioning records installation information about the following Oracle homes separately from information about other products: Oracle Business Intelligence (Oracle BI), Oracle Global Order Processing (GOP), Web Tier, and Web Tier Common Oracle home. RUP Installer expects information about all products to be recorded in the same place. For more information about home directories, see "Provisioned Oracle Fusion Applications Home Directories" in the *Oracle Fusion Applications Administrator's Guide*.

The following steps describe how to manually register the all missing Oracle homes in central inventory.

1. Verify that the default Inventory Pointer file points to the central inventory on the primordial host on which RUP Installer runs. The default Inventory Pointer is located in the registry key, `\\HKEY_LOCAL_MACHINE\\Software\Oracle\inst_loc`.

2. Run `attachHome` from the BI Oracle home, for example, *APPLICATIONS_BASE*`\fusionapps\bi`.

   (Windows) *BI_HOME*`\oui\bin\attachHome.bat -jreLoc` *JAVA_HOME_LOCATION*

3. Run `attachHome` from the GOP Oracle home, for example, *APPLICATIONS_BASE*`\fusionapps\gop`.

   (Windows) *GOP_HOME*`\oui\bin\attachHome.bat -jreLoc` *JAVA_HOME_LOCATION*

4. Run `attachHome` from the Web Tier Oracle home, for example, *APPLICATIONS_BASE*\webtier_mwhome\webtier.

   (Windows) *WEBTIER_HOME*\oui\bin\attachHome.bat -jreLoc *JAVA_HOME_LOCATION*

5. Run `attachHome` from the Web Tier Common Oracle home, for example, *APPLICATIONS_BASE*\webtier_mwhome\oracle_common.

   (Windows) *WEBTIER_COMMON_HOME*\oui\bin\attachHome.bat -jreLoc *JAVA_HOME_LOCATION*

6. Run `attachHome` from the Web Tier Webgate Oracle home, for example, *APPLICATIONS_BASE\webtier_mwhome\webgate*.

   (Windows) *WEBTIER_WEBGATE_HOME*\oui\bin\attachHome.bat -jreLoc *JAVA_HOME_ LOCATION*

7. Run `attachHome` from the Oracle Common Oracle home, for example, *APPLICATIONS_BASE\fusionapps\oracle_common*.

   (Windows) *COMMON_HOME*\oui\bin\attachHome.bat -jreLoc *JAVA_HOME_LOCATION*

8. Register the dependency between the BI Oracle home and Oracle Common Oracle home.

   Run Oracle Universal Installer with the -updateHomeDeps option and pass a dependency list. The syntax for the dependency list is:

   `HOME_DEPENDENCY_LIST={ORACLE_HOME:DEPENDENT_ORACLE_HOME}`

   Example for Business Intelligence:

   ```
   (Windows) BI_HOME\oui\bin\setup.exe -updateHomeDeps "HOME_DEPENDENCY_LIST=
   {APPLICATIONS_BASE\fusionapps\bi:APPLICATIONS_BASE\fusionapps\oracle_common}"
   -jreLoc JAVA_HOME_LOCATION
   ```

9. Register the dependency between Web Tier Oracle home and Web Tier Common Oracle home.

   ```
   (Windows) WEBTIER_HOME\oui\bin\setup.exe -updateHomeDeps "HOME_DEPENDENCY_LIST=
   {APPLICATIONS_BASE\webtier_mwhome\webtier:APPLICATIONS_BASE\webtier_
   mwhome\oracle_common}"
   jreLoc JAVA_HOME_LOCATION
   ```

10. Verify that the central inventory now contains the correct GOP, BI, and Web Tier information. Open the `inventory.xml` file from the `ContentsXML` subdirectory in your central inventory directory using a text editor. You can find your central inventory directory by looking in the default Oracle Inventory pointer file mentioned in Step 1. Verify that there are entries for GOP and for BI, and that the BI entry lists the Oracle Common dependency you specified in Step 6. Do the same for Web Tier information. Ensure that you do not modify `inventory.xml` in any way, as this may corrupt your system.

    Example entries in `inventory.xml`:

    ```
    <HOME NAME="OH1109401105" LOC="APPLICATIONS_BASE/fusionapps/gop" TYPE="O"
    IDX="11">
    <HOME NAME="OH198367808" LOC="APPLICATIONS_BASE/fusionapps/bi" TYPE="O"
    IDX="12">
        <DEPHOMELIST>
            <DEPHOME LOC="APPLICATIONS_BASE/fusionapps/oracle_common"/>
        </DEPHOMELIST>
    </HOME>
    <HOME NAME="OH987588708" LOC="APPLICATIONS_BASE/webtier_mwhome/webtier"
    ```

```
TYPE="O" IDX="13">
   <DEPHOMELIST>
      <DEPHOME LOC="APPLICATIONS_BASE/webtier_mwhome/oracle_common"/>
   </DEPHOMELIST>
</HOME>
<HOME NAME="OH1271096710" LOC="APPLICATIONS_BASE/webtier_mwhome/oracle_common"
TYPE="O" IDX="14">
   <REFHOMELIST>
      <REFHOME LOC="APPLICATIONS_BASE/webtier_mwhome/webtier"/>
   </REFHOMELIST>
</HOME>
```

> **Note:** Rerunning the ATTACH_HOME command does not cause any
> issues.

## 2.5.10 Run Health Checker on the Database Host

Perform the following steps to run Health Checker from the database host.

1. Create a ZIP archive of the Health Checker framework that exists on the
   primordial host, by extracting the contents from the Release 7 Repository. You
   created this repository, *SHARED_LOCATON/*11.1.7.0.0/Repository, in
   Section 2.3.2.3, "Release 7 Repository Directories".

   Run the following commands:

   ```
   (UNIX)
   setenv APPLICATIONS_BASE APPLICATIONS_BASE
   cd REPOSITORY_LOCATION/installers/farup/Disk1/upgrade
   bin/hczip.py /any_scratch_directory/hc.zip --repoLoc $REPOSITORY_LOCATION

   (Windows)
   set APPLICATIONS_BASE=C:\AT
   cd REPOSITORY_LOCATION\installers\farup\Disk1\upgrade
   bin\hczip.py C:\any_scratch_directory\hc.zip
   ```

2. Use FTP or another method to transfer the hc.zip file to the DB host.

3. Create a directory where you want the Health Checker framework contents to
   reside. You must choose a separate directory that does not overlap with any
   provisioned components. This directory is referred to as *HC_TOP* in this section.

   ```
   mkdir /u01/hcframework
   cd /u01/hcframework
   cp hc.zip /u01/hcframework
   unzip hc.zip
   ```

4. Set the following environment variables:

   – APPLICATIONS_BASE - The *HC_TOP* directory, where hc.zip was unzipped.

   – REPOSITORY_LOCATION - The directory where the repository is staged.

   – JAVA_HOME - The Java home.

   – ORACLE_HOME - The Oracle Database Home directory.

   – PATH - The path to Oracle_home/bin.

   – LISTENER_NAME - The Oracle database listener name.

   – ORACLE_SID - The Oracle database SID.

- TNS_ADMIN - `$ORACLE_HOME/network/admin`.

- LD_LIBRARY_PATH- `$ORACLE_HOME/lib`.

- GRID_HOME - On RAC configurations, set this to GRID_HOME. Otherwise set to ORACLE_HOME.

On Windows, append *ORACLE_HOME/*bin to the current path, as follows:

```
Set PATH=%PATH%;ORACLE_HOME\bin
```

5. Run Health Checker and specify `-hostType` and the `-jreLoc` on this host. Note that `-jreLoc` is the same as the *JAVA_HOME* location for this host.

```
(UNIX)
$REPOSITORY_LOCATION/installers/farup/Disk1/upgrade/bin/hcplug.sh -hostType
[DB|OHS] -jreLoc location_of_Java -manifest
REPOSITORY_
LOCATION/installers/farup/Disk1/upgrade/config/PreDowntimeUpgradeReadinessHealt
hChecks.xml -DlogLevel=FINEST [-logDir logfile_directory]

(Windows)
%REPOSITORY_LOCATION%\installers\farup\Disk1\upgrade\bin\hcplug.cmd -hostType
[DB|OHS] -jreLoc location_of_Java -manifest
REPOSITORY_
LOCATION\installers\farup\Disk1\upgrade\config\PreDowntimeUpgradeReadinessHealt
hChecks.xml -DlogLevel=FINEST [-logDir logfile_directory]
```

6. If Health Checker fails or reports an issue that must be corrected, follow the steps in Section A.2.2.4, "Troubleshoot Health Checker Failures."

### 2.5.11 Install the MKS Toolkit (Windows Only)

Perform the following steps to install the MKS Toolkit on Windows 64 before upgrading:

1. Download and install version MKS Toolkit 9.4p1 (or higher) from http://www.mkssoftware.com.

2. Confirm that c:\mksnt is present in the global PATH variable.

## 2.6 What To Do Next

To proceed with the upgrade on Linux and Windows platform, follow the steps in Section 3, "Updating the Oracle Fusion Applications and Oracle Identity Management Databases".

To proceed with the upgrade for non-Linux or non-Windows platforms, follow the steps in Appendix C, "Platform Specific Pre-Upgrade Steps".

# 3

# Updating the Oracle Fusion Applications and Oracle Identity Management Databases

This chapter describes how to update your Oracle Fusion Applications database before an upgrade.

> **Note:** This is a downtime activity and can be planned and performed in a separate downtime window prior to the upgrade.

If you are upgrading from Release 5, and you use Oracle Exadata Database Machine, start with Section 3.1, "Apply Exadata Patches for Release 6". If you are upgrading from Release 5 and you do not use Oracle Exadata Database Machine, start with Section 3.2, "Run RUP Lite for RDBMS for the Upgrade From Release 5 to Release 6"

If you are upgrading from Release 6, and you use Oracle Exadata Database Machine, start with Section 3.3, "Apply Exadata Patches for Release 7". If you are upgrading from Release 6, and you do not use Oracle Exadata Database Machine, start with Section 3.4, "Run RUP Lite for RDBMS for Upgrade to Release 7".

> **Note:** It is a best practice to apply these patches on Oracle Identity Management databases to keep both the Oracle Fusion Application database and Oracle Identity Management databases synchronized. It is also a best practice to back up your Oracle Fusion Applications and Oracle Identity Management databases before patching. For more information, see "Backing Up and Recovering Oracle Fusion Applications" in the *Oracle Fusion Applications Administrator's Guide*.

## 3.1 Apply Exadata Patches for Release 6

If you use Oracle Exadata Database Machine, manually apply the patches listed in this section, followed by any patches you downloaded in Section 2.3.5, "Download and Unzip Repository and Patches for the Upgrade from Release 5 to Release 6". Do not run RUP Lite for RDBMS.

If you are on Linux64, Solaris Sparc64, or Solaris86-64 platforms and use the Oracle Exadata Database Machine, download and apply the quarterly database patch for your platform, the generic patches in the following list, and the list of specific patches for your platform from My Oracle Support.

After applying the patches for your platform, proceed to Section 3.3, "Apply Exadata Patches for Release 7".

### 3.1.1 Quarterly Database Patches

Apply the quarterly database patch (Patch 14474780 - QUARTERLY DATABASE PATCH FOR EXADATA (OCT 2012 - 11.2.0.3.11) for your platform:

- Linux: p14474780_112030_Linux-x86-64.zip
- Solaris Sparc64: p14474780_112030_SOLARIS64.zip
- Solaris86-64: p14474780_112030_Solaris86-64.zip

### 3.1.2 Generic Exadata Patches

Apply the following generic patches, which are not platform-specific:

- p12317925_112030_Generic.zip
- p13508115_112030_Generic.zip
- p14698700_112030_Generic.zip

### 3.1.3 Linux Exadata Patches

Apply the following Exadata patches if you are on the Linux64 platform:

- p12552578_1120311ExadataDatabase_Linux-x86-64.zip
- p12646746_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
- p13615767_1120311ExadataDatabase_Linux-x86-64.zip
- p13632653_112030_Linux-x86-64.zip
- p13714926_1120311ExadataDatabase_Linux-x86-64.zip
- p13902963_1120311ExadataDatabase_Linux-x86-64.zip
- p14029429_112030_Linux-x86-64.zip
- p14058884_112030_Linux-x86-64.zip
- p14164849_112030_Linux-x86-64.zip
- p14226599_112030_Linux-x86-64.zip
- p14499293_1120311ExadataDatabase_Linux-x86-64.zip
- p14653598_1120311ExadataDatabase_Linux-x86-64.zip
- p14679292_112030_Linux-x86-64.zip
- p14741727_1120311ExadataDatabase_Linux-x86-64.zip
- p14757709_1120311ExadataDatabase_Linux-x86-64.zip
- p14793338_1120311ExadataDatabase_Linux-x86-64.zip
- p14837414_1120311ExadataDatabase_Linux-x86-64.zip

- p15843238_1120311ExadataDatabase_Linux-x86-64.zip

### 3.1.4 Solaris Sparc64 Exadata Patches

Apply the following Exadata patches if you are on the Solaris Sparc64 platform:

- p12552578_1120311ExadataDatabase_SOLARIS64.zip
- p12646746_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
- p13615767_1120311ExadataDatabase_SOLARIS64.zip
- p13632653_112030_SOLARIS64.zip
- p13714926_1120311ExadataDatabase_SOLARIS64.zip
- p13902963_1120311ExadataDatabase_SOLARIS64.zip
- p14029429_112030_SOLARIS64.zip
- p14058884_112030_SOLARIS64.zip
- p14164849_112030_SOLARIS64.zip
- p14226599_112030_SOLARIS64.zip
- p14499293_1120311ExadataDatabase_SOLARIS64.zip
- p14653598_1120311ExadataDatabase_SOLARIS64.zip
- p14679292_112030_SOLARIS64.zip
- p14741727_1120311ExadataDatabase_SOLARIS64.zip
- p14757709_1120311ExadataDatabase_SOLARIS64.zip
- p14793338_1120311ExadataDatabase_SOLARIS64.zip
- p14837414_1120311ExadataDatabase_SOLARIS64.zip
- p15843238_1120311ExadataDatabase_SOLARIS64.zip

### 3.1.5 Solaris 86 X64 Exadata Patches

Apply the following Exadata patches if you are on the Solaris X64 platform:

- p12552578_1120311ExadataDatabase_Solaris86-64.zip
- p12646746_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

- p13615767_1120311ExadataDatabase_Solaris86-64.zip

- p13632653_112030_Solaris86-64.zip

- p13714926_1120311ExadataDatabase_Solaris86-64.zip

- p13902963_1120311ExadataDatabase_Solaris86-64.zip

- p14029429_112030_Solaris86-64.zip

- p14058884_112030_Solaris86-64.zip

- p14164849_112030_Solaris86-64.zip

- p14226599_112030_Solaris86-64.zip

- p14499293_1120311ExadataDatabase_Solaris86-64.zip

- p14653598_1120311ExadataDatabase_Solaris86-64.zip

- p14679292_112030_Solaris86-64.zip

- p14741727_1120311ExadataDatabase_Solaris86-64.zip

- p14757709_1120311ExadataDatabase_Solaris86-64.zip

- p14793338_1120311ExadataDatabase_Solaris86-64.zip

- p14837414_1120311ExadataDatabase_Solaris86-64.zip

- p15843238_1120311ExadataDatabase_Solaris86-64.zip

Proceed to Section 3.3, "Apply Exadata Patches for Release 7."

## 3.2 Run RUP Lite for RDBMS for the Upgrade From Release 5 to Release 6

Run the RUP Lite for RDBMS utility to perform the tasks required to update your Oracle Fusion Applications database before you upgrade. RUP Lite for RDBMS can be run in the following modes:

- **Validate mode:**

    - Validates database parameters as described in Table 3–1

- **Set database parameters mode:**

    - Sets database parameters to the values described in Table 3–1, if required

    - Restarts the database instance, if requested

- **Apply mode:**

    - Stops the listener and shuts down the database instance (optional)

    - Configures Oracle Configuration Manager (OCM) in disconnected mode, if required

    - Unzips Opatch, if it is available in *REPOSITORY_LOCATION*

    - Applies patch set updates (PSUs) and one-off patches in *REPOSITORY_LOCATION*

    - Applies downloaded one-off patches in the 11.1.7.0.0_post_repo_patches directory

    - Starts the listener and the database instance (optional)

- – Runs `catbundle.sql` if any PSUs were applied

- – Runs `catmetx.sql`

- **Apply Post Changes mode:**

  - – Performs SQL*Plus actions after patches apply

Table 3–1 displays the recommendations for tuning the database parameters. The `validate` mode of RUP Lite for RDBMS verifies whether these parameters contain the recommended value. The `setdbparameter` mode of RUP Lite for RDBMS updates the parameters to the recommended value.

*Table 3–1    Recommended Values for Database Parameters*

| Parameter | Type | Location | Recommendation |
|---|---|---|---|
| DISK_ASYNCH_IO | Disk IO | Spfile/pfile | true |
| FILESYSTEMIO_OPTIONS | Disk IO | Spfile/pfile | unset so the database chooses a default value based on the platform |
| INBOUND_CONNECT_ TIMEOUT_listener_name | Connection timeout | *TNS_ ADMIN*/listener.ora | 120 |
| SQLNET.INBOUND_CONNECT_ TIMEOUT | Connection timeout | *TNS_ ADMIN*/sqlnet.ora | 130 |
| ACTIVE_SESSION_LEGACY_ BEHAVIOR | Initialization | Spfile/pfile | true |

RUP Lite for RDBMS uses non-interactive OPatch calls to apply RDBMS patches. OPatch tries to install and configure Oracle Configuration Manager (OCM) if OCM has not already been installed and configured. This causes non-interactive OPatch calls to fail in some cases. To avoid this issue, Oracle recommends that you install OCM prior to running RUP Lite for RDBMS. If you plan to use OCM, you should configure it after you install it. If you do not plan to use OCM, you can either configure it in disconnected mode or let RUP Lite for RDBMS configure it. If you install OCM and do not configure it, RUP Lite for RDBMS will automatically configure it in disconnected mode. For more information, see "Installing Oracle Configuration Manager Using the Command Line Interface" in the *Oracle Configuration Manager Installation and Administration Guide*.

Run RUP Lite for RDBMS to apply the mandatory Oracle Database patches mentioned in the "Oracle Database" section of Oracle Fusion Applications release notes. This step applies Oracle Database patches that reside in both the `REPOSITORY_LOCATION` and the `11.1.6.0.0_post_repo_patches` directories, which you downloaded in Section 2.3.5, "Download and Unzip Repository and Patches for the Upgrade from Release 5 to Release 6". Follow the steps in Section 3.2.1, "Run RUP Lite for RDBMS".

## 3.2.1 Run RUP Lite for RDBMS

If you are running Oracle Fusion Applications on a RAC database, follow the steps in Section 3.2.2, "Run RUP Lite for RDBMS in a RAC Database".

Perform the following steps to run RUP Lite for RDBMS in three modes: `validate`, `setdbparameters`, and `apply`:

1. Verify that your OPatch version is 11.2.0.3.3. If the OPatch version is different, then apply the version of OPatch that is delivered in the Release 6 Repository. It is

available at *REPOSITORY_LOCATION/*installers/database/opatch/p6880880_
112000_Linux-x86-64.zip.

2. Copy the TPBundler.zip file to any temporary directory, such as *work_dir* in the following example:

```
cp REPOSITORY_LOCATION/installers/pre_install/TPBundler.zip work_dir
```

3. Unzip TPBundler.zip in the *work_dir* directory, which contains the following files after unzipping:

```
createTPBundle.jar
createTPBundle.cmd
createTPBundle.sh
ojdl.jar
tpBundleConfig_DB.xml
tpBundleConfig_IDM.xml
tpBundleConfig_OHS.xml
README.txt
```

4. The createTPBundler utility creates the RDBMS patch bundle, DBPatches.zip, and RUP Lite for RDBMS. This patch bundle contains the mandatory prerequisite patches that are delivered in *REPOSITORY_LOCATION* as well as any patches you may have downloaded.

   Use the following command syntax to run createTPBundler, which creates DBPatches.zip in a temporary directory, referred to as *work_dir* in the example. Note that *work_dir* must have read/write permissions.

```
(UNIX)
sh createTPBundle.sh -shiphomelocation REPOSITORY_LOCATION -tempdir work_dir
-target DB [-patchdownloadloc location_of_downloaded_patches]
```

```
(Windows)
createTPBundle.cmd -shiphomelocation REPOSITORY_LOCATION -tempdir work_dir
-target DB [-patchdownloadloc location_of_downloaded_patches]
```

   The following options are available for createTPBundler:

   – -shiphomelocation: Location of the createTPBundler repository.

   – -tempdir: Destination directory to which the generated zip file was copied.

   – -target: Target against which the copy should be initiated. Valid values are IDM, DB, OH. Use the DB value.

   – -patchdownloadloc: Location of the patch directory where you downloaded the patches in Section 2.3.5, "Download and Unzip Repository and Patches for the Upgrade from Release 5 to Release 6". Use this option only if you downloaded patches to a directory other than the default patch download directory, which is 11.1.6.0.0_post_repo_patches.

   – -logfile: Full path of the createTPbundle log file. The default is createTPBundle.log in the current directory.

   – -loglevel: Log level for the createTPbundler utility. Valid values are SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST. The default value is INFO.

5. Copy DBPatches.zip to any temporary directory on the database server host.

6. Log in to the database server host.

7.  Unzip `DBPatches.zip` to any temporary directory on the database server host. The following subdirectories and files exist after unzipping.

```
|-- DB_timestamp
    -- db_server_bundle
        |-- README.txt
        |-- bin
        |   |-- ruplite.bat
        |   |-- ruplite.sh
        |-- metadata
        |   |-- env.properties
        |   |-- installer.properties
        |   |-- plugin-metadata.txt
        |-- custom_db_server
        |    -- database
        |        -- patch
        |            -- downloaded one-off patches
        |-- db_server
        |   |-- database
        |       |-- opatch
        |       |   -- OPatch zip file
        |       |-- patch
        |       |   -- One-off patches in repository
        |       |-- psu
        |       |   -- Patch Set Updates in repository
        |-- db
        |   |--RUP Lite related files
        |-- lib
        |   |--RUP Lite related files
        |-- ruplite
        |   |--RUP Lite related files
        |-- techpatch
        |   |--TPU related files
```

8.  Perform this step only if you are running RUP Lite for RDBMS on an Oracle VM environment.

    As the root user, change the permissions on the DB_*timestamp* subdirectory:

    ```
    chmod -R 777 DB_timestamp
    ```

    Exit out of root user to ensure that you do not perform the remaining steps as root.

9.  Set executable permissions on `ruplite.sh`. (UNIX only)

    ```
    chmod -R 755 DB_timestamp/db_server_bundle/bin/ruplite.sh
    ```

10. Set the `JAVA_HOME` environment variable as shown in the following example:

    ```
    (UNIX)
    setenv JAVA_HOME java_home_location (must be jdk6)

    (Windows)
    set JAVA_HOME=java_home_location (must be jdk6)
    ```

11. Update the following properties in the *work_dir*/DB_*timestamp*/db_server_ bundle/metadata/env.properties file. Example values are shown.

    -   ORACLE_SID: Use an instance name that belongs to the `fusionapps` database.

    -   ORACLE_HOME: Use an Oracle home directory on which patches must be applied, such as `/u01/db/11.2.0.3`.

- TNS_ADMIN: Use a valid location that contains SQL*Net configuration files for the database.

- LISTENER_NAME: Use a listener name.

- PFILE=/u01/db/11.2.0.3/dbs/init.ora, for example. You can retrieve this value by running the following query:

  ```
  select NAME, VALUE from v$parameter where NAME like '%file%';
  ```

  Update the PFILE property if your database is started using pfile.

- DBSERVER_RESTART=true or false.

  To minimize downtime, you can use "false" for setdbparameters mode, and "true" for apply mode.

  If DBSERVER_RESTART is set to "false", the database server, listener and other related services must be manually stopped before running RUP Lite in apply mode. Then after running RUP Lite in apply mode, you must manually run Steps a through d.

  If the value for this property is set to "true", RUP Lite automatically stops the listener and database before applying patches. In addition, RUP Lite automatically performs the following actions after applying patches when DBSERVER_RESTART=true:

  **a.** Start the database instance.

  **b.** Start the listener.

  **c.** Run catbundle.sql with arguments "psu apply" on non-windows and "winbundle apply" on windows.

  ```
  (UNIX)
  $ORACLE_HOME/rdbms/admin/catbundle.sql psu apply

  (Windows)
  %ORACLE_HOME%\rdbms\admin\catbundle.sql winbundle apply
  ```

  For a list of catbundle.sql errors that can be ignored, see Section 6.19.17, "Ignorable Errors Reported by catbundle.sql".

  **d.** Run ORACLE_HOME/rdbms/admin/catmetx.sql.

  ```
  (UNIX)
  $ORACLE_HOME/rdbms/admin/catmetx.sql

  (Windows)
  %ORACLE_HOME%\rdbms\admin\catmetx.sql
  ```

**12.** Verify that the java version is 1.6 or above by using the following command:

```
(UNIX)
$JAVA_HOME/bin/java -version

(Windows)
%JAVA_HOME%\bin\java -version
```

If your version is lower, download 1.6 or a higher version from My Oracle Support.

**13.** Stop all user applications.

**14.** Change directory to the following location:

```
DB_timestamp/db_server_bundle/bin
```

**15.** Run RUP Lite for RDBMS in `validate` mode. The database instance and listener must be up.

```
(UNIX) ruplite.sh validate
(Windows) ruplite.bat validate
```

**16.** Review the log file, `output/logs/ruplitedbvalidate.log`, to confirm whether the database parameters contain the values you set in Step 11 and the values displayed in Table 3–1, " Recommended Values for Database Parameters". If any errors occurred, you can find them in this log file.

If any of the parameters do not contain the recommended value, proceed to the next step to run RUP Lite for RDBMS in `setdbparameters` mode. If all parameters are correct, proceed to Step 19 to run RUP Lite for RDBMS in `apply` mode.

**17.** Run RUP Lite for RDBMS in `setdbparameters` mode. The database instance and listener must be up.

```
(UNIX) ruplite.sh setdbparameters
(Windows) ruplite.bat setdbparameters
```

**18.** Review the log file, `output/logs/ruplitedbsetdbparameters.log`, to confirm whether the database parameters contain the values displayed in Table 3–1, " Recommended Values for Database Parameters". If any errors occurred, you can find them in this log file also.

**19.** Running RUP Lite for RDBMS in `apply` mode starts and stops only the Fusion Applications database listener and the database server. You must stop any other applications or processes that are running from the Oracle Fusion Applications home directory, except the OPSS Security Store, before you run RUP Lite for RDBMS. For more information, see "Starting and Stopping" in the *Oracle Fusion Applications Administrator's Guide*. Also confirm that the BI presentation servers are shut down.

You can set the parameter `DBSERVER_RESTART` (available in `metadata/env.properties`) to "false" if you want to manually shut down the database, stop the listener before patching, and start it up after applying the patches. For Windows, if you set `DBSERVER_RESTART` to "false", follow the steps in Section 3.4.3, "Stop Services on Windows Before Running RUP Lite For RDBMS".

---

**Note:** To avoid an issue with active files while patching, ensure that no applications or processes are running from the `ORACLE_HOME` that is referenced in `metadata/env.properties`. If `DBSERVER_RESTART`=true, you can ignore the database instance and listener processes because RUP Lite brings them down.

---

Run RUP Lite for RDBMS in `apply` mode.

```
(UNIX) ruplite.sh
(Windows) ruplite.bat
```

**20.** Review the following log files located under the `output/logs` directory if any errors occurred:

```
ruplitedb.log
tp_property_editor_timestamp.log
db_apply_downloaded_patches_timestamp.log
db_apply_repository_patches_timestamp.log
```

```
db_validate_downloaded_patches_timestamp.log
db_validate_repository_patches_timestamp.log
downloaded_patch_validate_results_timestamp.xml
repository_patch_validate_results_timestamp.xml
post_db_restart_actions_timestamp.log
```

If RUP Lite for RDBMS fails, resolve the issue reported in the log files. When you restart a failed session, RUP Lite for RDBMS ignores the successful actions, starts with the failed action, and proceeds from that point.

The post_db_restart_actions_*timestamp.*log file includes the output from catbundle.sql and catmetx.sql. For a list of catbundle.sql errors that can be ignored, see Section 6.19.17, "Ignorable Errors Reported by catbundle.sql".

**21.** If you set DBSERVER_RESTART to "false", perform the steps in Step 11, a. through d.

**22.** You must manually execute any manual steps that are documented in the README.txt file of the patches you applied with RUP Lite for RDBMS. RUP Lite for RDBMS does not execute manual steps from the README.txt file of the patch.

**23.** Proceed to Section 3.2.3, "Run Additional Post Database Start Scripts for Patches for Release 6".

## 3.2.2  Run RUP Lite for RDBMS in a RAC Database

Perform the following steps to run RUP Lite for RDBMS in a RAC database. You must run RUP Lite for RDBMS on all available file systems. This may involve multiple hosts and nodes. Note that a single Oracle home can be shared by multiple nodes, and in this case, running RUP Lite on a single node of such a group is sufficient.

**1.** Follow Steps 1 through 10 in Section 3.2.1, "Run RUP Lite for RDBMS".

**2.** Stop all user applications that use the Oracle home directory being patched.

**3.** Update the following properties in the *work_dir*/DB_*timestamp*/db_server_ bundle/metadata/env.properties file. Example values are shown.

- ORACLE_HOME: Use an Oracle home directory on which patches must be applied, such as /u01/db/11.2.0.3.

- ORACLE_SID: Use an instance name that belongs to the fusionapps database and is run against the ORACLE_HOME set in the previous property.

- TNS_ADMIN: Use a valid tns_admin location, which is typically located under the grid infra and contains listener.ora and sqlnet.ora files.

- LISTENER_NAME: Use a listener name.

- PFILE=/u01/db/11.2.0.3/dbs/init.ora, for example. You can retrieve this value by running the following query:

  ```
  select NAME, VALUE from v$parameter where NAME like '%file%';
  ```

  Update the PFILE property if your database is started using pfile.

- DBSERVER_RESTART=false

  Note that the value of DBSERVER_RESTART must be "false".

**4.** Verify that the java version is 1.6 or above by using the following command:

```
(UNIX)
$JAVA_HOME/bin/java -version

(Windows)
```

```
%JAVA_HOME%\bin\java -version
```

5. Change directory to the following location:

   ```
   DB_timestamp/db_server_bundle/bin
   ```

6. Run RUP Lite for RDBMS in `validate` mode. The database instance and listener must be up.

   ```
   (UNIX) ruplite.sh validate
   (Windows) ruplite.bat validate
   ```

7. Review the log file, `output/logs/ruplitevalidate.log`, to confirm whether the database parameters contain the values you set in Step 3 and the values displayed in Table 3–1, " Recommended Values for Database Parameters". If any errors occurred, you can find them in this log file also.

   If any of the parameters do not contain the recommended value, proceed to the next step to run RUP Lite for RDBMS in `setdbparameters` mode. If all parameters are correct, proceed to Step 10.

8. Run RUP Lite for RDBMS in `setdbparameters` mode. The database instance and listener must be up.

   ```
   (UNIX) ruplite.sh setdbparameters
   (Windows) ruplite.bat setdbparameters
   ```

9. Review the log file, `output/logs/ruplitesetdbparameters.log`, to confirm whether the database parameters contain the values displayed in Table 3–1, " Recommended Values for Database Parameters". If any errors occurred, you can find them in this log file also.

10. Shut down all Oracle RAC databases on all nodes in the cluster, even those that are sharing the same host. Database instances that are running could cause issues that prevent patches from applying successfully or you could receive errors because the patches update files that are in use.

    To shut down an Oracle RAC database, enter the following command in a command window, where `CRS_home` is the location of the Grid home directory and `sales` is the name of the database in the following example:

    ```
    (UNIX)
    CRS_home/bin/srvctl stop database -d sales

    (Windows)
    CRS_home\bin\srvctl stop database -d sales
    ```

11. Stop the listener that is running from all Oracle homes in the cluster, using the following command. Note that all services must be shut down if the OIM and OID databases are configured on same listener.

    ```
    (UNIX)
    CRS_home/bin/srvctl stop listener [-l listener_name]

    (Windows)
    CRS_home\bin\srvctl stop listener [-l listener_name]
    ```

12. To avoid an issue with active files while patching, ensure that no applications or processes are running from the ORACLE_HOME that is referenced in `metadata/env.properties`.

13. Run RUP Lite for RDBMS in `apply` mode.

```
(UNIX) ruplite.sh
(Windows) ruplite.bat
```

14. Review the following log files located under the `output/logs` directory if any errors occurred:

```
ruplitedb.log
tp_property_editor_timestamp.log
db_apply_downloaded_patches_timestamp.log
db_apply_repository_patches_timestamp.log
db_validate_downloaded_patches_timestamp.log
db_validate_repository_patches_timestamp.log
downloaded_patch_validate_results_timestamp.xml
repository_patch_validate_results_timestamp.xml
post_db_restart_actions_timestamp.log
```

If RUP Lite for RDBMS fails, resolve the issue reported in the log files. When you restart a failed session, RUP Lite for RDBMS ignores the successful actions, starts with the failed action, and proceeds from that point.

15. RAC databases often share a single ORACLE_HOME for all RAC instances. If you have this configuration, continue to the next step.

If you do not have this configuration, you must update the files in the other ORACLE_HOMEs for your RAC database. To update the other ORACLE_HOMEs, repeat Steps 4 through 8 in Section 3.4.1, "Run RUP Lite for RDBMS" for RAC instances with non-shared ORACLE_HOMEs. Then repeat Steps 3 through 15 in this section for all RAC instances. Note that this may involve multiple hosts and nodes.

16. Start the database.

17. Start the listener from all Oracle homes in the cluster. For Windows, start the services described Section 3.4.3, "Stop Services on Windows Before Running RUP Lite For RDBMS".

18. After the database is started, run the following commands:

```
(UNIX)
cd $ORACLE_HOME/rdbms/admin
sqlplus /nolog
SQL> CONNECT / AS SYSDBA
SQL> @catbundle.sql psu apply
SQL> QUIT

(Windows)
cd %ORACLE_HOME%\rdbms\admin
sqlplus /nolog
SQL> CONNECT / AS SYSDBA
SQL> @catbundle.sql winbundle apply
SQL> QUIT
```

For a list of `catbundle.sql` errors that can be ignored, see Section 6.19.17, "Ignorable Errors Reported by catbundle.sql".

```
(UNIX)
cd $ORACLE_HOME/rdbms/admin
sqlplus /nolog
SQL> CONNECT / AS SYSDBA
SQL> @catmetx.sql
SQL> QUIT
```

```
(Windows)
cd %ORACLE_HOME%\rdbms\admin
sqlplus /nolog
SQL> CONNECT / AS SYSDBA
SQL> @catmetx.sql
SQL> QUIT
```

**19.** Proceed to Section 3.2.3, "Run Additional Post Database Start Scripts for Patches for Release 6".

### 3.2.3 Run Additional Post Database Start Scripts for Patches for Release 6

Perform the following steps on the DB host by any user that has system privileges. Perform these steps on only one of the nodes in the case of a RAC setup. If any of the following steps requires a database stop and start, the same user that performs these steps must also perform the stop and start.

**1.** You must manually execute any additional manual steps that are documented in the README.txt file of the patches applied with RUP Lite for RDBMS. RUP Lite for RDBMS does not execute manual steps from the README.txt file of the patch.

If there is more than one ORACLE_HOME in the RAC database, you do not need to run SQL scripts again when patching the 2nd through the *n*th ORACLE_HOME, but you do need to perform any manual steps that update ORACLE_HOME.

Database patches can be found at the following locations:

*SHARED_UPGRADE_LOCATION/POD_NAME/RELEASE_VERSION/*DB/*HOST_NAME/*RUPLiteDB/DB_
*TIME_STAMP*/db_server_bundle/db_server/database/psu (if it exists)

*SHARED_UPGRADE_LOCATION/POD_NAME/RELEASE_VERSION/*DB/*HOST_NAME/*RUPLiteDB/DB_
*TIME_STAMP*/db_server_bundle/custom_db_server/database/patch (if it exists)

*SHARED_UPGRADE_LOCATION/POD_NAME/RELEASE_VERSION/*DB/*HOST_NAME/*RUPLiteDB/DB_
*TIME_STAMP*/db_server_bundle/db_server/database/patch

Example location:

```
/u01/shared_location/CRM/11.1.6.0.0/DB/racNode1.mycompany.com/RUPLiteDB/DB_
2012-08-06_04-44-01/db_server_bundle/db_server/database/patch/
```

**2.** Proceed to Section 3.4, "Run RUP Lite for RDBMS for Upgrade to Release 7".

## 3.3 Apply Exadata Patches for Release 7

If you are on Linux64, Solaris Sparc64, or Solaris86-64 platforms and use the Oracle Exadata Database Machine, download and apply the generic patches in the following list, and the list of specific patches for your platform from My Oracle Support.

### 3.3.1 Quarterly Database Patches

Apply the quarterly database patch (Patch 14474780 - QUARTERLY DATABASE PATCH FOR EXADATA (OCT 2012 - 11.2.0.3.11) for your platform, if you did not apply these patches in Section 3.1.1, "Quarterly Database Patches".

- Linux: p14474780_112030_Linux-x86-64.zip

- Solaris Sparc64: p14474780_112030_SOLARIS64.zip

- Solaris86-64: p14474780_112030_Solaris86-64.zip

### 3.3.2  Generic Exadata Patches

Apply all of the following generic patches, which are not platform-specific:

- p12317925_112030_Generic.zip
- p13508115_112030_Generic.zip
- p14698700_112030_Generic.zip

### 3.3.3  Linux Exadata Patches

Apply the following Exadata patches if you are on the Linux64 platform:

- p12552578_1120311ExadataDatabase_Linux-x86-64.zip
- p12646746_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
- p13615767_1120311ExadataDatabase_Linux-x86-64.zip
- p13632653_112030_Linux-x86-64.zip
- p13743357_1120311ExadataDatabase_Linux-x86-64.zip
- p13902963_1120311ExadataDatabase_Linux-x86-64.zip
- p14029429_112030_Linux-x86-64.zip
- p14058884_112030_Linux-x86-64.zip
- p14164849_112030_Linux-x86-64.zip
- p14226599_112030_Linux-x86-64.zip
- p14499293_1120311ExadataDatabase_Linux-x86-64.zip
- p14555370_1120311ExadataDatabase_Linux-x86-64.zip
- p14653598_1120311ExadataDatabase_Linux-x86-64.zip
- p14679292_112030_Linux-x86-64.zip
- p14741727_1120311ExadataDatabase_Linux-x86-64.zip
- p14757709_1120311ExadataDatabase_Linux-x86-64.zip
- p14775679_1120311ExadataDatabase_Linux-x86-64.zip
- p14808639_1120311ExadataDatabase_Linux-x86-64.zip
- p14837414_1120311ExadataDatabase_Linux-x86-64.zip
- p15843238_1120311ExadataDatabase_Linux-x86-64.zip
- p16100861_1120311ExadataDatabase_Linux-x86-64.zip
- p16207583_1120311ExadataDatabase_Linux-x86-64.zip
- p16369388_1120311ExadataDatabase_Linux-x86-64.zip

### 3.3.4 Solaris Sparc64 Exadata Patches

Apply the following Exadata patches if you are on the Solaris Sparc64 platform:

- p12552578_1120311ExadataDatabase_SOLARIS64.zip
- p12646746_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
- p13615767_1120311ExadataDatabase_SOLARIS64.zip
- p13632653_112030_SOLARIS64.zip
- p13743357_1120311ExadataDatabase_SOLARIS64.zip
- p13902963_1120311ExadataDatabase_SOLARIS64.zip
- p14029429_112030_SOLARIS64.zip
- p14058884_112030_SOLARIS64.zip
- p14164849_112030_SOLARIS64.zip
- p14226599_112030_SOLARIS64.zip
- p14499293_1120311ExadataDatabase_SOLARIS64.zip
- p14555370_1120311ExadataDatabase_SOLARIS64.zip
- p14653598_1120311ExadataDatabase_SOLARIS64.zip
- p14679292_112030_SOLARIS64.zip
- p14741727_1120311ExadataDatabase_SOLARIS64.zip
- p14757709_1120311ExadataDatabase_SOLARIS64.zip
- p14775679_1120311ExadataDatabase_SOLARIS64.zip
- p14808639_1120311ExadataDatabase_SOLARIS64.zip
- p14837414_1120311ExadataDatabase_SOLARIS64.zip
- p15843238_1120311ExadataDatabase_SOLARIS64.zip
- p16100861_1120311ExadataDatabase_SOLARIS64.zip
- p16207583_1120311ExadataDatabase_SOLARIS64.zip
- p16369388_1120311ExadataDatabase_SOLARIS64.zip

### 3.3.5 Solaris 86 X64 Exadata Patches

Apply the following Exadata patches if you are on the Solaris X64 platform:

- p12552578_1120311ExadataDatabase_Solaris86-64.zip
- p12646746_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

- p13615767_1120311ExadataDatabase_Solaris86-64.zip

- p13632653_112030_Solaris86-64.zip

- p13743357_1120311ExadataDatabase_Solaris86-64.zip

- p13902963_1120311ExadataDatabase_Solaris86-64.zip

- p14029429_112030_Solaris86-64.zip

- p14058884_112030_Solaris86-64.zip

- p14164849_112030_Solaris86-64.zip

- p14226599_112030_Solaris86-64.zip

- p14499293_1120311ExadataDatabase_Solaris86-64.zip

- p14555370_1120311ExadataDatabase_Solaris86-64.zip

- p14653598_1120311ExadataDatabase_Solaris86-64.zip

- p14679292_112030_Solaris86-64.zip

- p14741727_1120311ExadataDatabase_Solaris86-64.zip

- p14757709_1120311ExadataDatabase_Solaris86-64.zip

- p14775679_1120311ExadataDatabase_Solaris86-64.zip

- p14808639_1120311ExadataDatabase_Solaris86-64.zip

- p14837414_1120311ExadataDatabase_Solaris86-64.zip

- p15843238_1120311ExadataDatabase_Solaris86-64.zip

- p16100861_1120311ExadataDatabase_Solaris86-64.zip

- p16207583_1120311ExadataDatabase_Solaris86-64.zip

- p16369388_1120311ExadataDatabase_Solaris86-64.zip

## 3.4 Run RUP Lite for RDBMS for Upgrade to Release 7

Run the RUP Lite for RDBMS utility to perform the tasks required to update your Oracle Fusion Applications database before you upgrade to Release 7. RUP Lite for RDBMS can be run in the following modes:

- **Validate mode:**

  - Validates database parameters as described in Table 3–1

- **Set database parameters mode:**

  - Sets database parameters to the values described in Table 3–1, if required

  - Restarts the database instance, if requested

- **Apply mode:**

  - Stops the listener and shuts down the database instance (optional)

- Configures Oracle Configuration Manager (OCM) in disconnected mode, if required

- Unzips Opatch, if it is available in *REPOSITORY_LOCATION*

- Applies patch set updates (PSUs) and one-off patches in *REPOSITORY_ LOCATION*

- Applies downloaded one-off patches in the `11.1.7.0.0_post_repo_patches` directory

- Starts the listener and the database instance (optional)

- Runs `catbundle.sql` if any PSUs were applied

- Runs `catmetx.sql`

- **Apply Post Changes mode:**

    - Performs SQL*Plus actions after patches apply

RUP Lite for RDBMS uses non-interactive OPatch calls to apply RDBMS patches. OPatch tries to install and configure Oracle Configuration Manager (OCM) if OCM has not already been installed and configured. This causes non-interactive OPatch calls to fail in some cases. To avoid this issue, Oracle recommends that you install OCM prior to running RUP Lite for RDBMS. If you plan to use OCM, you should configure it after you install it. If you do not plan to use OCM, you can either configure it in disconnected mode or let RUP Lite for RDBMS configure it. If you install OCM and do not configure it, RUP Lite for RDBMS will automatically configure it in disconnected mode. For more information, see "Installing Oracle Configuration Manager Using the Command Line Interface" in the *Oracle Configuration Manager Installation and Administration Guide*.

If you do not use Oracle Exadata Database Machine, run RUP Lite for RDBMS to automatically apply the mandatory Oracle Database patches mentioned in the "Oracle Database" section of Oracle Fusion Applications release notes. This step applies Oracle Database patches that reside in both the *REPOSITORY_LOCATION* and the `11.1.7.0.0_ post_repo_patches` directories, which you downloaded in Section 2.3.6, "Download and Unzip Repository and Patches for Release 6 to Release 7 Upgrade". Follow the steps in Section 3.4.1, "Run RUP Lite for RDBMS".

If you use Oracle Exadata Database Machine, do not run RUP Lite for RDBMS.

## 3.4.1 Run RUP Lite for RDBMS

If you are running Oracle Fusion Applications on a RAC database, follow the steps in Section 3.4.2, "Run RUP Lite for RDBMS in a RAC Database".

Perform the following steps to run RUP Lite for RDBMS in three modes: `validate`, `setdbparameters`, and `apply`:

1. Apply the version of OPatch that is delivered in the repository. It is available at *REPOSITORY_LOCATION*`/installers/database/opatch/p6880880_112000_ Linux-x86-64.zip`.

2. Copy the `TPBundler.zip` file to any temporary directory, such as *work_dir* in the following example:

    ```
    cp REPOSITORY_LOCATION/installers/pre_install/TPBundler.zip work_dir
    ```

3. Unzip `TPBundler.zip` in the *work_dir* directory, which contains the following files after unzipping:

```
createTPBundle.jar
createTPBundle.cmd
createTPBundle.sh
ojdl.jar
tpBundleConfig_DB.xml
tpBundleConfig_IDM.xml
tpBundleConfig_OHS.xml
README.txt
```

4. The `createTPBundler` utility creates the RDBMS patch bundle, `DBPatches.zip`, and RUP Lite for RDBMS. This patch bundle contains the mandatory prerequisite patches that are delivered in *REPOSITORY_LOCATION* as well as any patches you may have downloaded.

   Use the following command syntax to run `createTPBundler`, which creates `DBPatches.zip` in a temporary directory, referred to as *work_dir* in the example. Note that *work_dir* must have read/write permissions.

   ```
   (UNIX)
   sh createTPBundle.sh -shiphomelocation REPOSITORY_LOCATION -tempdir work_dir
   -target DB [-patchdownloadloc location_of_downloaded_patches]

   (Windows)
   createTPBundle.cmd -shiphomelocation REPOSITORY_LOCATION -tempdir work_dir
   -target DB [-patchdownloadloc location_of_downloaded_patches]
   ```

   The following options are available for `createTPBundler`:

   – `-shiphomelocation`: Location of the `createTPBundler` repository.

   – `-tempdir`: Destination directory to which the generated zip file was copied.

   – `-target`: Target against which the copy should be initiated. Valid values are IDM, DB, OH. Use the DB value.

   – `-patchdownloadloc`: Location of the patch directory where you downloaded the patches in Section 2.3.6, "Download and Unzip Repository and Patches for Release 6 to Release 7 Upgrade". Use this option only if you downloaded patches to a directory other than the default patch download directory, which is `11.1.7.0.0_post_repo_patches`.

   – `-logfile`: Full path of the `createTPbundle` log file. The default is `createTPBundle.log` in the current directory.

   – `-loglevel`: Log level for the `createTPbundler` utility. Valid values are SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST. The default value is INFO.

5. Copy `DBPatches.zip` to any temporary directory on the database server host.

6. Log in to the database server host.

7. Unzip `DBPatches.zip` to any temporary directory on the database server host. The following subdirectories and files exist after unzipping.

   ```
   |-- DB_timestamp
       -- db_server_bundle
           |-- README.txt
           |-- bin
           |   |-- ruplite.bat
           |   |-- ruplite.sh
           |-- metadata
           |   |-- env.properties
   ```

```
                           |   |-- installer.properties
                           |   |-- plugin-metadata.txt
                           |-- custom_db_server
                           |    -- database
                           |        -- patch
                           |            -- downloaded one-off patches
                           |-- db_server
                           |   |-- database
                           |       |-- opatch
                           |       |   -- OPatch zip file
                           |       |-- patch
                           |       |   -- One-off patches in repository
                           |       |-- psu
                           |       |   -- Patch Set Updates in repository
                           |-- db
                           |   |--RUP Lite related files
                           |-- lib
                           |   |--RUP Lite related files
                           |-- ruplite
                           |   |--RUP Lite related files
                           |-- techpatch
                           |   |--TPU related files
```

8. Perform this step only if you are running RUP Lite for RDBMS on an Oracle VM environment.

   As the root user, change the permissions on the DB_*timestamp* subdirectory:

   ```
   chmod -R 777 DB_timestamp
   ```

   Exit out of root user to ensure that you do not perform the remaining steps as root.

9. Set executable permissions on `ruplite.sh`. (UNIX only)

   ```
   chmod -R 755 DB_timestamp/db_server_bundle/bin/ruplite.sh
   ```

10. Set the `JAVA_HOME` environment variable as shown in the following example:

    ```
    (UNIX)
    setenv JAVA_HOME java_home_location (must be jdk6)

    (Windows)
    set JAVA_HOME=java_home_location (must be jdk6)
    ```

11. Update the following properties in the *work_dir*/DB_*timestamp*/db_server_ bundle/metadata/env.properties file. Example values are shown.

    - ORACLE_SID=Use an instance name that belongs to the `fusionapps` database.

    - ORACLE_HOME=Use an Oracle home directory on which patches must be applied, such as `/u01/db/11.2.0.3`.

    - TNS_ADMIN=Use a valid location that contains SQL*Net configuration files for the database.

    - LISTENER_NAME=Use a listener name.

    - PFILE=/u01/db/11.2.0.3/dbs/init.ora, for example. You can retrieve this value by running the following query:

      ```
      select NAME, VALUE from v$parameter where NAME like '%file%';
      ```

      Update PFILE if your database is started using pfile.

- DBSERVER_RESTART=true or false

  To minimize downtime, you can use "false" for setdbparameters mode, and "true" for apply mode.

  If DBSERVER_RESTART is set to "false", the database server, listener and other related services must be manually stopped before running RUP Lite in apply mode. Then after running RUP Lite in apply mode, you must run Step 21.

  If the value for this property is set to "true", RUP Lite automatically stops the listener and database before applying patches. In addition, RUP Lite automatically performs the following actions after applying patches when DBSERVER_RESTART=true:

  **a.** Start the database instance.

  **b.** Start the listener.

  **c.** Run catbundle.sql with arguments "psu apply" on non-windows and "winbundle apply" on windows.

  ```
  (UNIX)
  $ORACLE_HOME/rdbms/admin/catbundle.sql psu apply

  (Windows)
  %ORACLE_HOME%\rdbms\admin\catbundle.sql winbundle apply
  ```

  For a list of catbundle.sql errors that can be ignored, see Section 6.19.17, "Ignorable Errors Reported by catbundle.sql".

  **d.** Run ORACLE_HOME/rdbms/admin/catmetx.sql.

  ```
  (UNIX)
  $ORACLE_HOME/rdbms/admin/catmetx.sql

  (Windows)
  %ORACLE_HOME%\rdbms\admin\catmetx.sql
  ```

  **e.** For each patch applied, run the post installation script, postinstall.sql, if it exists.

**12.** Verify that the java version is 1.6 or above by using the following command:

```
(UNIX)
$JAVA_HOME/bin/java -version

(Windows)
%JAVA_HOME%\bin\java -version
```

If your version is lower, download 1.6 or a higher version from My Oracle Support.

**13.** Stop all user applications.

**14.** Change directory to the following location:

```
DB_timestamp/db_server_bundle/bin
```

**15.** Run RUP Lite for RDBMS in validate mode. The database instance and listener must be up.

```
(UNIX) ruplite.sh validate
(Windows) ruplite.bat validate
```

**16.** Review the log file, `output/logs/ruplitevalidate.log`, to confirm whether the database parameters contain the values you set in Step 11 and the values displayed in Table 3–1, " Recommended Values for Database Parameters". If any errors occurred, you can find them in this log file.

If any of the parameters do not contain the recommended value, proceed to the next step to run RUP Lite for RDBMS in `setdbparameters` mode. If all parameters are correct, proceed to Step 19 to run RUP Lite for RDBMS in `apply` mode.

**17.** Run RUP Lite for RDBMS in `setdbparameters` mode. The database instance and listener must be up.

```
(UNIX) ruplite.sh setdbparameters
(Windows) ruplite.bat setdbparameters
```

**18.** Review the log file, `output/logs/ruplitesetdbparameters.log`, to confirm whether the database parameters contain the values displayed in Table 3–1, " Recommended Values for Database Parameters". If any errors occurred, you can find them in this log file also.

**19.** Running RUP Lite for RDBMS in `apply` mode starts and stops only the Fusion Applications database listener and the database server. You must stop any other applications or processes that are running from the Oracle Fusion Applications home directory, except the OPSS Security Store, before you run RUP Lite for RDBMS. For more information, see "Starting and Stopping" in the *Oracle Fusion Applications Administrator's Guide*. Also confirm that the BI presentation servers are shut down.

You can set the parameter `DBSERVER_RESTART` (available in `metadata/env.properties`) to "false" if you want to manually shut down the database, stop the listener before patching, and start it up after applying the patches. For Windows, if you set `DBSERVER_RESTART` to "false", follow the steps in Section 3.4.3, "Stop Services on Windows Before Running RUP Lite For RDBMS".

> **Note:** To avoid an issue with active files while patching, ensure that no applications or processes are running from the `ORACLE_HOME` that is referenced in `metadata/env.properties`. If `DBSERVER_RESTART=`true, you can ignore the database instance and listener processes because RUP Lite brings them down.

Run RUP Lite for RDBMS in `apply` mode.

```
(UNIX) ruplite.sh
(Windows) ruplite.bat
```

**20.** Review the following log files located under the `output/logs` directory if any errors occurred:

```
ruplitedb.log
tp_property_editor_timestamp.log
db_apply_downloaded_patches_timestamp.log
db_apply_repository_patches_timestamp.log
db_validate_downloaded_patches_timestamp.log
db_validate_repository_patches_timestamp.log
downloaded_patch_validate_results_timestamp.xml
repository_patch_validate_results_timestamp.xml
post_db_restart_actions_timestamp.log
```

If RUP Lite for RDBMS fails, resolve the issue reported in the log files. When you restart a failed session, RUP Lite for RDBMS ignores the successful actions, starts with the failed action, and proceeds from that point.

The `post_db_restart_actions_timestamp.log` file includes the output from `catbundle.sql` and `catmetx.sql`. For a list of `catbundle.sql` errors that can be ignored, see Section 6.19.17, "Ignorable Errors Reported by catbundle.sql".

21. If you set `DBSERVER_RESTART` to "false", perform the following steps:

    a. Start the database instance

    b. Start the listener

    c. Run RUP Lite for RDBMS in `applypostchanges` mode.

       ```
       (UNIX) ruplite.sh applypostchanges
       (Windows) ruplite.bat applypostchanges
       ```

    d. Review the following log files, located under the `output/logs` directory, if any errors occurred:

       ```
       ruplitedbapplypostchanges.log
       post_db_restart_actions_timestamp.log
       ```

       These log files are generated by running ruplite in `applypostchanges` mode. The `post_db_restart_actions_timestamp.log` file includes the output from `catbundle.sql` and `catmetx.sql`. For a list of `catbundle.sql` errors that can be ignored, see Section 6.19.17, "Ignorable Errors Reported by catbundle.sql".

22. You must manually execute any manual steps that are documented in the `README.txt` file of the patches you applied with RUP Lite for RDBMS. RUP Lite for RDBMS executes `postinstall.sql` if it is mentioned as a manual step. All other steps have to be done manually.

23. Proceed to Section 3.4.4, "Run Additional Post Database Start Scripts for Patches for Release 7".

## 3.4.2 Run RUP Lite for RDBMS in a RAC Database

Perform the following steps to run RUP Lite for RDBMS in a RAC database. You must run RUP Lite for RDBMS on all available file systems. This may involve multiple hosts and nodes. Note that a single Oracle home can be shared by multiple nodes, and in this case, running RUP Lite on a single node of such a group is sufficient.

1. Follow Steps 1 through 10 in Section 3.4.1, "Run RUP Lite for RDBMS".

2. Stop all user applications that use the Oracle home directory being patched.

3. Update the following properties in the `work_dir/DB_timestamp/db_server_bundle/metadata/env.properties` file. Example values are shown.

   - ORACLE_HOME=Use an Oracle home directory on which patches must be applied, such as `/u01/db/11.2.0.3`.

   - ORACLE_SID=Use an instance name that belongs to the `fusionapps` database and is run against the ORACLE_HOME set in the previous property.

   - TNS_ADMIN=Use a valid `tns_admin` location, which is typically located under the grid infra and contains `listener.ora` and `sqlnet.ora` files.

   - LISTENER_NAME=Use a listener name.

   - PFILE=`/u01/db/11.2.0.3/dbs/init.ora`, for example.

Update PFILE if your database is started using pfile.

- DBSERVER_RESTART=false

  Note that the value of DBSERVER_RESTART must be "false".

4. Verify that the java version is 1.6 or above by using the following command:

```
(UNIX)
$JAVA_HOME/bin/java -version

(Windows)
%JAVA_HOME%\bin\java -version
```

5. Change directory to the following location:

```
DB_timestamp/db_server_bundle/bin
```

6. Run RUP Lite for RDBMS in validate mode. The database instance and listener must be up.

```
(UNIX) ruplite.sh validate
(Windows) ruplite.bat validate
```

7. Review the log file, output/logs/ruplitevalidate.log, to confirm whether the database parameters contain the values you set in Step 3 and the values displayed in Table 3–1, " Recommended Values for Database Parameters". If any errors occurred, you can find them in this log file also.

   If any of the parameters do not contain the recommended value, proceed to the next step to run RUP Lite for RDBMS in setdbparameters mode. If all parameters are correct, proceed to Step 10 to run RUP Lite for RDBMS in apply mode.

8. Run RUP Lite for RDBMS in setdbparameters mode. The database instance and listener must be up.

```
(UNIX) ruplite.sh setdbparameters
(Windows) ruplite.bat setdbparameters
```

9. Review the log file, output/logs/ruplitesetdbparameters.log, to confirm whether the database parameters contain the values displayed in Table 3–1, " Recommended Values for Database Parameters". If any errors occurred, you can find them in this log file also.

10. Shut down all Oracle RAC databases on all nodes in the cluster, even those that are sharing the same host. Database instances that are running could cause issues that prevent patches from applying successfully or you could receive errors because the patches update files that are in use.

    To shut down an Oracle RAC database, enter the following command in a command window, where CRS_home is the location of the Grid home directory and sales is the name of the database in the following example:

```
(UNIX)
CRS_home/bin/srvctl stop database -d sales

(Windows)
CRS_home\bin\srvctl stop database -d sales
```

11. Stop the listener that is running from all Oracle homes in the cluster, using the following command:

```
(UNIX)
CRS_home/bin/srvctl stop listener [-l listener_name]
```

```
(Windows)
CRS_home\bin\srvctl stop listener [-l listener_name]
```

12. To avoid an issue with active files while patching, ensure that no applications or processes are running from the ORACLE_HOME that is referenced in `metadata/env.properties`.

13. Run RUP Lite for RDBMS in `apply` mode.

```
(UNIX) ruplite.sh
(Windows) ruplite.bat
```

14. Review the following log files located under the `output/logs` directory if any errors occurred:

```
ruplitedb.log
tp_property_editor_timestamp.log
db_apply_downloaded_patches_timestamp.log
db_apply_repository_patches_timestamp.log
db_validate_downloaded_patches_timestamp.log
db_validate_repository_patches_timestamp.log
downloaded_patch_validate_results_timestamp.xml
repository_patch_validate_results_timestamp.xml
```

If RUP Lite for RDBMS fails, resolve the issue reported in the log files. When you restart a failed session, RUP Lite for RDBMS ignores the successful actions, starts with the failed action, and proceeds from that point.

15. RAC databases often share a single ORACLE_HOME for all RAC instances. If you have this configuration, continue to the next step.

If you do not have this configuration, you must update the files in the other ORACLE_HOMEs for your RAC database. To update the other ORACLE_HOMEs, repeat Steps 4 through 8 in Section 3.4.1, "Run RUP Lite for RDBMS" for RAC instances with non-shared ORACLE_HOMEs. Then repeat Steps 3 through 15 in this section for all RAC instances. Note that this may involve multiple hosts and nodes.

16. Start the database.

17. Run RUP Lite for RDBMS in `applypostchanges` mode.

```
(UNIX) ruplite.sh applypostchanges
(Windows) ruplite.bat applypostchanges
```

18. Review the following log files, located under the `output/logs` directory, if any errors occurred:

```
ruplitedbapplypostchanges.log
post_db_restart_actions_timestamp.log
```

These log files are generated by running ruplite in `applypostchanges` mode. The `post_db_restart_actions_timestamp.log` file includes the output from `catbundle.sql` and `catmetx.sql`. For a list of `catbundle.sql` errors that can be ignored, see Section 6.19.17, "Ignorable Errors Reported by catbundle.sql".

19. You must manually execute any manual steps that are documented in the `README.txt` file of the patches you applied with RUP Lite for RDBMS. RUP Lite for RDBMS executes `postinstall.sql` if it is mentioned as a manual step. All other steps have to be done manually.

If there is more than one ORACLE_HOME in the RAC database, you do not need to run SQL scripts again when patching the 2nd through the *n*th ORACLE_HOME, but you do need to perform any manual steps that update ORACLE_HOME.

**20.** Start the listener from all Oracle homes in the cluster. For Windows, start the services described Section 3.4.3, "Stop Services on Windows Before Running RUP Lite For RDBMS".

**21.** Proceed to Section 3.4.4, "Run Additional Post Database Start Scripts for Patches for Release 7".

## 3.4.3 Stop Services on Windows Before Running RUP Lite For RDBMS

For a Windows platform, the following services should be stopped before you run RUP Lite for RDBMS.

> **Note:** You do not shut down services if `DBSERVER_RESTART=true` in `env.properties`, which is the default case. You must shut down services only if you set `DBSERVER_RESTART=false` in `env.properties`.

- OracleOraDb11g_home1TNSListenerLISTENER_<SID>

- OracleOraDb11g_home1ClrAgent

- OracleDBConsole<SID>

- OracleJobScheduler<SID>

- OracleService<SID>

- OracleMTSRecoveryService

- Windows Management Instrumentation

- Distributed Transaction Coordinator

- Oracle <SID> VSS Writer Service

If RUP Lite for RDBMS fails to stop or start a service, you can manually manage each service from the Control Panel. Select **Administrative Tools**, then **Services**. Right click on each service and choose the **Stop** or **Start** option.

## 3.4.4 Run Additional Post Database Start Scripts for Patches for Release 7

RUP Lite for RDBMS consolidates the README.txt files for all applied patches into one consolidated README.txt file, which is located in the *OUI_Component*_readme.txt directory. You must manually execute any manual steps that are documented in the consolidated README.txt file. RUP Lite for RDBMS executes `postinstall.sql` if it is mentioned as a manual step. All other steps have to be performed manually on the DB host by any user that has system privileges. Perform these steps on only one of the nodes in the case of a RAC setup.

Database patches can be found at the following locations:

*SHARED_UPGRADE_LOCATION/POD_NAME/RELEASE_VERSION*/DB/RUPLiteDB/DB_*TIME_STAMP*/db_server_bundle/db_server/database/psu (if exists)

*SHARED_UPGRADE_LOCATION/POD_NAME/RELEASE_VERSION*/DB/RUPLiteDB/DB_*TIME_STAMP*/db_server_bundle/db_server/database/patch

Example location:

```
/u01/shared_location/CRM/11.1.7.0.0/DB/RUPLiteDB/DB_2012-08-07_
03-43-22/db_server_bundle/db_server/database/patch/
```

# 4

# Upgrading to Oracle Fusion Applications Release 7

This chapter describes the steps required to upgrade to Oracle Fusion Applications 11*g* Release 7 (11.1.7).

This chapter contains the following topics:

- Steps for the Release 5 to Release 6 Hop of the Chained Upgrade
- Steps for the Release 6 to Release 7 Upgrade
- Upgrade Orchestrator Completes Successfully
- Pause Point Steps

## 4.1 Steps for the Release 5 to Release 6 Hop of the Chained Upgrade

If you are performing a single hop upgrade from Release 6 to Release 7, proceed to Section 4.2, "Steps for the Release 6 to Release 7 Upgrade".

Perform the following steps for the Release 5 to Release 6 hop of the chained upgrade:

- Run Upgrade Orchestrator in Pre-Down Time Mode
- Run Upgrade Orchestrator During Down Time
- Pause Point 1 - Back Up the OPSS Security Store
- Update Status to Success
- Resume Upgrade Orchestrator
- Pause Point 2 - Back Up Oracle Fusion Applications
- Update Status to Success
- Resume Upgrade Orchestrator
- Pause Point 3 - Upgrade Oracle Identity Management From Release 5 to Release 6
- Update Status to Success
- Resume Upgrade Orchestrator
- Pause Point 5 - Run RUP Lite for OVM in Post-Root Mode (Oracle VM Only)
- Update Status to Success (Oracle VM Only)
- Resume Upgrade Orchestrator (Oracle VM Only)
- Pause Point 6 - Start External Servers

- [Update Status to Success](#)
- [Resume Upgrade Orchestrator](#)

## 4.1.1 Run Upgrade Orchestrator in Pre-Down Time Mode

> **Note:** This step is designed to be run before your down time. If you choose not to run this step before down time, Upgrade Orchestrator will run this as its first step during down time, which could significantly increase your down time.

Perform the following steps to run Upgrade Orchestrator in pre-down time mode. If you choose to run Upgrade Orchestrator in pre-down time mode multiple times, even if all tasks were successful during a previous run, certain validations will always run, such as the property file validation, host check validation, and the RUP Lite for OVM property validation. Upgrade Orchestrator runs Health Checker as part of the upgrade process, but if you want to run the Health Checker utility manually, see Section A.2.2.3, "How to Run Health Checker."

1. Start Upgrade Orchestrator by running the following commands on all host types, including the respective scaled out hosts. This command should be run on all hosts at the same time. Note that the value POD_NAME for -pod refers to the directory you created in Section 2.3.7, "Unzip Orchestration.zip".

   You are prompted for the Master Orchestration Password, which you created in Section 2.4.2.1, "Select a Master Orchestration Password", because certain orchestration tasks require login credentials.

   a. Run the following command to start orchestration on the primordial host:

   ```
   (Unix)
   cd ORCH_LOCATION/bin
   ./orchestration.sh -pod POD_NAME -hosttype PRIMORDIAL -phase PreDowntime
   [-DlogLevel=log_level]

   (Windows)
   cd ORCH_LOCATION\bin
   orchestration.cmd -pod POD_NAME -hosttype PRIMORDIAL -phase PreDowntime
   [-DlogLevel=log_level]
   ```

   b. Run the following command to start orchestration on each Midtier host that is listed in the HOSTNAME_MIDTIER property in the pod.properties file:

   ```
   (Unix)
   cd ORCH_LOCATION/bin
   ./orchestration.sh -pod POD_NAME -hosttype MIDTIER -phase PreDowntime
   [-DlogLevel=log_level]

   (Windows)
   cd ORCH_LOCATION\bin
   orchestration.cmd -pod POD_NAME -hosttype MIDTIER -phase PreDowntime
   [-DlogLevel=log_level]
   ```

   c. Run the following command to start orchestration on each OHS host that is listed in the HOSTNAME_OHS property in the pod.properties file:

   ```
   (Unix)
   cd ORCH_LOCATION/bin
   ./orchestration.sh -pod POD_NAME -hosttype OHS -phase PreDowntime
   ```

```
[-DlogLevel=log_level]

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd -pod POD_NAME -hosttype OHS -phase PreDowntime
[-DlogLevel=log_level]
```

**d.** Run the following command to start orchestration on each IDM host that is listed in the following properties in the `pod.properties` file:

- HOSTNAME_IDMOID

- HOSTNAME_IDMOIM

- HOSTNAME_IDMOHS

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh -pod POD_NAME -hosttype IDM -phase PreDowntime
[-DlogLevel=log_level]

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd -pod POD_NAME -hosttype IDM -phase PreDowntime
[-DlogLevel=log_level]
```

Upgrade Orchestrator runs the tasks in Table 4–1.

*Table 4–1   Tasks Run During PreDowntime Phase*

| Task Name | Task ID | Host Types |
|---|---|---|
| Validate Mandatory Orchestration Properties | PropertyValidationPlugin | Primordial, OHS, Midtier, IDM |
| Validate Host Types | HostTypeValidatePlugin | Primordial, OHS, Midtier, IDM |
| Validate RUP Lite for OVM Properties | RupLiteOvmValidatePlugin | Primordial, OHS, Midtier, IDM |
| Register Database Schema Information | RegisterDBSchemaInfo | Primordial |
| Register System User Information | SystemUserSeeding (This task runs only during the upgrade from Release 6 to Release 7) | Primordial |
| Run Data Quality Checks | DataQualityChecks | Primordial |
| Run Upgrade Readiness (Pre-Downtime) Checks | PreDowntimeChecks | Primordial, OHS, Midtier |

**2.** Ensure that all actions performed by Upgrade Orchestrator were successful before proceeding to the next step.

> **Note:** If this command results in any hanging or failed tasks on any host, perform the steps in Section 6.6.2, "Safely Exit Upgrade Orchestrator" to safely exit Upgrade Orchestrator.
>
> If Upgrade Orchestrator in `PreDowntime` mode on the primordial host does not safely exit, you must either fix the issue or perform the step manually. Then you must rerun Upgrade Orchestrator in `PreDowntime` mode on the primordial host. It is mandatory that the `PreDowntime` phase exits successfully. Do not continue with orchestration until the primordial host completes successfully.
>
> After the issue is resolved, you must restart Upgrade Orchestrator in `PreDowntime` mode on all hosts which were forced to exit, as well as those hosts that had failures.

Upgrade Orchestrator can exit for either a failure, a pause point, or upon successful completion. When orchestrator exits on failure, review the log files and take the appropriate corrective action. Then rerun Orchestrator using the commands specified in this section.

If a task in the `PreDowntime` phase fails and you want to manually fix the issues and skip the task, you can update the status of the task to success. In this case, use the `updatestatus` command, as shown in the following example using the `PreDowntimeChecks` taskid.

> **Note:** The `updateStatus` command should not be run on any hosts where orchestration is running. To terminate orchestration, follow the instructions in Section 6.4, "Terminate Upgrade Orchestration".

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype host_type -hostname host_
name -release release_name -phase phase_name -taskid PreDowntimeChecks -taskstatus
success
```

```
(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype host_type -hostname host_
name -release release_name -phase phase_name -taskid PreDowntimeChecks -taskstatus
success
```

For information about monitoring the progress of the upgrade, see Section 6.3, "Monitoring Upgrade Orchestration Progress". For information about troubleshooting, see Chapter 6, "Monitoring and Troubleshooting the Upgrade".

Note that when running the chained upgrade from Release 5 to Release 6 to Release 7, the Pre-down time checks are run for both Release 5 to Release 6 and Release 6 to Release 7 sequentially.

### 4.1.2 Run Upgrade Orchestrator During Down Time

Start Upgrade Orchestrator during down time by running the following commands on all host types, including the respective scaled out hosts. Note that the value *POD_NAME* for -pod refers to the directory you created in Section 2.3.7, "Unzip Orchestration.zip".

You are prompted for the Master Orchestration Password, which you created in Section 2.4.2.1, "Select a Master Orchestration Password", because certain orchestration tasks require login credentials.

1. Run the following command to start orchestration on the primordial host:

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh -pod POD_NAME -hosttype PRIMORDIAL [-DlogLevel=log_level]

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd -pod POD_NAME -hosttype PRIMORDIAL [-DlogLevel=log_level]
```

2. Run the following command to start orchestration on each Midtier host that is listed in the HOSTNAME_MIDTIER property in the pod.properties file:

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh -pod POD_NAME -hosttype MIDTIER [-DlogLevel=log_level]

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd -pod POD_NAME -hosttype MIDTIER [-DlogLevel=log_level]
```

3. Run the following command to start orchestration on each OHS host that is listed in the HOSTNAME_OHS property in the pod.properties file:

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh -pod POD_NAME -hosttype OHS [-DlogLevel=log_level]

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd -pod POD_NAME -hosttype OHS [-DlogLevel=log_level]
```

4. Run the following command to start orchestration on each IDM host that is listed in the following properties in the pod.properties file:

   - HOSTNAME_IDMOID

   - HOSTNAME_IDMOIM

   - HOSTNAME_IDMOHS

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh -pod POD_NAME -hosttype IDM [-DlogLevel=log_level]

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd -pod POD_NAME -hosttype IDM [-DlogLevel=log_level]
```

Section A.1, "Additional Information About Upgrade Orchestrator Commands" provides a complete list of options for the orchestration.sh command.

Upgrade Orchestrator can exit for either a failure, a pause point, or upon successful completion. When orchestrator exits on failure, review the log files and take the appropriate corrective action. Then rerun Orchestrator using the commands specified in this section.

For information about monitoring the progress of the upgrade, see Section 6.3, "Monitoring Upgrade Orchestration Progress". For information about troubleshooting,

see Chapter 6, "Monitoring and Troubleshooting the Upgrade".

Upgrade Orchestrator runs the tasks listed in Table 4–2.

*Table 4–2    Tasks Run During the DowntimePreFA Phase*

| Task Name | Task ID | Host Types |
|-----------|---------|------------|
| Deploy Missing SOA Shared Artifacts | DeploySoaShared (This task runs only during the upgrade from Release 6 to Release 7) | Primordial |
| Stop Index Schedules and Deactivate Index Optimization | StopIndexSchedules | Primordial |
| Stop All Servers | StopAllServers | Primordial, OHS, Midtier |
| Set CrashRecoveryEnabled Property to False | DisableCrashRecoveryEnabled | Primordial |
| Stop OPMN Control Processes | StopOPMNProcesses | Primordial, OHS, Midtier |
| Stop Node Managers | StopNodeManager | Primordial, Midtier |

> **Note:**   If the orchestration commands results in any hanging tasks on any host, do not use ctrl-C or ctrl-Z to exit. You must update the status of the task that is hanging by using the command in Section 6.6.2, "Safely Exit Upgrade Orchestrator". After you exit and the issue that caused the hanging is fixed, restart Upgrade Orchestrator, using the commands specified in this section, on the hosts that were forced to exit.

> **Note:**   The updateStatus command must not be run on a host where orchestration is already running. If, for some reason you have to run updateStatus for a task on a running host, you must ensure that it is safe to exit orchestration first across the entire environment. Then follow the steps below:
>
> 1. Terminate orchestration by following the instructions in Section 6.4, "Terminate Upgrade Orchestration".
> 2. Update the task status using the updateStatus command.
> 3. Restart orchestration on all the hosts when ready.

### 4.1.3  Pause Point 1 - Back Up the OPSS Security Store

Orchestration pauses so that you can back up the OPSS Security Store on the IDM host. Perform the steps in Section 4.4.1, "Back Up the OPSS Security Store".

If you have IIR installed and configured in your environment, you must stop IIR before performing any backups. Perform the steps in "Shutting Down Servers for High Availability" in the "Define Data Quality" chapter in the *Oracle Fusion Applications Customer Data Management Implementation Guide*.

### 4.1.4  Update Status to Success

After you successfully back up the OPSS Security Store, update the task status to "success" by running the following command:

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-release REL6 -phase DowntimePreFA -taskid BackupOPSS  -taskstatus success

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-release REL6 -phase DowntimePreFA -taskid BackupOPSS  -taskstatus success
```

### 4.1.5 Resume Upgrade Orchestrator

Resume orchestration on the IDM host using the command in Section 4.1.2, "Run Upgrade Orchestrator During Down Time", Step 4.

### 4.1.6 Pause Point 2 - Back Up Oracle Fusion Applications

Orchestration pauses so that you can back up the Oracle Fusion Applications environment. Perform the steps in Section 4.4.2, "Back Up Oracle Fusion Applications".

### 4.1.7 Update Status to Success

> **Note:** Ensure that you have backed up your Oracle Fusion Applications database and Oracle Identity Management database, as specified in Section 4.4.2, "Back Up Oracle Fusion Applications", before you run the commands in this section.

After you successfully perform the backups, update the task status to "success" on all hosts by running the following commands.

1. Update the task status on the primordial host.

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname
host_name -release REL6 -phase DowntimePreFA -taskid
BackupOracleFAPausePointPlugin -taskstatus success

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname
host_name -release REL6 -phase DowntimePreFA -taskid
BackupOracleFAPausePointPlugin -taskstatus success
```

2. Update the task status on each Midtier host that is listed in the HOSTNAME_MIDTIER property in the pod.properties file.

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_
name -release REL6 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin
-taskstatus success

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_
```

```
name -release REL6 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin
-taskstatus success
```

3. Update the task status on each OHS host that is listed in the `HOSTNAME_OHS` property in the `pod.properties` file.

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype OHS -hostname host_name
-release REL6 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin
-taskstatus success

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype OHS -hostname host_name
-release REL6 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin
-taskstatus success
```

4. Update the task status on each IDM host that is listed in following properties in the `pod.properties` file:

- HOSTNAME_IDMOID

- HOSTNAME_IDMOIM

- HOSTNAME_IDMOHS

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-release REL6 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin
-taskstatus success

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-release REL6 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin
-taskstatus success
```

### 4.1.8 Resume Upgrade Orchestrator

Resume orchestration on all host types, including the respective scaled out hosts, using the commands in Section 4.1.2, "Run Upgrade Orchestrator During Down Time", Steps 1 through 4.

### 4.1.9 Pause Point 3 - Upgrade Oracle Identity Management From Release 5 to Release 6

Orchestration pauses so that you can upgrade Oracle Identity Management. Perform the steps in Section 4.4.4, "Upgrade Oracle Identity Management Domain to 11g Release 6 (11.1.6)".

### 4.1.10 Update Status to Success

After you successfully upgrade Oracle Identity Management, update the task status to "success" on the IDM host.

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-release REL6 -phase DowntimePreFA -taskid UpgradeIDMPausePointPlugin  -taskstatus
```

```
success

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-release REL6 -phase DowntimePreFA -taskid UpgradeIDMPausePointPlugin -taskstatus
success
```

## 4.1.11 Resume Upgrade Orchestrator

Resume orchestration on each IDM host that is listed in the following properties in the
pod.properties file, using the command in Section 4.1.2, "Run Upgrade Orchestrator
During Down Time", Step 4:

- HOSTNAME_IDMOID

- HOSTNAME_IDMOIM

- HOSTNAME_IDMOHS

Upgrade Orchestrator runs the tasks in Table 4–3.

*Table 4–3    Tasks Run by Upgrade Orchestrator*

| Task Name | Task ID | Host Types |
| --- | --- | --- |
| Run Upgrade Readiness (During Downtime) Checks | DuringDowntimeChecks | Primordial, OHS, Midtier |
| Update JRE Memory Options | UpdateJREMemoryOptions | Primordial |
| Remove Conflicting Patches for Oracle Fusion Middleware Component Oracle Homes | RemoveConflictingPatches | Primordial |
| Install Oracle Fusion Applications LCM Tools for Oracle VM | InstallFaSaasLcmTools | Primordial, OHS, IDM |
| Run RUP Lite for OVM in Offline Mode as Application User | RupLiteOvmOffline | Primordial, OHS, Midtier, IDM |
| Run Oracle Fusion Applications RUP Installation Part 1 of 2 | RunFirstRUPInstaller | Primordial |
| Run RUP Lite for Domain Configuration | RunRUPLiteForDomainsConfig | Midtier |
| Start Node Managers | StartNodeManager | Primordial, Midtier |
| Start OPMN Control Processes | StartOPMNProcesses | Primordial, OHS, Midtier, |
| Run Oracle Fusion Applications RUP Installation Part 2 of 2 | RunSecondRUPInstaller | Primordial |
| *DowntimeDuringFA Phase* | | |
| Run Oracle Fusion Applications RUP Installation Part 1 of 2 | RunFirstRUPInstaller | Primordial |
| Run RUP Lite for Domain Configuration | RunRUPLiteForDomainsConfig | Midtier |
| Start Node Managers | StartNodeManager | Primordial, Midtier |
| Start OPMN Control Processes | StartOPMNProcesses | Primordial, OHS, Midtier, |

**Table 4–3 (Cont.) Tasks Run by Upgrade Orchestrator**

| Task Name | Task ID | Host Types |
|---|---|---|
| Run Oracle Fusion Applications RUP Installation Part 2 of 2 | RunSecondRUPInstaller | Primordial |
| *DowntimePostFA Phase* | | |
| Running Vital Signs Checks | VitalSignsChecks | Primordial |
| Invoke an Instance of UpdateSOAMDS SOA Composite | UpdateMDSSOAComposite | Primordial |
| Prepare for Oracle Fusion Applications WebTier Upgrade | CopyWebtierUpgradeToCentralLoc | Primordial |
| Stop Oracle Fusion Applications - APPOHS | StopOPMNProcesses | OHS |
| Remove Conflicting Patches for Oracle Fusion Applications WebTier Oracle Homes | RemoveConflictingPatches | OHS |
| Upgrade Oracle Fusion Applications OHS Binaries | UpgradeOHSBinary | OHS |
| Upgrade Oracle Fusion Applications OHS Configuration | UpgradeOHSConfig | OHS |
| Run RUP Lite for BI | RunRUPLiteForBI | Midtier |
| Run RUP Lite for OVM in Online Mode as Application User | RupLiteOvmOnline | Primordial, OHS, Midtier, IDM |

## 4.1.12 Pause Point 5 - Run RUP Lite for OVM in Post-Root Mode (Oracle VM Only)

If you are not running on an Oracle VM environment, proceed to Section 4.1.15, "Pause Point 6 - Start External Servers".

If you are running Oracle Fusion Applications on an Oracle VM environment, orchestration pauses so you can run RUP Lite for OVM in post-root mode as the root user on the primordial, OHS, Midtier, and IDM hosts.

Perform the steps in Section 4.4.7, "Run RUP Lite for OVM in Post-Root Mode for Release 6".

## 4.1.13 Update Status to Success (Oracle VM Only)

After successful completion of running RUP Lite for OVM in post-root mode, update the task status to "success" by performing the following steps:

1. Update the task status on the primordial host:

```
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname
host_name -release REL6 -phase DowntimePostFA -taskid
RupLiteOvmPostRootPausePointPlugin -taskstatus success
```

2. Update the task status on the OHS host that is listed in the HOSTNAME_OHS property in the pod.properties file:

```
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype OHS -hostname host_name
-release REL6 -phase DowntimePostFA -taskid RupLiteOvmPostRootPausePointPlugin
-taskstatus success
```

**3.** Update the task status on each Midtier host that is listed in the `HOSTNAME_MIDTIER` property in the `pod.properties` file

```
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_
name -release REL6 -phase DowntimePostFA -taskid
RupLiteOvmPostRootPausePointPlugin -taskstatus success
```

**4.** Update the task status on each IDM host that is listed in following properties in the `pod.properties` file:

- `HOSTNAME_IDMOID`

- `HOSTNAME_IDMOIM`

- `HOSTNAME_IDMOHS`

```
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-release REL6 -phase DowntimePostFA -taskid RupLiteOvmPostRootPausePointPlugin
-taskstatus success
```

### 4.1.14  Resume Upgrade Orchestrator (Oracle VM Only)

Resume orchestration on all host types, including the respective scaled out hosts, using the commands in Section 4.1.2, "Run Upgrade Orchestrator During Down Time", Steps 1 through 4.

### 4.1.15  Pause Point 6 - Start External Servers

Orchestration pauses on the Midtier host so you can start the GOP server and IIR instance.

Perform the steps in Section 4.4.9, "Start External Servers".

### 4.1.16  Update Status to Success

After the GOP server starts, set the task status to "success" on the Midtier host.

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_
name -release REL6 -phase DowntimePostFA -taskid
StartExternalServersPausePointPlugin -taskstatus success
```

```
(Windows)
cd ORCH_LOCATION\bin
.\orchestration.cmd updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_
name -release REL6 -phase DowntimePostFA -taskid
StartExternalServersPausePointPlugin -taskstatus success
```

### 4.1.17  Resume Upgrade Orchestrator

Resume orchestration on the Midtier host using the command in Section 4.1.2, "Run Upgrade Orchestrator During Down Time", Step 2.

Upgrade Orchestrator runs the tasks in Table 4–4.

*Table 4–4    Tasks Run During the DowntimePostFA Phase*

| Task Name | Task ID | Host Types |
|---|---|---|
| Set CrashRecoveryEnabled Property to True | EnableCrashRecoveryEnabled | Primordial |
| Run Post Upgrade Health Checks | PostUpgradeChecks | Primordial, OHS, Midtier |
| Running Data Quality Checks | DataQualityChecks | Primordial |
| Run Post Upgrade Cleanup Tasks | PostUpgradeCleanup | Primordial |

> **Note:** Upgrade Orchestrator continues with the upgrade. Proceed to Section 4.2.2, "Run Upgrade Orchestrator During Down Time".

## 4.2  Steps for the Release 6 to Release 7 Upgrade

Perform following steps for the Release 6 to Release 7 hop.

- Run Upgrade Orchestrator in Pre-Down Time Mode
- Run Upgrade Orchestrator During Down Time
- Pause Point 1 - Back Up the OPSS Security Store
- Update Status to Success
- Resume Upgrade Orchestrator
- Pause Point 2 - Back Up Oracle Fusion Applications
- Update Status to Success
- Resume Upgrade Orchestrator
- Pause Point 3 - Upgrade Oracle Identity Management From Release 6 to Release 7
- Update Status to Success
- Resume Upgrade Orchestrator
- Pause Point 4 - Run RUP Lite for OVM in Pre-Root Mode (Oracle VM Only)
- Orchestration Runs Tasks for Oracle VM and non-Oracle VM
- Update Status to Success (Oracle VM Only)
- Resume Upgrade Orchestrator (Oracle VM Only)
- Pause Point 5 - Run RUP Lite for OVM in Post-Root Mode (Oracle VM Only)
- Update Status to Success (Oracle VM Only)
- Resume Upgrade Orchestrator (Oracle VM Only)
- Pause Point 6 - Start External Servers
- Update Status to Success
- Resume Upgrade Orchestrator
- Pause Point 7 - Back Up Oracle Fusion Applications Before Language Pack Upgrade (Language Pack Only)
- Update Status to Success

■   Resume Upgrade Orchestrator (Language Pack Only)

### 4.2.1 Run Upgrade Orchestrator in Pre-Down Time Mode

Perform the steps in Section 4.1.1, "Run Upgrade Orchestrator in Pre-Down Time Mode".

### 4.2.2 Run Upgrade Orchestrator During Down Time

Perform the steps in Section 4.1.2, "Run Upgrade Orchestrator During Down Time". Note that only the following tasks are run:

■   Stop All Servers

■   Set CrashRecoveryEnbled Property to False

■   Stop OPMN Control Processes

■   Stop Node Managers

### 4.2.3 Pause Point 1 - Back Up the OPSS Security Store

Orchestration pauses so that you can back up the OPSS Security Store on the IDM host. Perform the steps in Section 4.4.1, "Back Up the OPSS Security Store".

If you have Informatica Identity Resolution (IIR) installed and configured in your environment, you must stop IIR before performing any backups. Perform the steps in "Shutting Down Servers for High Availability" in the "Define Data Quality" chapter in the *Oracle Fusion Applications Customer Data Management Implementation Guide*.

### 4.2.4 Update Status to Success

After you successfully back up the OPSS Security Store, update the task status to "success" by running the following command:

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-release REL7 -phase DowntimePreFA -taskid BackupOPSS  -taskstatus success

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-release REL7 -phase DowntimePreFA -taskid BackupOPSS  -taskstatus success
```

### 4.2.5 Resume Upgrade Orchestrator

Resume orchestration on the IDM host using the command in Section 4.1.2, "Run Upgrade Orchestrator During Down Time", Step 4.

### 4.2.6 Pause Point 2 - Back Up Oracle Fusion Applications

Orchestration pauses so that you can back up the Oracle Fusion Applications environment. Perform the steps in Section 4.4.2, "Back Up Oracle Fusion Applications".

### 4.2.7  Update Status to Success

> **Note:**  Ensure that you have backed up your Oracle Fusion
> Applications database and Oracle Identity Management database, as
> specified in Section 4.4.2, "Back Up Oracle Fusion Applications",
> before you run the commands in this section.

After you successfully perform the backups, update the task status to "success" on all
hosts by running the following commands.

1. Update the task status on the primordial host.

   ```
   (Unix)
   cd ORCH_LOCATION/bin
   ./orchestration.sh updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname
   host_name  -release REL7 -phase DowntimePreFA -taskid
   BackupOracleFAPausePointPlugin -taskstatus success

   (Windows)
   cd ORCH_LOCATION\bin
   orchestration.sh updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname
   host_name  -release REL7 -phase DowntimePreFA -taskid
   BackupOracleFAPausePointPlugin -taskstatus success
   ```

2. Update the task status on each Midtier host that is listed in the `HOSTNAME_MIDTIER`
   property in the `pod.properties` file.

   ```
   (Unix)
   cd ORCH_LOCATION/bin
   ./orchestration.sh updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_
   name -release REL7 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin
   -taskstatus success

   (Windows)
   cd ORCH_LOCATION\bin
   orchestration.cmd updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_
   name -release REL7 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin
   -taskstatus success
   ```

3. Update the task status on each OHS host that is listed in the `HOSTNAME_OHS`
   property in the `pod.properties` file.

   ```
   (Unix)
   cd ORCH_LOCATION/bin
   ./orchestration.sh updateStatus -pod POD_NAME -hosttype OHS -hostname host_name
   -release REL7 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin
   -taskstatus success

   (Windows)
   cd ORCH_LOCATION\bin
   orchestration.cmd updateStatus -pod POD_NAME -hosttype OHS -hostname host_name
   -release REL7 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin
   -taskstatus success
   ```

4. Update the task status on each IDM host that is listed in following properties in
   the `pod.properties` file:

   - `HOSTNAME_IDMOID`

   - `HOSTNAME_IDMOIM`

- HOSTNAME_IDMOHS

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-release REL7 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin
-taskstatus success

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-release REL7 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin
-taskstatus success
```

### 4.2.8 Resume Upgrade Orchestrator

Resume orchestration on all host types, including the respective scaled out hosts, using the commands in Section 4.1.2, "Run Upgrade Orchestrator During Down Time", Steps 1 through 4.

### 4.2.9 Pause Point 3 - Upgrade Oracle Identity Management From Release 6 to Release 7

Orchestration pauses so that you can upgrade Oracle Identity Management. Perform the steps in Section 4.4.5, "Upgrade Oracle Identity Management Domain to 11g Release 7 (11.1.7)".

### 4.2.10 Update Status to Success

After you successfully upgrade Oracle Identity Management, update the task status to "success" on the IDM host.

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-release REL7 -phase DowntimePreFA -taskid UpgradeIDMPausePointPlugin -taskstatus
success

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-release REL7 -phase DowntimePreFA -taskid UpgradeIDMPausePointPlugin -taskstatus
success
```

### 4.2.11 Resume Upgrade Orchestrator

Resume orchestration on each IDM host that is listed in the following properties in the pod.properties file, using the command in Section 4.1.2, "Run Upgrade Orchestrator During Down Time", Step 4:

- HOSTNAME_IDMOID

- HOSTNAME_IDMOIM

- HOSTNAME_IDMOHS

Upgrade Orchestrator runs the tasks in Table 4–5.

**Table 4–5    Tasks Run During the DowntimePreFA Phase**

| Task Name | Task ID | Host Types |
|---|---|---|
| Run Upgrade Readiness (During Downtime) Checks | DuringDowntimeChecks | Primordial, OHS, Midtier |
| Update JRE Memory Options | UpdateJREMemoryOptions | Primordial |
| Remove Conflicting Patches for Oracle Fusion Middleware Component Oracle Homes | RemoveConflictingPatches | Primordial |
| Upgrade JDK | UpgradeJDK | Primordial |
| Install Oracle Fusion Applications LCM Tools for Oracle VM | InstallFaSaasLcmTools | Primordial, OHS, IDM |
| Prepare for Oracle Fusion Applications LCM Tools for Oracle VM Upgrade | PrepareLCMToolsForOVMUpgrade | Primordial |
| Apply Oracle Fusion Applications LCM Tools for Oracle VM Patches | ApplyLCMToolsForOVMPatches | Primordial, OHS, IDM |

If you are not running on a Oracle VM environment, Orchestration runs the tasks listed in Table 4–6 and you can proceed to Section 4.2.19, "Pause Point 6 - Start External Servers". If you are running on a Oracle VM environment, proceed to Section 4.2.12, "Pause Point 4 - Run RUP Lite for OVM in Pre-Root Mode (Oracle VM Only)."

## 4.2.12 Pause Point 4 - Run RUP Lite for OVM in Pre-Root Mode (Oracle VM Only)

If you are running Oracle Fusion Applications on an Oracle VM environment, orchestration pauses so you can run RUP Lite for OVM in pre-root mode as the root user on the primordial, OHS, Midtier, and IDM hosts. Perform the steps in Section 4.4.6, "Run RUP Lite for OVM in Pre-Root Mode for Release 7".

## 4.2.13 Update Status to Success (Oracle VM Only)

After successful completion of running RUP Lite for OVM in pre-root mode, update the task status to "success".

1.  Update the task status on the primordial host:

    ```
    cd ORCH_LOCATION/bin
    ./orchestration.sh updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname
    host_name -release REL7 -phase DowntimePreFA -taskid
    RupLiteOvmPreRootPausePointPlugin  -taskstatus success
    ```

2.  Update the task status on the OHS host that is listed in the HOSTNAME_OHS property in the pod.properties file:

    ```
    cd ORCH_LOCATION/bin
    ./orchestration.sh updateStatus -pod POD_NAME -hosttype OHS -hostname host_name
    -release REL7 -phase DowntimePreFA -taskid RupLiteOvmPreRootPausePointPlugin
    -taskstatus success
    ```

3.  Update the task status on each Midtier host that is listed in the HOSTNAME_MIDTIER property in the pod.properties file

    ```
    cd ORCH_LOCATION/bin
    ./orchestration.sh updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_
    name -release REL7 -phase DowntimePreFA -taskid
    RupLiteOvmPreRootPausePointPlugin -taskstatus success
    ```

**4.** Update the task status on each IDM host that is listed in following properties in the `pod.properties` file:

- `HOSTNAME_IDMOID`

- `HOSTNAME_IDMOIM`

- `HOSTNAME_IDMOHS`

```
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-release REL7 -phase DowntimePreFA -taskid RupLiteOvmPreRootPausePointPlugin
-taskstatus success
```

## 4.2.14 Resume Upgrade Orchestrator (Oracle VM Only)

Resume orchestration on all host types, including the respective scaled out hosts, using the commands in Section 4.1.2, "Run Upgrade Orchestrator During Down Time", Steps 1 through 4.

## 4.2.15 Orchestration Runs Tasks for Oracle VM and non-Oracle VM

Upgrade Orchestrator runs the tasks in the following table.

*Table 4–6 Tasks Run by Upgrade Orchestrator for both Oracle VM and non-Oracle VM*

| Task Name | Task ID | Host Types |
|---|---|---|
| Run RUP Lite for OVM in Offline Mode as Application User (NOTE: this task runs only for Oracle VM environments) | RupLiteOvmOffline | Primordial, OHS, Midtier, IDM |
| Run Oracle Fusion Applications RUP Installation Part 1 of 2 | RunFirstRUPInstaller | Primordial |
| Run RUP Lite for Domain Configuration | RunRUPLiteForDomainsConfig | Midtier |
| Start Node Managers | StartNodeManager | Primordial, Midtier |
| Start OPMN Control Processes | StartOPMNProcesses | Primordial, OHS, Midtier, |
| Run Oracle Fusion Applications RUP Installation Part 2 of 2 | RunSecondRUPInstaller | Primordial |
| *DowntimePostFA Phase* | | |
| Running Vital Signs Checks | VitalSignsChecks | Primordial |
| Invoke an Instance of UpdateSOAMDS SOA Composite | UpdateMDSSOAComposite | Primordial |
| Prepare for Oracle Fusion Applications WebTier Upgrade | CopyWebtierUpgradeToCentralLoc | Primordial |
| Stop Oracle Fusion Applications - APPOHS | StopOPMNProcesses | OHS |
| Remove Conflicting Patches for Oracle Fusion Applications WebTier Oracle Homes | RemoveConflictingPatches | OHS |
| Upgrade Oracle Fusion Applications OHS Binaries | UpgradeOHSBinary | OHS |

*Table 4–6 (Cont.) Tasks Run by Upgrade Orchestrator for both Oracle VM and*

| Task Name | Task ID | Host Types |
|---|---|---|
| Upgrade Oracle Fusion Applications OHS Configuration | UpgradeOHSConfig | OHS |
| Run RUP Lite for BI | RunRUPLiteForBI | Midtier |
| Run RUP Lite for OVM in Online Mode as Application User | RupLiteOvmOnline | Primordial, OHS, Midtier, IDM |

## 4.2.16 Pause Point 5 - Run RUP Lite for OVM in Post-Root Mode (Oracle VM Only)

If you are running Oracle Fusion Applications on an Oracle VM environment, orchestration pauses so you can run RUP Lite for OVM in post-root mode as the root user on the primordial, OHS, Midtier, and IDM hosts.

Perform the steps in Section 4.4.8, "Run RUP Lite for OVM in Post-Root Mode for Release 7".

## 4.2.17 Update Status to Success (Oracle VM Only)

After successful completion of running RUP Lite for OVM in post-root mode, update the task status to "success" by performing the following steps:

1. Update the task status on the primordial host:

   ```
   cd ORCH_LOCATION/bin
   ./orchestration.sh updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname
   host_name -release REL7 -phase DowntimePostFA -taskid
   RupLiteOvmPostRootPausePointPlugin -taskstatus success
   ```

2. Update the task status on the OHS host that is listed in the HOSTNAME_OHS property in the pod.properties file:

   ```
   cd ORCH_LOCATION/bin
   ./orchestration.sh updateStatus -pod POD_NAME -hosttype OHS -hostname host_name
   -release REL7 -phase DowntimePostFA -taskid RupLiteOvmPostRootPausePointPlugin
   -taskstatus success
   ```

3. Update the task status on each Midtier host that is listed in the HOSTNAME_MIDTIER property in the pod.properties file

   ```
   cd ORCH_LOCATION/bin
   ./orchestration.sh updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_
   name -release REL7 -phase DowntimePostFA -taskid
   RupLiteOvmPostRootPausePointPlugin -taskstatus success
   ```

4. Update the task status on each IDM host that is listed in following properties in the pod.properties file:

   - HOSTNAME_IDMOID

   - HOSTNAME_IDMOIM

   - HOSTNAME_IDMOHS

   ```
   cd ORCH_LOCATION/bin
   ./orchestration.sh updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
   -release REL7 -phase DowntimePostFA -taskid RupLiteOvmPostRootPausePointPlugin
   -taskstatus success
   ```

### 4.2.18 Resume Upgrade Orchestrator (Oracle VM Only)

Resume orchestration on all host types, including the respective scaled out hosts, using the commands in Section 4.1.2, "Run Upgrade Orchestrator During Down Time", Steps 1 through 4.

### 4.2.19 Pause Point 6 - Start External Servers

Orchestration pauses on the Midtier host so you can start the GOP server and IIR instance.

Perform the steps in Section 4.4.9, "Start External Servers".

### 4.2.20 Update Status to Success

After the GOP server and IIR instance start, set the task status to "success" on the Midtier host.

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_
name -release REL7 -phase DowntimePostFA -taskid
StartExternalServersPausePointPlugin -taskstatus success

(Windows)
cd ORCH_LOCATION\bin
.\orchestration.cmd updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_
name -release REL7 -phase DowntimePostFA -taskid
StartExternalServersPausePointPlugin -taskstatus success
```

### 4.2.21 Resume Upgrade Orchestrator

Resume orchestration on the Midtier host using the command in Section 4.1.2, "Run Upgrade Orchestrator During Down Time", Step 2.

Upgrade Orchestrator runs the tasks in Table 4–7.

*Table 4–7    Tasks Run During the DowntimePostFA Phase*

| Task Name | Task ID | Host Types |
|---|---|---|
| Set CrashRecoveryEnabled Property to True | EnableCrashRecoveryEnabled | Primordial, Midtier |
| Run Post Upgrade Health Checks | PostUpgradeChecks | Primordial, OHS, Midtier |
| Run Data Quality Checks | DataQualityChecks | Primordial |
| Run Post Upgrade Cleanup Tasks | PostUpgradeCleanup | Primordial |

> **Note:**    If you just completed the upgrade to Release 7 and do not have language packs installed, proceed to Section 4.3, "Upgrade Orchestrator Completes Successfully". If you just completed the upgrade to Release 7 and have language packs installed, proceed to Section 4.2.22, "Pause Point 7 - Back Up Oracle Fusion Applications Before Language Pack Upgrade (Language Pack Only)".

## 4.2.22  Pause Point 7 - Back Up Oracle Fusion Applications Before Language Pack Upgrade (Language Pack Only)

If only the US English language is installed on your environment, proceed to Section 4.3, "Upgrade Orchestrator Completes Successfully".

If you have set the `SKIP_UPGRADE_FOR_LANGUAGE` option to skip languages, the upgrade for those languages will not be performed as part of orchestration. In this case, you must manually upgrade the skipped languages after Upgrade Orchestrator completes successfully. Proceed to Section 4.3, "Upgrade Orchestrator Completes Successfully".

If you have languages other than US English installed on your Oracle Fusion Applications environment, Upgrade Orchestrator pauses so you can back up your Oracle Fusion Applications environment before your languages are upgraded. Perform the steps in Section 4.4.2, "Back Up Oracle Fusion Applications".

## 4.2.23  Update Status to Success

After you successfully back up the Oracle Fusion Applications environment, update the task status to "success" on all hosts:

1.  Update the task status on the primordial host:

    ```
    (Unix)
    cd ORCH_LOCATION/bin
    ./orchestration.sh updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname
    host_name -release REL7 -phase DowntimePostFA -taskid
    BackupOracleFAPausePointPlugin -taskstatus success

    (Windows)
    cd ORCH_LOCATION\bin
    orchestration.cmd updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname
    host_name -release REL7 -phase DowntimePostFA -taskid
    BackupOracleFAPausePointPlugin -taskstatus success
    ```

2.  Update the task status on each Midtier host that is listed in the `HOSTNAME_MIDTIER` property in the `pod.properties` file:

    ```
    (Unix)
    cd ORCH_LOCATION/bin
    ./orchestration.sh updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_
    name -release REL7 -phase DowntimePostFA -taskid BackupOracleFAPausePointPlugin
    -taskstatus success

    (Windows)
    cd ORCH_LOCATION\bin
    orchestration.cmd updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_
    name -release REL7 -phase DowntimePostFA -taskid BackupOracleFAPausePointPlugin
    -taskstatus success
    ```

3.  Update the task status on each OHS host that is listed in the `HOSTNAME_OHS` property in the `pod.properties` file:

    ```
    (Unix)
    cd ORCH_LOCATION/bin
    ./orchestration.sh updateStatus -pod POD_NAME -hosttype OHS -hostname host_name
    -release REL7 -phase DowntimePostFA -taskid BackupOracleFAPausePointPlugin
    -taskstatus success

    (Windows)
    cd ORCH_LOCATION\bin
    ```

```
orchestration.cmd updateStatus -pod POD_NAME -hosttype OHS -hostname host_name
-release REL7 -phase DowntimePostFA -taskid BackupOracleFAPausePointPlugin
-taskstatus success
```

4. Update the task status on each IDM host that is listed in following properties in the `pod.properties` file:

- `HOSTNAME_IDMOID`

- `HOSTNAME_IDMOIM`

- `HOSTNAME_IDMOHS`

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-release REL7 -phase DowntimePostFA -taskid BackupOracleFAPausePointPlugin
-taskstatus success

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-release REL7 -phase DowntimePostFA -taskid BackupOracleFAPausePointPlugin
-taskstatus success
```

### 4.2.24 Resume Upgrade Orchestrator (Language Pack Only)

Resume orchestration on all host types, including the respective scaled out hosts, using the commands in Section 4.1.2, "Run Upgrade Orchestrator During Down Time", Steps 1 through 4.

Upgrade Orchestrator runs the tasks in Table 4–8.

*Table 4–8    Tasks Run For the Language Pack Upgrade*

| Task Name | Task ID | Host Types |
| --- | --- | --- |
| Upgrade All Installed Languages | LanguagePackInstall | Primordial |
| Stop All Servers | StopServersAfterLP | Primordial |
| Start All Servers | StartSeversAfterLP | Primordial |
| Run Post Language Pack Health Checks | PostLangPackChecks | Primordial |

## 4.3 Upgrade Orchestrator Completes Successfully

Upgrade Orchestrator generates the Oracle Fusion Applications Orchestrator Upgrade Report report upon successful completion of the upgrade, which you review as a post-upgrade task. Proceed to Chapter 5, "Post-Upgrade Tasks for Oracle Fusion Applications".

## 4.4 Pause Point Steps

This section describes the detailed steps required by each of the following default pause points:

- Back Up the OPSS Security Store

- Back Up Oracle Fusion Applications

- Back Up Oracle Fusion Applications on a Windows Platform

- Upgrade Oracle Identity Management Domain to 11g Release 6 (11.1.6)

- Upgrade Oracle Identity Management Domain to 11g Release 7 (11.1.7)

- Run RUP Lite for OVM in Post-Root Mode for Release 6

- Run RUP Lite for OVM in Post-Root Mode for Release 7

- Run RUP Lite for OVM in Pre-Root Mode for Release 7

- Start External Servers

## 4.4.1  Back Up the OPSS Security Store

Upgrade Orchestrator upgrades all WLS domains to the 11gR1 PS5 MLR1 (11.1.1.6.1) level so you must perform the following backups. Make sure you perform your backups in directories that you can restore from. You can use any directory to back up the data, as long as you know where to restore the backup from.

1.  **OPSS Security Store**

    Back up all data under the root node of the OPSS Security Store. Perform the following steps to identify the root node in the Oracle Internet Directory hosting the OPSS Security store using Fusion Applications Control. For more information, see "Reassociating with Fusion Middleware Control" in the *Oracle Fusion Middleware Application Security Guide*.

    **a.**  Open the Farm_CommonDomain.

    **b.**  Open the WebLogic Domain.

    **c.**  Open the CommonDomain.

    **d.**  Find the domain name of the root node under Root Node Details, which is under the Edit Security Provider region.
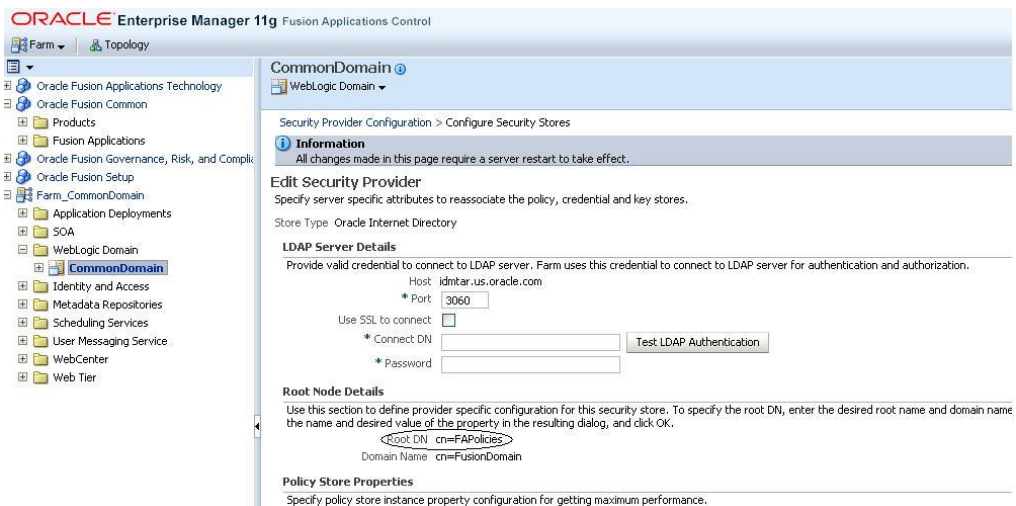


    In case of an upgrade failure, restore this node entirely.

    The `ldifwrite` and `bulkload` operations that follow must be performed on the system where the Oracle Internet Directory hosting the OPSS Security store resides. When initiating `ldifwrite` and `bulkload`, Oracle Internet Directory requires the Oracle Internet Directory process and the database behind Oracle Internet Directory to be up and running.

    - Set the following environment variables.

```
(Unix)
setenv ORACLE_HOME   OID_ORACLE_HOME
setenv ORACLE_INSTANCE   OID_INSTANCE_HOME

(Windows)
set ORACLE_HOME=OID_ORACLE_HOME
set ORACLE_INSTANCE=OID_INSTANCE_HOME
```

Example:

```
(Unix)
setenv ORACLE_HOME /u01/oid/oid_home
setenv ORACLE_INSTANCE /u01/oid/oid_inst

(Windows)
set ORACLE_HOME=\u01\oid\oid_home
set ORACLE_INSTANCE \u01\oid\oid_inst
```

■   Create the backup. The backup is created in the *SHARED_UPGRADE_ LOCATION/POD_NAME/release/* directory.

In the system where the Oracle Internet Directory is located, produce an LDIF file by running `ldifwrite` as illustrated in the following command. Note that you are prompted for the Operational Data Store (ODS) password.

```
OID_HOME/ldap/bin/ldifwrite connect="srcOidDbConnectStr"
basedn="cn=FAPolicies", "c=us" ldiffile="srcOid.ldif"
```

Example:

```
/u01/oid/oid_home/ldif/bin/ldifwrite connect="oidddb"
basedn="cn=FAPolicies" ldiffile="srcOid.ldif"
```

This command writes all entries under the node `cn=FAPolicies` to the file `srcOid.ldif`. After generated, move this file to the directory that was previously identified, to hold all backup data.

■   Perform the following steps if you need to restore the backup.

–   Ensure Oracle Internet Directory is up and running.

–   Perform a `bulkdelete` on Oracle Internet Directory nodes.

–   In the Oracle Internet Directory system, verify that there are no schema errors or bad entries by running `bulkload`, as illustrated in the following command:

```
OID_HOME/ldap/bin/bulkload connect="dstOidDbConnectStr" check=true
generate=true restore=true file="fullPath2SrcOidLdif"
```

If duplicate DNs (common entries between the source and destination directories) are detected, review them to prevent unexpected results.

–   Load data into the Oracle Internet Directory by running `bulkload` as illustrated in the following command:

```
OID_HOME/ldap/bin/bulkload connect="dstOidDbConnectStr" load=true
file="fullPath2SrcOidLdif"
```

For more information about the `bulkload` command, see "Performing Bulk Operations" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

For more information about migrating Oracle Internet Directory, see "Migrating Large Volume Policy and Credential Stores" in th*e Oracle Fusion Middleware Application Security Guide*.

2. **Bootstrap Wallet**

   Back up the `cwallet.sso file` in the `DOMAIN_HOME`/config/fmwconfig/bootstrap directory for **each WLS domain** in an Oracle Fusion Applications installation. You must take backups of each `cwallet.sso` file for each domain and when you restore, you must be careful to restore the correct file. For example, if you back up `cwallet.sso` from the Common Domain, then you must restore it in the Common Domain upon failure. If you back up `cwallet.sso` from the BI domain, you must restore it to the BI Domain upon failure.

If you are performing the steps for the Release 5 to Release 6 hop of the chained upgrade, proceed to Section 4.1.4, "Update Status to Success."

If you are performing the steps for the Release 6 to Release 7 upgrade, proceed to Section 4.2.4, "Update Status to Success."

## 4.4.2 Back Up Oracle Fusion Applications

Back up your entire Oracle Fusion Applications environment by following the steps for performing a full offline backup in "Backing Up and Recovering Oracle Fusion Applications" in the *Oracle Fusion Applications Administrator's Guide*. Include the following components in your backup:

- Back Up Your Database
- Back Up Upgrade Orchestrator Directories
- Back Up OHS Host and /etc/hosts
- Back Up the Central Inventory

For additional back up steps that are specific to Windows, refer to Section 4.4.3, "Back Up Oracle Fusion Applications on a Windows Platform".

### 4.4.2.1 Back Up Your Database

Database upgrade and patching is a prerequisite to the Oracle Fusion Applications Upgrade. You must backup your Oracle Fusion Applications database and Oracle Identity Management database before and after applying all prerequisite patches and before starting the Oracle Fusion Applications upgrade. For more information, see "Backing Up and Recovering Oracle Fusion Applications" in the *Oracle Fusion Applications Administrator's Guide*. Turn on Oracle Flashback Database as a best practice before taking a backup of the Oracle Fusion Applications database.

### 4.4.2.2 Back Up Upgrade Orchestrator Directories

Upgrade Orchestrator writes to work areas specified by properties in the `pod.properties` file. Ensure that you back up the work directories during all Oracle Fusion Applications backup pause points. During any restore of your environment, you must restore the orchestration work directories to the same backup point.

Backup directories are specified by the following properties in the `pod.properties` file:

- ORCHESTRATION_CHECKPOINT_LOCATION
- ORCHESTRATION_CHECKPOINT_ARCHIVE_LOCATION
- SHARED_UPGRADE_LOCATION

If these directories are shared among multiple environments then the backups of these directories must be specific to the environment (*POD_NAME*). The restore should also be specific to that environment (*POD_NAME*), as shown in the following examples:

- ORCHESTRATION_CHECKPOINT_LOCATION/*POD_NAME*

- ORCHESTRATION_CHECKPOINT_ARCHIVE_LOCATION /ARCHIVE/*POD_NAME*

- SHARED_UPGRADE_LOCATION/*POD_NAME*

> **Note:** When restoring the Oracle Fusion Applications environment from a backup, you must restore the orchestration directories if you want to continue using orchestration from the backup pause points in the orchestration flow.

### 4.4.2.3 Back Up OHS Host and /etc/hosts

On the OHS host, back up `/u01/APPLTOP` and `/u02/instance`.

Back up the `/etc/hosts` file.

### 4.4.2.4 Back Up the Central Inventory

Upgrade Orchestrator upgrades and applies Oracle Fusion Middleware and Oracle Fusion Application patches to your Oracle Fusion Applications environment. As a best practice, back up your central inventory along with other Oracle homes before the upgrade. On the primordial host, the location of the central inventory can be obtained by looking at the inventory pointer file (`oraInst.loc` on Linux), located in *FA_ORACLE_HOME*.

If you are performing the steps for the Release 5 to Release 6 hop of the chained upgrade, proceed to Section 4.1.7, "Update Status to Success."

If you are performing the steps for the Release 6 to Release 7 upgrade, proceed to Section 4.2.7, "Update Status to Success."

If you are performing the steps for a language pack upgrade, proceed to Section 4.2.23, "Update Status to Success."

## 4.4.3 Back Up Oracle Fusion Applications on a Windows Platform

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      |        |

|  | Total | Copied | Skipped | Mismatch | FAILED | Extras |
|---|---|---|---|---|---|---|
| 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.

   Back up the inventory location referenced in the registry `HKEY_LOCAL_ MACHINE\SOFTWARE\ORACLE\inst_loc`.

3. Back up the registry.

   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 RUP Installer.

5. Save the system PATH variable.

### 4.4.4 Upgrade Oracle Identity Management Domain to 11*g* Release 6 (11.1.6)

Perform the following steps to upgrade the Oracle Identity Management domain to 11g Release 6 (11.1.6):

1. Remove conflicting patches on all nodes in the Oracle Identity Management domain.

   To remove conflicting patches, run the patch removal script contained in patch 16572470. You downloaded patch 16572470 while performing the steps in Section 2.3.4, "Download and Unzip the Patch Conflict Manager Utility". To run the script, follow the instructions contained in the README.txt file included with patch 16572470.

> **Important:** You must run the conflicting patch removal script on every node in the domain before you apply any upgrade patch. Specifically, you must run the script on each of the following nodes before applying any upgrade patch:
>
> - IDM Node
> - IAM Node
> - OHS Node
>
> You can learn more about each of the nodes in the domain by referring to Section 4.4.4.1, "Oracle Identity Management Overview for 11g Release 6 (11.1.6)."

2. Apply upgrade patches to each of the nodes in the Oracle Identity Management domain.

   To apply the upgrade patches, perform the steps in Section 4.4.4.2, "Oracle Identity Management Patches for the IDM Domain for 11g Release 6 (11.1.6)."

3. Determine if any additional mandatory patches are required and apply them.

   To determine if any additional patches are required for upgrading the Oracle Identity Management domain, refer to the "Additional Mandatory Patches for the IDM Domain" section of the *Technical Release Notes for Oracle Fusion Applications 11g Release 6 (11.1.6)*.

   > **Important:** If any additional patches are listed in that section of the Technical Release Notes, you must apply them to upgrade the Oracle Identity Management domain.

4. Review known problems and perform workarounds.

   Known issues, and their workarounds, in each release are documented in the Technical Release Notes. Review the known problems in Oracle Identity Management for this release and perform their workarounds by referring to each of the following sections in the *Technical Release Notes for Oracle Fusion Applications 11g Release 6 (11.1.6)*:

   - Pre-Installation Known Issues
   - Installation Known Issues
   - Post-Installation Known Issues
   - Platform-Specific Known Issues
   - Upgrade Known Issues
   - Post Upgrade Known Issues
   - Run Time Environment Known Issues

### 4.4.4.1  Oracle Identity Management Overview for 11g Release 6 (11.1.6)

Oracle Identity Management for Oracle Fusion Applications 11g Release 6 (11.1.6) includes patches for the following products that are installed in the Oracle Identity Management domain:

- Oracle Internet Directory

- Oracle Virtual Directory

- Oracle Directory Services Manager

- Oracle Platform Security Services

- Oracle Web Services Manager

- Oracle Identity Manager

- Oracle Access Manager

- Oracle Identity Federation

- Oracle IDM Tools

- Oracle WebGate

The following sections provide an overview of the Identity Management Domain, Nodes, and Oracle homes for Oracle Fusion Applications 11g Release 6 (11.1.6).

#### 4.4.4.1.1 IDM Node

- WEBLOGIC_ORACLE_HOME - The following Oracle products are installed in this Oracle home:

  - Oracle WebLogic Server

- IDM_ORACLE_COMMON_HOME - This is also known as the ORACLE_ COMMON_HOME. The following Oracle Identity Management products are installed in this Oracle home:

  - Oracle Platform Security Services

  - Oracle Web Services Manager

- IDM_ORACLE_HOME - This is also known as the OID_ORACLE_HOME. The following Oracle Identity Management products are installed in this Oracle home:

  - Oracle Internet Directory

  - Oracle Virtual Directory

  - Oracle Directory Services Manager

  - Oracle Identity Federation

#### 4.4.4.1.2 IAM Node

- WEBLOGIC_ORACLE_HOME - The following Oracle products are installed in this Oracle home:

  - Oracle WebLogic Server

- IAM_ORACLE_COMMON_HOME - This is also known as the ORACLE_ COMMON_HOME. The following Oracle Identity Management products are installed in this Oracle home:

  - Oracle Platform Security Services

  - Oracle Web Services Manager

- IAM_ORACLE_HOME - This is also known as the OIM_ORACLE_HOME. The following Oracle Identity Management products are installed in this Oracle home:

  - Oracle Identity Manager

  - Oracle Access Manager

- – Oracle IDM Tools

- OIF_ORACLE_HOME

  - – Oracle Identity Federation

- SOA_ORACLE_HOME - This is typically installed under the IAM_ORACLE_ HOME. The following products are installed in this Oracle home:

  - – Oracle SOA Suite

### 4.4.4.1.3  OHS Node

- OHS_ORACLE_HOME - This is also known as the WEBTIER_ORACLE_HOME. The following Oracle products are installed in this Oracle home:

  - – Oracle HTTP Server

- OHS_ORACLE_COMMON_HOME - This is also known as the ORACLE_ COMMON_HOME. The following Oracle Identity Management products are installed in this Oracle home:

  - – Oracle Platform Security Services

  - – Oracle Web Services Manager

- WEBGATE_ORACLE_HOME - The following Oracle Identity Management products are installed in this Oracle home:

  - – Oracle WebGate

### 4.4.4.1.4  Database Node

- RDBMS_ORACLE_HOME - This is your ORACLE_HOME of Oracle Database. You must apply the mandatory database patches to this Oracle home.

  - – Oracle Database

### 4.4.4.1.5  Software and Patches

The software and patches for Oracle Identity Management for Oracle Fusion Applications 11*g* Release 7 (11.1.7) are available in the *FA_Repository* under *REPOSITORY_LOCATION*/installers. Please review the individual patch Readme.txt file before applying them.

**Upgrading from a prior release:**

- If you are upgrading your Oracle Identity Management for Oracle Fusion Applications 11g Release 1, Update 3 (11.1.4) to Release 5 (11.1.5), then refer to the *Oracle Fusion Applications Patching Guide*.

- If you are upgrading your Oracle Identity Management for Oracle Fusion Applications 11g Release 1, Update 2 (11.1.2) to Update 3 (11.1.4), then refer to Support Note: 1435333.1.

- If you are upgrading your Oracle Identity Management for Oracle Fusion Applications 11g Release 1, Update 1 (11.1.3) to Update 2 (11.1.4), then refer to Support Note: 1441704.1.

**Using OPatch with the napply Option:**

- Starting with Oracle Fusion Applications 11g Release 6 (11.1.6), Oracle recommends that you apply all FMW patches on the IDM domain. The opatch napply option facilitates applying all the patches in a directory in one session. You do not need to download the individual patches, extract them, and install them

one after another. The *FA_Repository* contains all the required patches for Oracle Fusion Middleware Patch Set 5 (11.1.1.5.0). For more information, see *Oracle Universal Installer and OPatch User's Guide for Windows and UNIX*.

■ Because your environment may already have some patches, you may see the Superset warning when you apply certain patches. You can ignore this.

### 4.4.4.2 Oracle Identity Management Patches for the IDM Domain for 11g Release 6 (11.1.6)

The following section details the Oracle Identity Management Patches for the IDM Domain:

#### 4.4.4.2.1 Prerequisites

Ensure that your environment meets the following requirements before you install or uninstall the patch:

1. Review and download the latest version of OPatch 11.1.x via Patch 6880880 (OPatch version 11.1.0.8.2 or later).

   ■ Oracle recommends that you use the latest version of OPatch. Review the My Oracle Support note 224346.1-Opatch-Where Can I Find the Latest Version of Opatch?

   ■ For more information about `opatch` usage, see "Patching Oracle Fusion Middleware with Oracle OPatch" in the *Oracle Fusion Middleware Patching Guide*.

   ---
   **See Also:** *Oracle Universal Installer and OPatch User's Guide for Windows and UNIX* for more information about OPatch.

   ---

2. Verify the OUI Inventory

   1. OPatch needs access to a valid OUI inventory to apply patches. Validate the OUI inventory with the following command: `$opatch lsinventory`.

   2. If the command reports an error, contact Oracle Support for assistance in validating and verifying the inventory setup before proceeding.

3. Confirm that the executables appear in your system PATH.

   1. The patching process uses the `unzip` and `opatch` executables. After setting the ORACLE_HOME environment, confirm whether the following executables exist before proceeding to the next step:

      – `which opatch`

      – `which unzip`

   2. If either of these executables do not show in the PATH, correct the problem before proceeding.

#### 4.4.4.2.2 Patch the Database (RDBMS_ORACLE_HOME)

Ensure the patches listed in Chapter 3, "Updating the Oracle Fusion Applications and Oracle Identity Management Databases" are applied on the Identity Management database to keep both Oracle Fusion Applications and Identity Management databases synchronized. Follow the steps in Chapter 3 to apply the patches.

> **Note:** The minimum supported RDBMS version for Oracle IDM database is 11.2.0.3.0.

#### 4.4.4.2.3 Patch the WebLogic Server on OID and OIM Nodes

You must patch the WebLogic server on OID and OIM nodes but not on OHS or DB nodes. The WebLogic server patches are available under the *FA_Repository*/installers/smart_update/weblogic directory. Follow the patch Readme and apply all patches in the directory. Use the following command to apply all patches:

```
java -jar FA_Repository/installers/smart_update/suwrapper/bsu-wrapper.jar\
 -bsu_home=/bea/mw_home/utils/bsu -meta=./suw_metadata.txt -install \
 -patchlist=WLS_Patch_List\
 -patch_download_dir=FA_Repository/installers/smart_update/weblogic\
 -prod_dir=/u01/oim/wlserver_10.3
```

For the WLS Patch List, provide a comma-separated list of WLS patches from the following directory in the *FA_Repository*: *FA_Repository*/installers/smart_update/weblogic

#### 4.4.4.2.4 Patch the IDM Node (IDM_ORACLE_HOME)

The patches for this Oracle home are available under the *FA_Repository*/installers/pltsec/patch directory that is appropriate for your platform. Follow the patch Readme and apply all patches in the directory.

1. Back up the OPSS Security Store, as described in Section 4.1.3.

2. Set your Oracle home to IDM_ORACLE_HOME.

3. Use opatch with the napply option to apply all patches.

4. Perform the Oracle Internet Directory Patch post-patching instructions that are described in the Readme.

#### 4.4.4.2.5 Patch the Common Oracle homes

**Patch the Common Oracle homes on All Nodes**

Your deployment should have at least the following Common Oracle homes.

■ IDM_ORACLE_COMMON_HOME

■ IAM_ORACLE_COMMON_HOME

■ OHS_ORACLE_COMMON_HOME

The patches for these Oracle homes are available under the *FA_Repository*/installers/oracle_common/patch directory that is appropriate for your platform. Follow the patch Readme and apply all patches in the directory.

■ Set your Oracle home to the appropriate Common Oracle home.

■ Use opatch with the napply option to apply all patches.

> **Note:** You must apply all the patches to all the Common Oracle homes.

#### 4.4.4.2.6 Patch the IAM Node

**Patch IAM_ORACLE_HOME**

The patches for this Oracle home are available under the
*FA_Repository*/installers/idm/patch directory that is appropriate for your
platform. Follow the patch Readme and apply the patches in the directory.

1. Ensure that the following servers are up and running:

   - Oracle Internet Directory

   - Oracle Directory Services Manager

   - Oracle Virtual Directory

2. Set your Oracle home to IAM_ORACLE_HOME.

3. Use opatch with the napply option to apply all patches.

**Post-Patch Instructions**

- Perform the Oracle Identity Manager Patch post-patching instructions that are
  described in the Readme.

- Perform the Oracle Access Manager Patch post-patching instructions that are
  described in the Readme.

- Perform the Oracle IDM Tools Patch post-patching instructions that are described
  in the Readme.

**Patch SOA_ORACLE_HOME**

The patches for this Oracle home are available under the
*FA_Repository*/installers/soa/patch directory that is appropriate for your
platform. Follow the patch Readme and apply the patches in the directory.

1. Set your Oracle home to SOA_ORACLE_HOME.

2. Use opatch with the napply option to apply all patches.

**Patch OIF_ORACLE_HOME**

The patches for this Oracle home are available under the
*FA_Repository*/installers/oif/patch directory that is appropriate for your
platform. Follow the patch Readme and apply the patches in the directory.

1. Set your Oracle home to OIF_ORACLE_HOME.

2. Use opatch with the napply option to apply all patches.

#### 4.4.4.2.7 Patch the OHS Node

**Patch OHS_ORACLE_HOME**

The patches for this Oracle home are available under the *FA_
Repository*/installers/webtier/patch directory that is appropriate for your
platform. Follow the patch Readme and apply the patches in the directory.

1. Ensure that the following servers are up and running:

   - WebLogic Administration Server

   - Oracle Identity Manager managed servers

   - Oracle Access Manager managed servers

   - Oracle SOA Suite managed servers

   - Oracle Identity Federation managed servers

**2.** Set your Oracle home to OHS_ORACLE_HOME.

**3.** Use `opatch` with the `napply` option to apply all patches.

**Patch WEBGATE_ORACLE_HOME**

The patches for this Oracle home are available under the
`FA_Repository`/installers/webgate/patch directory that is appropriate for your
platform. Follow the patch Readme and apply the patches in the directory.

**1.** Ensure that all IDM and IAM servers are accessible using LBR endpoints (if
enabled) or using OHS port 7777.

**2.** Set your Oracle home to WEBGATE_ORACLE_HOME.

**3.** Use `opatch` with the `napply` option to apply all patches.

#### 4.4.4.2.8  Additional Mandatory Patches for the IDM Domain

Follow the steps detailed in "Additional Mandatory Patches for the IDM Domain" in
the *Oracle Fusion Applications release notes*.

### 4.4.4.3  Verify the Oracle Identity Management Domain

To verify that the upgrades and patches to the Oracle Identity Management domain
were applied correctly, perform these steps:

**1.** Confirm you can access and log in to the Oracle WebLogic Administrative Server
console. For example:

`http://`*HOST*`:`*ADMIN_SERVER_PORT*`/console`

`https://`*HOST*`:`*SECURE_ADMIN_SERVER_PORT*`/console`

**2.** Confirm you can access and log in to Oracle Enterprise Manager Fusion
Middleware Control Console. For example:

`http://`*HOST*`:`*ADMIN_SERVER_PORT*`/em`

After completion of all steps in this section, proceed to Section 4.1.10, "Update Status
to Success."

## 4.4.5  Upgrade Oracle Identity Management Domain to 11*g* Release 7 (11.1.7)

> **Note:**  Before performing an upgrade to 11*g* Release 7 (11.1.7), check
> the *Technical Release Notes* for Oracle Fusion Applications 11g Release 7
> (11.1.7) for the latest information on patches.

Perform the following steps to upgrade the Oracle Identity Management domain to
11*g* Release 7 (11.1.7):

### 4.4.5.1  Overview

Oracle Identity Management for Oracle Fusion Applications 11*g*, Release 7 (11.1.7.0)
includes patches for the following products that are installed in the Oracle Identity
Management domain:

- Oracle Identity Manager

- Oracle IDM Tools

- Oracle Access Manager

- Oracle WebGate

- Oracle Internet Directory

The Oracle Fusion Applications Release 7 Identity Management software and patches for your appropriate platform are available in the Oracle Fusion Applications repository under *FA_Repository*/installers. Review the individual patch Readme before applying them.

### 4.4.5.2 About Identity Management Domain, Nodes and Oracle homes

This section explains the various Nodes and Oracle homes in the Identity Management domain for Oracle Fusion Applications 11g, Release 7 (11.1.7.0.0).

- Identity Management (IDM) Node

  - *WEBLOGIC_ORACLE_HOME*

    * Oracle WebLogic Server

  - *IDM_ORACLE_HOME*: This is also known as the *OID_ORACLE_HOME*. The following Oracle Identity Management products are installed in this Oracle home:

    * Oracle Internet Directory

    * Oracle Virtual Directory

    * Oracle Directory Services Manager

  - *IDM_ORACLE_COMMON_HOME*: The following Oracle Identity Management products are installed in this Oracle home:

    * Oracle Platform Security Services (OPSS)

    * Oracle Web Services Manager (OWSM)

- Identity and Access Management (IAM) Node

  - *WEBLOGIC_ORACLE_HOME*

    * Oracle WebLogic Server

  - *IAM_ORACLE_HOME*: This is also known as the *OIM_ORACLE_HOME*. The following Oracle Identity Management products are installed in this Oracle home:

    * Oracle Identity Manager

    * Oracle Access Manager

    * Oracle IDM Tools

    * Oracle Identity Federation

  - *SOA_ORACLE_HOME*: This is typically installed under the *IAM_ORACLE_HOME*. The following products are installed in this Oracle home:

    * Oracle SOA Suite

  - *IAM_ORACLE_COMMON_HOME*: The following Oracle Identity Management products are installed in this Oracle home:

    * OPSS

    * OWSM

- OHS Node

  - *OHS_ORACLE_HOME*: This is also known as the *WEB_ORACLE_HOME*. The following Oracle Identity Management products are installed in this Oracle home:

* Oracle WebGate

- *OHS_ORACLE_COMMON_HOME*: The following Oracle Identity Management products are installed in this Oracle home:

  * OPSS

  * OWSM

■ Database Node

- *RDBMS_ORACLE_HOME*: This is the *ORACLE_HOME* of the Oracle Database. You must apply mandatory database patches to this Oracle home.

### 4.4.5.3 Performing Pre-installation Tasks

Perform the following tasks before installation.

#### 4.4.5.3.1 Verifying Prerequisites

Ensure that your environment meets the following requirements before you install or uninstall the patch:

■ Review and download the latest version of OPatch 11.1.x via Patch 6880880 (OPatch version 11.1.0.8.2 or later).

  ■ Oracle recommends that you use the latest version of OPatch. Review the My Oracle Support note 224346.1-Opatch-Where Can I Find the Latest Version of Opatch?

  ---

  **See Also:** *Oracle Universal Installer and OPatch User's Guide for Windows and UNIX* for more information about OPatch.

  ---

■ Verify the OUI Inventory

  OPatch needs access to a valid OUI inventory to apply patches. Validate the OUI inventory with the following command:

  ```
  opatch lsinventory
  ```

  If the command errors out, contact Oracle Support for assistance in validating and verifying the inventory setup before proceeding.

■ Confirm the executables appear in your system PATH.

  The patching process uses the unzip and the OPatch executables. After setting the ORACLE_HOME environment, confirm whether the following executables exist, before proceeding to the next step.

  - which opatch

  - which unzip

#### 4.4.5.3.2 Stop the Servers and Processes

Stop the servers and processes, as follows:

■ In the Oracle Identity Management domain, stop all Oracle Identity Management services and processes using the following sequence. Do not stop the database.

> **Note:** Refer to Appendix E, "Stopping and Starting Identity Management Related Servers" for specific commands for stopping components.

Stop the following servers and processes:

– Oracle HTTP Server

– Oracle Identity Manager managed servers

– Oracle SOA managed servers

– Oracle Identity Federation managed servers

– Oracle Access Manager managed servers

– Oracle Directory Services Manager

– Oracle WebLogic Administration Server for the Oracle Identity Management domain

– Oracle Virtual Directory

– Oracle Internet Directory

#### 4.4.5.3.3 Create Backups

At a minimum, create the following backups:

- Middleware home directory (including the Oracle home directories inside the Middleware home)

- Local domain home directory

- Local Oracle instances

- Domain home and Oracle instances on any remote systems that use the Middleware home

- Back up your database and ensure the backup includes the schema version registry table, as each Fusion Middleware schema has a row in this table. The name of the schema version registry table is SYSTEM.SCHEMA_VERSION_REGISTRY$.

- Back up your Configurations and Stores—specifically, all data under the root node of the LDAP store.

- Back up any Oracle Identity Federation Java Server Pages (JSP) that you customized.

> **Note:** The patching process overwrites JSPs included in the `oif.ear` file. After you complete the patching process, restore your custom JSPs.

In addition to the preceding backups, Oracle recommends performing your organization's typical backup processes.

> **Note:** Refer to the "Backing Up Your Middleware Home, Domain Home and Oracle Instances," "Backing Up Your Database and Database Schemas," and "Backing Up Additional Configuration Information" sections in the *Oracle Fusion Middleware Patching Guide* for detailed information about creating the backups.

#### 4.4.5.3.4 Patch the Database Clients

The Database Client patches are available under the *FA_Repository*/installers/dbclient/patch directory. Follow the patch Readme and apply all the patches in the directory. Proceed as follows to apply all the patches:

- Set your Oracle home to RDBMS_ORACLE_HOME. For example:

  ```
  cd SHARED_LOCATION/11.1.7.0.0/Repository/installers/dbclient/patch
  setenv ORACLE_HOME/u01/oid/oid_home
  ```

- Run opatch using the napply option.

#### 4.4.5.3.5 Patch the WebLogic Servers on all Nodes (see above)

Oracle Fusion Applications 11*g* Release 7 (11.1.7) Identity Management continues to use Oracle WebLogic Server 10.3.6, which is the same version that Release 5 and Release 6 used. However, there may be additional Oracle WebLogic Server patches that you need to apply.

The WebLogic server patches are available under the *FA_Repository*/installers/smart_update/weblogic directory. Follow the patch Readme and apply all patches in the directory. Use the following commands to apply all the patches on *IDM NODE*:

```
cd FA_Repository/installers/smart_update/weblogic
ls *.jar
setenv WLS_PATCH_LIST = "…" # take the list of jars from the output of ls and
create a comma separated list without file extension, for example setenv WLS_
PATCH_LIST "1IHE,1PI6,BEJG,CM69,…"
chmod a+w /u01/oid/utils/bsu/cache_dir/patch-catalog.xml
java
-jar FA_Repository/installers/smart_update/suwrapper/bsu-wrapper.jar
-bsu_home=/u01/oid/utils/bsu/
-install -patchlist=$WLS_PATCH_LIST
-prod_dir=/u01/oid/wlserver_10.3/
-patch_download_dir=FA_Repository/installers/smart_update/weblogic/
-meta=FA_Repository/installers /smart_update/suwrapper/suw_metadata.txt
```

#### 4.4.5.3.6 Patch the WebLogic Servers on IAM Node

Oracle Fusion Applications 11*g* Release 7 (11.1.7) Identity and Access Management continues to use Oracle WebLogic Server 10.3.6, which is the same version that Release 5 and Release 6 used. However, there may be additional Oracle WebLogic Server patches that you need to apply.

Use the following commands:

```
cd FA_Repository/installers/smart_update/weblogic
ls *.jar
setenv WLS_PATCH_LIST = "…" # take the list of jars from the output of ls and
create a comma separated list without file extension, for example setenv WLS_
PATCH_LIST "1IHE,1PI6,BEJG,CM69,…"
chmod a+w /u01/oim/utils/bsu/cache_dir/patch-catalog.xml
```

```
java
-jar FA_Repository/installers/smart_update/suwrapper/bsu-wrapper.jar
-bsu_home=/u01/oim/utils/bsu/
-install -patchlist=$WLS_PATCH_LIST
-prod_dir=/u01/oim/wlserver_10.3/
-patch_download_dir=FA_Repository/installers/smart_update/weblogic/
-meta=FA_Repository/installers/smart_update/suwrapper/suw_metadata.txt
```

#### 4.4.5.3.7 Upgrade IDM Node Binaries to 11.1.1.7

Run IDM installer to upgrade Oracle Internet Directory and Oracle Virtual Directory to 11.1.1.7.

`FA_Repository/installers/idm/Disk1/runInstaller`

Follow the screens shown in Appendix A of *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

Specify Oracle home as `/u01/oid/OID_HOME` and Middleware home as `/u01/oid`.

#### 4.4.5.3.8 Upgrade IAM Node Binaries

Run the following installers:

- Run the IAM installer to upgrade Oracle Identity Manager and Oracle Access Manager to 11.1.7.0.

  `FA_Repository/installers/iamsuite/Disk1/runInstaller`

  Specify the Oracle home as `oim_home` and Middleware home as `/u01/oim`.

- Run the SOA installer to upgrade SOA to 11.1.1.7

  `FA_Repository/installers/soa/Disk1/runInstaller`

  Specify the Oracle home as `/u01/oim/soa_home` and Middleware home as `/u01/oim`.

- If Oracle Identity Federation was installed in the 11.1.1.6 environment, run the IDM installer to upgrade it to 11.1.7.0. Otherwise, skip this step.

  `FA_Repository/installers/idm/Disk1/runInstaller`

  Specify Oracle home as `/u01/oim/fmw_idm_home` and Middleware home as `/u01/oim`.

#### 4.4.5.3.9 Upgrade OHS Node Binaries to 11.1.1.7

Run the following installers:

- Run the OHS installer to upgrade OHS to 11.1.1.7.

  `FA_Repository/installers/webtier/Disk1/runInstaller`

  Specify Oracle home as `/u01/ohsauth/ohsauth_home` and Middleware home as `/u01/ohsauth`.

- Run the WebGate installer to upgrade WebGate to 11.1.1.7

  `FA_Repository/installers/webgate/Disk1/runInstaller`

  Specify Oracle home as `/u01/ohsauth/webgate` and Middleware home as `/u01/ohsauth`.

#### 4.4.5.3.10 Patch IDM_ORACLE_HOME

Apply Oracle Fusion Applications Release 7 patches as follows.

The patches for this Oracle home are available under the *FA_Repository*/installers/pltsec/patch directory for your appropriate platform. Follow the patch Readme and apply all patches in the directory as follows:

1. Set your Oracle home to IDM_ORACLE_HOME. For example:

   ```
   cd FA_Repository/installers/pltsec/patch
   setenv ORACLE_HOME /u01/oid/oid_home
   ```

2. Run opatch using the napply option.

   > **Note:** These patches are based on 11.1.1.7, so you must run the IDM installer to upgrade the binaries to 11.1.1.7 before you can apply these patches.

#### 4.4.5.3.11 Patch the Common Oracle homes on All Nodes

Apply Oracle Fusion Applications Release 7 patches as follows.

You deployment should have at least these (if not more) Oracle Common homes.

- *IDM_ORACLE_COMMON_HOME*

- *IAM_ORACLE_COMMON_HOME*

- *OHS_ORACLE_COMMON_HOME*

The patches for these Oracle homes are available under the *FA_Repository*/installers/oracle_common/patch directory for your appropriate platform. Follow the patch Readme and apply all patches in the directory to the Oracle Common homes as follows:

1. Set your Oracle home to *IDM_ORACLE_COMMON_HOME*. For example:

   ```
   cd FA_Repository/installers/oracle_common/patch
   setenv ORACLE_HOME /u01/oid/oracle_common
   ```

2. Run opatch using the napply option.

3. Set your Oracle home to *ORACLE_COMMON_HOME*. For example:

   ```
   setenv ORACLE_HOME /u01/oim/oracle_common
   ```

4. Run opatch using the napply option.

5. Set your Oracle home to *OHS_ORACLE_COMMON_HOME*. For example:

   ```
   setenv ORACLE_HOME /u01/ohsauth/oracle_common
   ```

6. Run opatch using the napply option.

   > **Note:** You must apply all the patches to all the Common Oracle homes.

#### 4.4.5.3.12 Patch IAM_ORACLE_HOME on the IAM Node

Apply Oracle Fusion Applications Release 7 patches as follows.

The patches for this Oracle home are available under the *FA_ Repository*/installers/idm/patch directory for your appropriate platform. Follow the patch Readme and apply all patches in the directory as follows:

1.  Set your Oracle home to IAM_ORACLE_HOME. For example:

    ```
    cd FA_Repository/installers/idm/patch
    setenv ORACLE_HOME /u01/oim/oim_home
    ```

2.  Run opatch using the napply option.

    > **Note:** Some of the patches have post-patch steps mentioned in the README of the patch. Do not run the post-patch steps now; only apply the patches using opatch napply.

#### 4.4.5.3.13  Patch SOA_ORACLE_HOME on the IAM Node

Apply Oracle Fusion Applications Release 7 patches as follows.

The patches for this Oracle home are available under the *FA_ Repository*/installers/soa/patch directory for your appropriate platform. Follow the patch Readme and apply all patches in the directory as follows:

1.  Set your Oracle home to *SOA_ORACLE_HOME*. For example:

    ```
    cd FA_Repository/installers/soa/patch
    setenv ORACLE_HOME /u01/oim/soa_home
    ```

2.  Run opatch using the napply option.

#### 4.4.5.3.14  Patch OHS_ORACLE_HOME on the OHS Node

Apply Oracle Fusion Applications Release 7 patches as follows.

The patches for this Oracle home are available under the *FA_ Repository*/*installers*/webtier/patch directory for your appropriate platform. Follow the patch Readme and apply all patches in the directory as follows:

1.  Set your Oracle home to *OHS_ORACLE_HOME*. For example:

    ```
    cd FA_Repository/installers/webtier/patch
    setenv ORACLE_HOME /u01/ohsauth/ohsauth_home
    ```

2.  Run opatch using the napply option.

#### 4.4.5.3.15  Patch WEBGATE_ORACLE_HOME on the OHS Node

Apply Oracle Fusion Applications Release 7 patches as follows.

The patches for this Oracle home are available under the *FA_ Repository*/installers/webgate/patch directory for your appropriate platform. Follow the patch Readme and apply all patches in the directory as follows:

1.  Set your Oracle home to *WEBGATE_ORACLE_HOME*. For example:

    ```
    cd FA_Repository/installers/webgate/patch
    setenv ORACLE_HOME /u01/ohsauth/webgate
    ```

2.  Run opatch using the napply option.

#### 4.4.5.3.16  Run Patch Set Assistant (PSA) to Upgrade OID Schemas to PS6

1. Run: `/u01/oid/oracle_common/bin/psa`

2. Choose the schema: `OID`.

3. Specify the OID connection string, for example:
   `idm-db.mycompany.com:1521/oiddb.mycompany.com`

4. Specify the schema name `ODS`, and specify the password for the `ODS` user.

#### 4.4.5.3.17  Run PSA to Upgrade OIM, SOA and Related Schemas to PS6

1. Run: `/u01/oim/oracle_common/bin/psa`

2. Choose the schemas: `ORASPDM`, `MDS`, `SOAINFRA`, and `OIM`.

3. Specify the OIM connection string, for example:
   `idm-db.mycompany.com:1521/oimdb.mycompany.com`

4. Specify the schema passwords and `SYS` password.

#### 4.4.5.3.18  Perform an OPSS Upgrade on IDM Node

Upgrade OPSS by using WLST, as follows:

1. Start Oracle Internet Directory, Oracle Identity Manager managed servers and other Oracle Identity Management services on the IDM node.

2. Execute the command:

```
/u01/oid/oracle_common/common/bin/wlst.sh
upgradeOpss(
jpsConfig='/u01/oid/user_projects/domains/oid_
domain/config/fmwconfig/jps-config.xml',
jaznData='/u01/oid/oracle_common/modules/oracle.jps_11.1.1/domain_
config/system-jazn-data.xml')
```

#### 4.4.5.3.19  Perform an OPSS Upgrade on IAM Node

Upgrade OPSS by using WLST, as follows:

1. Start Oracle Internet Directory, Oracle Identity Manager managed servers and other Oracle Identity Management services on the IAM node.

2. Execute the command:

```
/u01/oim/oracle_common/common/bin/wlst.sh
upgradeOpss(jpsConfig='/u01/oim/user_projects/domains/oim_
domain/config/fmwconfig/jps-config.xml',jaznData='/u01/oim/oracle_
common/modules/oracle.jps_11.1.1/domain_config/system-jazn-data.xml')
```

> **Note:** There is a known issue with the OPSS upgrade. The ODSM managed server generates errors and the URL does not work.
>
> If you encounter this issue, perform the following workaround for Bug 16198253:
>
> 1. Stop the wls_ods1 managed server.
>
> 2. Clean up the `tmp` directory
>
>    ```
>    rm -rf  /u01/oid/user_projects/domains/oid_domain/servers/wls_
>    ods1/tmp/*
>    ```
>
> 3. Start the wls_ods1 managed server.
>
> 4. Perform the upgrade step, using WLST, again.

### 4.4.5.3.20 Apply Patch for Bug 16774077

Follow the instructions in the `README` file.

### 4.4.5.3.21 Run the OIM Script for Upgrade

1. Ensure that the Oracle Database, Oracle Internet Directory, and WebLogic Administration Server are running. The Oracle Identity Manager managed server should be down.

2. Edit the file `/u01/oim/`*OIM_HOME*`/server/bin/oimPS1PS2upgrade.properties` and supply the appropriate values. For an example, refer to the properties in Appendix D.

3. Change directory to `/u01/oim/oim_home/server/bin` and run the upgrade script:

   ```
   cd /u01/oim/OIM_HOME/server/bin/oim
   oimPS1PS2upgrade.sh
   ```

4. Restart the WebLogic Administration server and all Oracle Identity Manager managed servers in the domain.

### 4.4.5.3.22 Upgrade the Oracle Web Services Manager (OWSM) Policies

1. Ensure that the Oracle Database, Oracle Internet Directory, WebLogic Administration Server, and Oracle Identity Manager servers are running.

2. Use WLST to perform the policy upgrade, as follows:

   ```
   /u01/oim/oracle_common/common/bin/wlst.sh
   connect("oim_admin","password", 't3://oimfa.mycompany.com:17001')
   upgradeWSMPolicyRepository()
   ```

## 4.4.5.4 Post-Patch Procedures

> **Note:** Some patches have online post-patch steps. For example, Oracle Identity Manager Patch 16774077 requires that you run `patch_oim_wls.bat` or `patch_oim_wls.sh`.

Perform the procedures in the following sections:

### 4.4.5.4.1 Start the Servers and Apply Post-Patch Steps

> **Note:** For information about starting the components, see
> Appendix E, "Stopping and Starting Identity Management Related
> Servers."

Start servers and processes in the following sequence:

1. Oracle Internet Directory (if not already started)

2. Oracle Virtual Directory

3. Oracle WebLogic Administration Server for the IDM node (if not already started)

4. Oracle Directory Services Manager (ODSM) managed servers

5. Oracle Access Manager managed servers (if not already started)

6. Oracle Identity Federation managed servers

7. Oracle SOA managed servers (if not already started)

8. Oracle Identity Manager managed servers (if not already started)

9. Oracle HTTP Server and Webgate (if not already started)

#### 4.4.5.4.2 Verify the Oracle Identity Management Domain

To verify that the upgrades and patches to the Oracle Identity Management domain
were applied correctly, perform the following steps:

- Confirm you can access and log in to the Oracle WebLogic Administration Server
  console at:

  ```
  http://HOST:ADMIN_SERVER_PORT/console
  https://HOST:SECURE_ADMIN_SERVER_PORT/console
  ```

- Confirm you can access and log in to Oracle Enterprise Manager Fusion
  Middleware Control at:

  ```
  http://HOST:ADMIN_SERVER_PORT/em
  ```

  After completion of the steps in this section, proceed to Section 4.2.10, "Update
  Status to Success."

### 4.4.6 Run RUP Lite for OVM in Pre-Root Mode for Release 7

Run RUP Lite for OVM in pre-root mode locally on every node on the Oracle VM, for
example, primordial, Midtier, IDM, and OHS. Use the `-i` option to point to the Release
7 `rupliteovm/metadata` directory that you set up as part of the pre-upgrade
preparation in Section 2.4.2.2.2, "Prepare RUP Lite for OVM for Release 7". You must
run this command as super user (root).

```
setenv JAVA_HOME java_home_directory
cd /u01/lcm/rupliteovm
bin/ruplite.sh pre-root -i ORCH_LOCATION/config/POD_
NAME/11.1.7.0.0/rupliteovm/metadata
```

Proceed to Section 4.2.13, "Update Status to Success (Oracle VM Only)."

### 4.4.7 Run RUP Lite for OVM in Post-Root Mode for Release 6

Run RUP Lite for OVM in post-root mode locally on every node on the Oracle VM, for
example, primordial, Midtier, IDM, and OHS. Use the `-i` option to point to the Release

6 `rupliteovm/metadata` directory that you set up as part of the pre-upgrade preparation in Section 2.4.2.2.1, "Prepare RUP Lite for OVM for Release 6". You must run this command as super user (root).

```
setenv JAVA_HOME java_home_directory
cd /u01/lcm/rupliteovm
bin/ruplite.sh post-root -i ORCH_LOCATION/config/POD_
NAME/11.1.6.0.0/rupliteovm/metadata
```

Proceed to Section 4.1.13, "Update Status to Success (Oracle VM Only)."

## 4.4.8 Run RUP Lite for OVM in Post-Root Mode for Release 7

Run RUP Lite for OVM in post-root mode locally on every node on the Oracle VM, for example, primordial, Midtier, IDM, and OHS. Use the -i option to point to the Release 7 `rupliteovm/metadata` directory that you set up as part of the pre-upgrade preparation in Section 2.4.2.2.2, "Prepare RUP Lite for OVM for Release 7". You must run this command as super user (root).

```
setenv JAVA_HOME java_home_directory
cd /u01/lcm/rupliteovm
bin/ruplite.sh post-root -i ORCH_LOCATION/config/POD_
NAME/11.1.7.0.0/rupliteovm/metadata
```

Note that this step shuts down the Webchat server.

Proceed to Section 4.2.17, "Update Status to Success (Oracle VM Only)."

## 4.4.9 Start External Servers

Perform the following steps:

- Start GOP Processes
- Start the IIR Instance

### 4.4.9.1 Start GOP Processes

Perform the following steps to start the GOP processes. Note that the `opmnctl` process for `gop_1` should be started only on the host machine which contains the `AdvancedPlanning` Managed Server. Do not start it on the primordial host.

1. Proceed to Step 2 if your GOP processes have been previously configured and have run before.

   If you are starting GOP processes for the first time, confirm that a datasource exists, in the form of XML files, under the *APPLICATIONS_BASE*/instance/gop_ 1/GOP/GlobalOrderPromisingServer1/datastore directory. Then run the `RefreshOpDatastore` ESS job by performing the following steps:

   a. Ensure that the `AdvancePlanning` Managed Server is running in the SCM domain.

   b. Invoke http://*scm - AdvancePlanning managedserver:port*/advancedPlanning/faces/MscCentralEssUi

   c. In the bottom list applet click on **Actions**, then **Schedule New Process**.

   d. Select **Search** under **Name**, and query for %Order%.

   e. Select **Refresh Order Promising Data** and click **OK**.

   f. Select all check boxes in the Process Details popup.

**g.** You can customize some options in the **Advanced** pane, but this is not mandatory.

**h.** Click **Submit** and note the process ID.

**i.** After you confirm that the process is complete, you should see information from the log file that is similar to the following example:

```
Running RefreshOpDatastore Job...
Got service proxy successfully.
Got callback url successfully.
Getting the job-parameters in the Map.
Added job parameters in the map
Web service sucessfully invoked
***** callback received *****
Return Status of job is SUCCESS
```

**j.** Proceed to Step 2.

**2.** Log in to Fusion Applications Control. For more information, see "Accessing Fusion Applications Control" in the *Oracle Fusion Applications Administrator's Guide*.

**3.** Access GOP by navigating to **Oracle Fusion Supply Chain Management**, then **Global Order Promising**, then **GlobalOrderPromisingServer1**.

**4.** Click **GlobalOrderPromisingServer1** to open the GlobalOrderPromisingServer1 page.

**5.** Select **Control** from the menu, then **Start Up**.

### 4.4.9.2 Start the IIR Instance

If you have IIR installed and configured in your environment, you must start IIR before resuming with next steps. Perform the steps in "Starting up and Shutting Down IIR" in the "Define Data Quality" chapter in the *Oracle Fusion Applications Customer Data Management Implementation Guide*.

If you are performing the steps for the Release 5 to Release 6 hop of the chained upgrade, proceed to Section 4.1.16, "Update Status to Success."

If you are performing the steps for the Release 6 to Release 7 upgrade, proceed to Section 4.2.20, "Update Status to Success."

# 5

# Post-Upgrade Tasks for Oracle Fusion Applications

This chapter describes the tasks you must perform after you complete the steps in Chapter 4, "Upgrading to Oracle Fusion Applications Release 7".

This chapter contains the following topics:

- Confirm Database Artifact Deployments Were Successful
- Review the Post RUP Installer Report
- Review the Orchestrator Upgrade Report
- Review Policy Store (JAZN) Analysis Reports
- Reload Custom Templates for BI Publisher Reports
- Add Administration Servers to the Machine Created During Scale Out
- Stop and Start Servers to Remove WebChat Connections
- Delete Webchat Tablespaces (Oracle VM Only)
- Confirm the Informatica Identity Resolution (IIR) Server is Running
- Perform Steps in Release Notes
- Resolve Conflicts That Occurred During Oracle BI Metadata Updates
- Perform Upgrade Steps for Oracle BI Applications
- Upgrade Oracle Fusion Project Portfolio Management Integration with Primavera P6
- Allocate Memory for HCM Workforce Management
- Ensure High Watermark Patch Bundles Were Applied

Note that Upgrade Orchestrator runs Health Checker for post-upgrade checks automatically, but if you want to run Health Checker manually, see Section A.2.2.3, "How to Run Health Checker.".

## 5.1 Confirm Database Artifact Deployments Were Successful

Confirm that the deployment of artifacts updated during the **Load Database Components** configuration assistant was successful by reviewing the Diagnostics report and log files. For more information, see "Diagnostics Report" in the *Oracle Fusion Applications Patching Guide*. Confirm the successful deployment for both Release 6 and Release 7 if you performed a chained upgrade.

## 5.2 Review the Post RUP Installer Report

Review the Post RUP Installer report to check for any errors or warnings that require attention. The Post RUP Installer report provides an overview of the tasks that Upgrade Orchestrator ran when it called RUP Installer. It is generated in HTML and XML files and includes links to log files. If you performed a chained upgrade, review the Post RUP Installer for the upgrade to Release 6 as well as the upgrade to Release 7.

The Post RUP Installer report displays the following information:

- **Configuration Assistant:** The name of the configuration assistant.

- **Attempts:** The number of times the configuration assistant ran.

- **Time Taken:** The duration of the configuration assistant in minutes and seconds.

- **Result:** The result of the configuration assistant, such as PASSED or FAILED.

- **Errors:** Any errors that were reported during the configuration assistant.

- **Log Files:** Link to log files for the configuration assistant.

For Release 6, the Post RUP Installer report files are located here:

*FA_ORACLE_HOME*/admin/FUSION/log/fapatch/fapatch_11.1.6.0:

```
PostRUPInstallerReport_20130613024237.html
PostRUPInstallerReport_20130613024237.log
PostRUPInstallerReport_20130613024237.xml
```

For Release 7, the Post RUP Installer report files are located here:

*APPLICATIONS_CONFIG*/lcm/logs/11.1.7.0.0/RUP:

```
PostRUPInstallerReport_20130610151550.html
PostRUPInstallerReport_20130610151550.log
PostRUPInstallerReport_20130610151550.xml
```

For information about resolving errors, see Chapter 6, "Monitoring and Troubleshooting the Upgrade".

## 5.3 Review the Orchestrator Upgrade Report

Review the Oracle Fusion Applications Orchestrator Upgrade Report to check for any errors or warnings that require attention, to confirm whether the upgrade completed successfully. If there were previous failures during the upgrade, this report would have been generated each time there was a failure. The report name is FAOrchestrationUpgradeReport_*release_hostype_hostname_timestamp*.html. The Upgrade Orchestrator report is generated for each pod and its location is defined in the mandatory ORCH_REPORT_LOCATION property in the *pod*.properties file. Previous reports are archived and available for troubleshooting purposes. For more information, see Section 1.3.4, "Oracle Fusion Applications Orchestrator Upgrade Report".

## 5.4 Review Policy Store (JAZN) Analysis Reports

Review the JAZN Analysis reports for potential conflicts and deletions that are not patched automatically during the upgrade. The reports are located in this directory:

*FA_ORACLE_HOME*/admin/JAZN/*stripe*/delta/report.txt

The *stripe* is crm, fscm, hcm, obi, soa, ucm or bpm.

Review the Modification section of the report to see the roles that were not updated during the upgrade. For each conflict that displays in this report, you must evaluate and manually patch the role by using Oracle Authorization Policy Manager (APM). For more information, see "Upgrading Oracle Fusion Applications Policies" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*.

The following example shows a typical Application Role conflict that has been modified by both the patch and production, therefore it is not applied during the upgrade.

```
MODIFICATION CONFLICTS
Artifact type: Application Role
Artifact Name: OBIA_PARTNER_CHANNEL_ADMINISTRATIVE_ANALYSIS_DUTY
Description: This artifact is modified at attribute level in patch version and
also in production.
```

Note the location of the following files for reference when using APM:

- Location of baseline files, where stripe is crm, fscm, hcm, obi, soa, ucm or bpm:

  *FA_ORACLE_HOME*/admin/JAZN/*stripe*/baseline

- Location of patch files for fscm, crm, and hcm stripes:

  *FA_ORACLE_HOME*/*stripe*/deploy/system-jazn-data.xml

- Location of patch files for the obi, soa, ucm or bpm stripes:

  *FA_ORACLE_HOME*/com/acr/security/jazn/bip_jazn-data.xml

## 5.5 Reload Custom Templates for BI Publisher Reports

Perform this step if you have customized BI Publisher reports.

Reload custom templates for BI Publisher reports on Oracle-delivered BI Publisher reports by following the steps in "Task: Upload the Template File to the Report Definition" in the *Oracle Fusion Applications Extensibility Guide for Business Analysts*.

## 5.6 Add Administration Servers to the Machine Created During Scale Out

Perform the steps in this section only if the steps in Section 2.5.5, "Validate Domain Directories" required you to temporarily add any Administration Servers back to the originally provisioned machine.

1. Log in to the WebLogic console for the domain.

2. Navigate to Environment, then Machines.

3. Find the machine that was created manually for the purposes of AdminServer high availability scaleout.

4. Click on the machine and go to the Servers tab.

5. Click **Lock & Edit** to make changes.

6. Click **Add**.

7. Select the AdminServer and click **Finish**.

8. Click **Activate Changes** to apply the changes.

## 5.7 Stop and Start Servers to Remove WebChat Connections

> **Note:** Perform the step in this section only if you are running Oracle Fusion Applications in an Oracle VM environment that was 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.

Stop and start the servers on the Common Domain and the CRM Managed Server to remove WebChat connections that were disabled by the DisableWebchatConnections plug-in when you ran RUP Lite for OVM. For more information, see "Starting and Stopping the Administration Servers and Managed Servers" in the *Oracle Fusion Applications Administrator's Guide*.

## 5.8 Delete Webchat Tablespaces (Oracle VM Only)

Run the following script to delete Webchat tablespaces:

1. Ensure that there are no guaranteed restore points in the database by performing the following steps:

   a. Connect as SYS user.

   b. Run the following SQL query:

   ```
   SELECT NAME, SCN, TIME, DATABASE_INCARNATION#,GUARANTEE_FLASHBACK_
   DATABASE,STORAGE_SIZE FROM
   V$RESTORE_POINT WHERE GUARANTEE_FLASHBACK_DATABASE='YES';
   ```

   If there are restore points returned by the query, drop the restore points and continue with the next steps.

2. To delete Webchat tablespaces, perform the following steps to run the script that is located on the primordial host.

   a. Connect to the fusion database as SYSDBA user.

   b. Run the following script:

   ```
   /u01/lcm/rupliteovm/ovm/scripts/dropwebchattablespaces.sql
   ```

   > **Note:** If the restore point is still required, perform the steps in this section until the restore point is no longer required, and is dropped.

## 5.9 Confirm the Informatica Identity Resolution (IIR) Server is Running

Confirm the IIR server is running. If it is not running, follow the steps in "Troubleshooting Informatica Identity Resolution and Data Quality Setup" in the "Define Data Quality" chapter of the *Oracle Fusion Applications Customer Data Management Implementation Guide* to manually check for files that need to be cleaned up and to retry the steps to start the server.

## 5.10 Perform Steps in Release Notes

Follow any post-upgrade steps mentioned in the Post-Upgrade Known Issues section of *Release Notes for Oracle Fusion Applications 11g Release 7 (11.1.7.0.0)*.

## 5.11 Resolve Conflicts That Occurred During Oracle BI Metadata Updates

Upgrade Orchestrator updates the applications policies for Oracle Business Intelligence during the **Apply Offline BI Metadata and Configuration Updates** configuration assistant. When Upgrade Orchestrator runs the **Apply Online BI Metadata and Configuration Updates** configuration assistant, it updates the Oracle BI Applications metadata in the Oracle BI repository and the Oracle BI Presentation Catalog for Oracle Fusion Transactional Business Intelligence and Oracle Business Intelligence Applications.

> **Note:** This section refers to different Oracle BI directory paths. The BI Oracle home contains the binary and library files necessary for Oracle BI. *BI_ORACLE_HOME* represents the BI Oracle home in path names.
>
> For more information about the Oracle BI directory structure, see "Oracle Business Intelligence Directory Structure" in *Oracle Fusion Middleware Upgrade Guide for Oracle Business Intelligence*.
>
> Also, see "Understanding Oracle Fusion Middleware Concepts" in *Oracle Fusion Middleware Administrator's Guide* for information about the Fusion Middleware directory structure.

This section contains the following topics:

- Resolve Conflicts in the Oracle BI Presentation Catalog
- Resolve Conflicts in the Oracle Business Intelligence Policy Store

### 5.11.1 Resolve Conflicts in the Oracle BI Presentation Catalog

When you run Upgrade Orchestrator, the Oracle BI Metadata Update Tool overwrites all customizations to catalog objects in the Presentation Catalog with the new Oracle-supplied content and logs conflicts in a conflict report.

After Upgrade Orchestrator completes, you must review the conflict report and decide whether you want to retain the new content or re-apply your customizations using a manual process.

**Points to Consider**

- The folders, `/shared/backup/shared` and `/shared/backup/system`, are created in the updated Presentation Catalog during the Upgrade Orchestrator and the Metadata Update Tool process. You access these folders through the Folders pane of the Catalog page in the Oracle BI Enterprise Edition user interface, as described in the following procedure.

  **Note:** The `/shared/backup` folder should not exist before Upgrade Orchestrator runs, because the updated Presentation Catalog file will not be copied to this folder if it already exists.

  As a precaution, to ensure the `/shared/backup` folder does not exist before Upgrade Orchestrator runs, you can optionally create an environment variable called `webcat.force.restore`, which will overwrite the contents of an existing

/shared/backup folder. This environment variable must be set in the shell prompt from where the orchestrator is going to be invoked, using the command, `setenv webcat.force.restore true`.

■ Conflicts that arise during Upgrade Orchestrator and the Metadata Update Tool process are stored in the folder /shared/backup/shared in the updated Presentation Catalog. Object references that have conflicts are also stored in /shared/backup/shared.

**To resolve conflicts in the Presentation Catalog:**

1. Locate the conflict report named `update-conflict-report.txt`, which is stored in the folder *BI_SHARED_DIR*/.biapps_patch_storage/update/*Run_ID*.

2. Sign in to Oracle Business Intelligence Enterprise Edition (Oracle BI EE).

   See "Signing In to Oracle BI Enterprise Edition" and "Navigating Oracle BI Enterprise Edition" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition (Oracle Fusion Applications Edition)* for instructions on signing in and navigating in the Oracle BI EE user interface.

3. Click **Catalog** in the global header.

4. In the Folders pane, navigate to **Shared Folders**, **backup**, and then **shared folder**.

5. Open an object that has a conflict. This object depicts the state of the object before Upgrade Orchestrator and the Metadata Update Tool were run.

6. Open a second instance of Oracle BI EE and the Presentation Catalog.

7. Navigate to the **Shared Folders** folder.

8. Open the same object you opened in step 5. This object depicts the state of the object after Upgrade Orchestrator and the Metadata Update Tool were run (and after the metadata updates were applied).

9. Compare the two objects and decide whether you want to retain the Oracle-supplied updated content or re-apply your customization from the previous version of the Presentation Catalog.

10. To re-apply your customization to an updated object, manually edit the object.

11. Repeat steps 5 through 10 for all objects that have conflicts.

## 5.11.2 Resolve Conflicts in the Oracle Business Intelligence Policy Store

When you run Upgrade Orchestrator, the Oracle BI Metadata Update Tool performs a safe upgrade on the Oracle Business Intelligence policy store, which means it updates only the metadata content that does *not* conflict with your customizations. Updated content that conflicts with your customizations is not applied. Conflicts are listed in the Oracle BI Metadata Tool update report, located at *BI_SHARED_DIR*/.biapps_patch_storage/update/*Timestamp*/policystore_delta/report.txt.

This procedure provides instructions for overriding the customizations of the previous Oracle Business Intelligence policy store by applying the Oracle-supplied updated content. This procedure uses Oracle Authorization Policy Manager. For detailed information about upgrading Oracle Fusion Applications policies using Oracle Authorization Policy Manager, see "Upgrading Oracle Fusion Applications Policies" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*.

**Note:** You do not need to back up your existing policy store file, because the Metadata Update Tool process does not overwrite your customizations.

**To resolve conflicts in the policy store:**

1. Log in to the Authorization Policy Manager Administration Console.

   See "Getting Started With Oracle Authorization Policy Manager" in *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)* for instructions.

2. Navigate to the **Home** tab of the Policy Upgrade Management page.

3. Click **Patch Application** in the upper-left corner of the page to display the Patch Application dialog.

4. Select the appropriate application from the **Application** list.

5. In the **Patch File** field, specify the new patch file name and location, for example, `BI_ORACLE_HOME/bifoundation/admin/provisioning/biapps-policystore.xml`.

6. In the **Baseline** field, specify the previous policy store that was backed up by the Oracle BI Metadata Update Tool, for example, `BI_ORACLE_HOME/.biapps_patch_storage_UPGRADE_from_VERSION/OH_BACKUP/bifoundation/admin/provisioning/biapps-policystore.xml`.

7. Navigate to the **Patch Details** tab to view the policy store conflicts.

   See the sections titled "Analyzing Patch Differences" and "Resolving Changes and Conflicts" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)* for instructions on taking the appropriate action regarding conflicts.

## 5.12 Perform Upgrade Steps for Oracle BI Applications

If you are deploying Oracle Business Intelligence Applications, then you must perform the post-installation or upgrade steps specified in "Roadmap for Installing, Setting Up, and Upgrading Oracle BI Applications" in the *Oracle Fusion Middleware Installation and Configuration Guide for Oracle Business Intelligence Applications*.

## 5.13 Upgrade Oracle Fusion Project Portfolio Management Integration with Primavera P6

If you have installed Oracle Fusion Project Portfolio Management and configured it to integrate with Primavera P6 Enterprise Project Portfolio Management, then perform the following manual steps, depending on whether you are upgrading from Release 6 or from Release 5.

### 5.13.1 Upgrade From Release 5

Perform the following steps if you are upgrading from Release 5:

1. Register the Primavera P6 Endpoint address details in Oracle Fusion Functional Setup Manager.

   a. Click 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*

2. Upgrade the Fusion PPM Bridge and other related configurations in Primavera P6. For more information, see "Upgrading to Fusion REL 6" in the *Primavera P6 EPPM Administrator's Guide for an Oracle Database*.

### 5.13.2 Upgrade from Release 6

Perform this step if you are upgrading from Release 6.

Upgrade the Fusion PPM Bridge and other related configurations in Primavera P6. For information on upgrading and working with Oracle Fusion Project Portfolio Management, see "Updating Fusion PPM Bridge in WebLogic" in the *Primavera P6 EPPM Administrator's Guide for an Oracle Database*.

## 5.14 Allocate Memory for HCM Workforce Management

This section is applicable only if you plan to use the Human Capital Management (HCM) Workforce Reputation Management product packaged with the Workforce Deployment, or Workforce Development product offerings.

1. The physical machine hosting 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 HCM Workforce Reputation Management (`WorkforceReputationServer_1`) managed server. The HCM Workforce Reputation Management externalization process may use up to 16 GB of memory.

   Perform the following steps to specify memory allocation for HCM Workforce Reputation Management (`WorkforceReputationServer_1`) managed server:

   - Edit the fusionapps_start_params.properties file located under *APPLICATIONS_CONFIG*/domains/*host_name*/HCMDomain/config.

   - Locate the # HCMDomain: Main Settings section in the file. Replace the line:

     ```
     fusion.HCMDomain.WorkforceReputationCluster.default.minmaxmemory.main=-Xms512m -Xmx2048
     ```

     with:

     ```
     fusion.HCMDomain.WorkforceReputationCluster.default.minmaxmemory.main=-Xms4096m -Xmx8192m
     ```

   - Save the `fusionapps_start_params.properties` file.

2. Restart HCM Workforce Reputation Management (`WorkforceReputationServer_1`) managed server either from the WebLogic console or Enterprise Management for the HCM domain. For more information, see "Chapter 4, Performing Routine Administrative Tasks" in the *Oracle Fusion Applications Administrator's Guide*.

## 5.15 Ensure High Watermark Patch Bundles Were Applied

Ensure you have applied the following high water mark patch bundles on your current environment prior to upgrading to next release:

- Fusion Middleware Patch Bundles for Fusion Applications

- Fusion Application Patch Bundles

To get more information about high watermark patch bundles, contact Oracle Support.

# 6

# Monitoring and Troubleshooting the Upgrade

This chapter provides information to assist you in troubleshooting upgrade issues.

This chapter contains the following topics:

## 6.1 General Troubleshooting for an Upgrade Orchestrator Failure

When Upgrade Orchestrator exits with a failure on any upgrade task, it sends an email to the recipients specified in the `EMAIL_TO_RECIPIENT` and `EMAIL_CC_RECIPIENT` properties in the `pod.properties` file. This email contains the Oracle Fusion Applications Orchestrator Upgrade Report as an attachment. The report name is `FAOrchestrationUpgradeReport_release_hosttype_hostname_timestamp.html`. This report specifies the location of the Fusion Applications Orchestration Action Summary

report, which provides information about the failure, corrective action, and relevant log files. The orchestration log file is a good point to start for any troubleshooting, as it captures logs from different upgrade tasks as well as console messages. The orchestration log file is located in *APPLICATIONS_CONFIG*/lcm/logs/11.1.7.0.0/orchestration/*host_name*-rel5-7_*hosttype_timestamp*.log.

Figure 6–1 depicts the high level flow for troubleshooting Upgrade Orchestrator failures.

*Figure 6–1   Troubleshooting Flow*
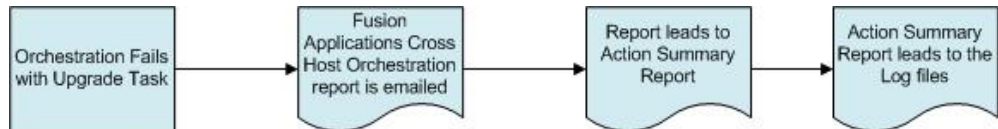


Figure 6–2 depicts the reports and log files generated by Upgrade Orchestrator.

*Figure 6–2   Upgrade Orchestrator Reports*



Previous reports are archived whenever a new report is generated, as described in Section 6.6.3, "Unable to Find the Orchestrator Upgrade Report After Failure". For more information about the report, see Section 1.3.4, "Oracle Fusion Applications Orchestrator Upgrade Report".

## 6.2  Log Locations

The following types of log files are described in this section:

## 6.2.1 Upgrade Orchestrator Log File Directories

The following table contains a list of log directories for Upgrade Orchestrator activities. Note that for the chained Release 5 to 6 to 7 upgrade, the log directories for Upgrade Orchestrator activities are logged under 11.1.7.0.0 even when you are running the Release 5 to Release 6 upgrade. If you want to use a different location for log directories, provide the location in the LOG_LOCATION property, which exists in the IDM.properties and OHS.properties files. For more information, see Appendix B, "Upgrade Orchestrator Properties Files".

*Table 6–1    Log Directories for Upgrade Orchestrator Activities*

| Log directory name | Description |
|---|---|
| *host_name*-rel5-7_*timestamp*.html | HTML files on the primordial and midtier hosts. |
| *APPLICATIONS_CONFIG*/lcm/logs/11.1.7.0.0/orchestration/*host_name*-rel5-7_*timestamp*.log | Log files on the primordial and midtier hosts. |
| *ORCH_LOCATION-host_name*-rel5-7_*timestamp*.html | HTML files on the OHS, IDM, and database hosts. |
| *APPLICATIONS_CONFIG*/instance/lcm/logs/11.1.7.0.0/orchestration/ARCHIVE/*host_name*_rel5-7/*timestamp* | Directory for archived log files |
| Under the *host_name*-rel5-7_worker/DowntimePostFA directory:<br><br>■ *host_name*-rel5-7_CopyWebtierUpgradeToCentralLoc_*timestamp*.log<br><br>■ *host_name*-rel5-7_DataQualityChecks_*timestamp*.log<br><br>■ *host_name*-rel5-7_PostUpgradeChecks_*timestamp*.log<br><br>■ *host_name*-rel5-7_UpdateMDSSOAComposite_*timestamp*.log<br><br>■ *host_name*-rel5-7_VitalSignsChecks_*timestamp*.log<br><br>Under the *host_name*-rel5-7_primordial_worker/PreDowntime directory:<br><br>■ *host_name*-rel5-7_DataQualityChecks_*timestamp*.log<br><br>■ *host_name*-rel5-7_PreDowntimeChecks_*timestamp*.log | Individual log files for the Health Checker plug-ins that run in parallel, which are stored in separate directories. |

## 6.2.2 RUP Installer Log File Directories

The following table contains a list of log directories for RUP Installer activities.

*Table 6–2    Log Directories for RUP Installer Activities*

| Log directory name | Description |
| --- | --- |
| *oracle_inventory*/logs | Installation phase and Oracle Fusion Middleware patch set installation logs. |
| *APPLICATIONS_ CONFIG*/lcm/logs/11.1.7.0.0/RUP | Top level directory for RUP Installer logs. |
| *APPLICATIONS_ CONFIG*/lcm/logs/11.1.7.0.0/RUP/ARCHIVE/*t imestamp* | Top level log directory where log files are moved when you retry the installation session. |
| *APPLICATIONS_ CONFIG*/lcm/logs/11.1.7.0.0/RUP/configlogs | Top level log directory for configuration assistants. A log file exists for each configuration assistant. For more information, see Section 6.2.2.1, "Log Files for Configuration Assistants". |
| *APPLICATIONS_ CONFIG*/lcm/logs/11.1.7.0.0/RUP/PatchManage r_DBPatch | Database upload configuration assistant logs after failure or completion. For more information, see Section 6.2.2.2, "Log Files for the Database Upload Configuration Assistant". |
| *APPLICATIONS_ BASE*/instance/BIInstance/diagnostics/logs | Oracle Business Intelligence logs. |
| *APPLICATIONS_ CONFIG*/lcm/logs/11.1.7.0.0/RUP/StartStop | StartStop utility logs. Note that server logs are located under respective domains. For example, the AdminServer log for CommonDomain is under *APPLICATIONS_ CONFIG*/domains/*hostname*/CommonDomain /servers/AdminServer/logs. |
| *APPLICATIONS_ CONFIG*/lcm/logs/11.1.7.0.0/RUP/soalogs | SOA artifacts configuration assistant logs. Note that SOA server logs are located under respective domains. For example, the SOA server logs for CommonDomain are under *APPLICATIONS_ CONFIG*/domains/*hostname*/CommonDomain /servers/soa_server1/logs. For more information, see Section 6.16.1, "SOA Composite Log Files". |
| *APPLICATIONS_ CONFIG*/lcm/logs/11.1.7.0.0/RUP/PatchManage r_DownloadedPatches | Applying Downloaded Patches configuration assistant logs. |

### 6.2.2.1  Log Files for Configuration Assistants

During the configuration phase of the upgrade, each configuration assistant creates its own log file under the *APPLICATIONS_CONFIG*/lcm/logs/11.1.7.0.0/RUP/configlogs directory. All messages that are generated during the configuration assistant processing are written to this log file. The only information related to configuration assistants that is written to the main log file, *APPLICATIONS_ CONFIG*/lcm/logs/11.1.7.0.0/RUP, are those messages that indicate that a configuration assistant started and the result of its processing, such as success or error.

### 6.2.2.2  Log Files for the Database Upload Configuration Assistant

During the execution of the database upload configuration assistant, log files are created under the /lcm/logs directory. Upon completion or failure of the database

upload, the log files move to the *APPLICATIONS_ CONFIG*/lcm/logs/11.1.7.0.0/RUP/PatchManager_DBPatch directory.

### 6.2.2.3  Log Files for Upgrade from Release 5 to Release 6

Release 6 log files are located in this directory:

```
APPLICATIONS_BASE/fusionapps/applications/admin/FUSION/log/fapatch/fapatch_
11.1.6.0
```

If you are performing a chained upgrade from Release 5 to Release 6 to Release 7, before starting the upgrade to Release 7, the Release 6 logs will move to this archive location:

```
APPLICATIONS_CONFIG/lcm/archive/log/fapatch/fapatch_11.1.6.0.0
```

## 6.2.3  Log Files for RUP Lite for OVM

The log file for running RUP Lite for OVM in pre-root mode is in the following location:

```
/u01/lcm/rupliteovm/output/logs/11.1.7.0.0/host_name/ruplitepre-root.log
```

Log files for running RUP Lite for OVM in post-root mode are in the following locations:

- For the Release 5 to Release 6 hop:

  ```
  /u01/lcm/rupliteovm/output/logs/11.1.6.0.0/host_name/ruplitepost-root.log
  ```

- For the Release 6 to Release 7 hop:

  ```
  /u01/lcm/rupliteovm/output/logs/11.1.7.0.0/host_name/ruplitepost-root.log
  ```

# 6.3  Monitoring Upgrade Orchestration Progress

You can monitor the progress of the upgrade by monitoring the console output or by running the getStatus command. You can run this command on any host, to get the upgrade status for that host or for other hosts. The command follows:

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh getStatus -pod POD_NAME -hosttype host_type -hostname host_name
-release release_version [-phase phase_name] [-taskid task_id] [-taskstatus task_
status]

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd getStatus -pod POD_NAME -hosttype host_type -hostname host_name
-release release_version [-phase phase_name] [-taskid task_id] [-taskstatus task_
status]
```

#### Example 6–1   Retrieve the overall status of the upgrade

```
./orchestration.sh getStatus -pod fcsm -hosttype PRIMORDIAL -hostname host_name
-release REL7
```

#### Example 6–2   Retrieve all tasks in a phase

```
./orchestration.sh getStatus -pod fcsm -hosttype PRIMORDIAL -hostname host_name
-release REL7 -phase predowntime
```

***Example 6–3   Retrieve all tasks with a specific status***

```
./orchestration.sh getStatus -pod fscm -hosttype PRIMORDIAL -hostname host_name
-release REL7 -taskstatus success
```

***Example 6–4   Retrieve the status of a specific task***

```
./orchestration.sh getStatus -pod fscm -hosttype PRIMORDIAL -hostname host_name
-release REL7 -taskid HostTypeValidatePlugin
```

Table A–3 displays a complete list of options for the `orchestration.sh getStatus` command.

If any upgrade tasks fail, the Orchestrator Upgrade Report is generated and mailed as an attachment to the user specified in the `EMAIL_TO_RECIPIENT` property in the `pod.properties` file. For more information, see Section 1.3.4, "Oracle Fusion Applications Orchestrator Upgrade Report". For information about troubleshooting failures, refer to the appropriate section in Chapter 6, "Monitoring and Troubleshooting the Upgrade" to resolve the issue. After a failure, restart Orchestrator on the host where it failed, using the same commands you used in Section 4.1.2, "Run Upgrade Orchestrator During Down Time".

If any configuration assistants fail while RUP Installer is running, Upgrade Orchestrator does not display a message, fail, or send an email until RUP Installer exits with a failure.

If the Loading Database Components step in RUP Installer fails, you receive an email notification only when all workers are in a FAILED or IDLE (no tasks assigned to it) state. To resolve this type of issue, follow the steps in Section 6.13.1, "Error While Loading Database Components Using Orchestration".

## 6.4  Terminate Upgrade Orchestration

Orchestration can be terminated on all hosts under scenarios that require you to issue an exit command across the entire environment. This section describes the commands to use to terminate orchestration on all hosts.

When you need to terminate an orchestration session on a pod for reasons such as, not being able to complete the upgrade within a certain time, or unexpected issues that may require significant time to resolve, run the following command:

```
cd /ORCH_LOCATION/bin
./orchestration.sh exitOrchestration –pod POD_NAME –hosttype host_type
```

The `exitOrchestration` command terminates the orchestration session on all hosts across all host types in the specified pod. This command can be run from any individual host for the entire environment and/or pods. The `hosttype` argument must match the host from which you issue this command. Upgrade Orchestration sends a notification after all hosts exit from orchestration. After you receive this notification, you must run the following command to clear the exit status on all hosts:

```
cd /ORCH_LOCATION/bin
./orchestration.sh clearExitOrchestration -pod POD_NAME –hosttype host_type
```

After the `clearExitOrchestration` command runs, you can continue with the upgrade or take other appropriate actions on the pod.

> **Note:** From the time `exitOrchestration` is issued, until
> `clearExitOrchestration` is issued, no other command can be issued
> on the `pod`. Also, `exitOrchestration` can be issued from any host but
> is applicable for all the hosts under a pod.

## 6.5 Canceling the Oracle Fusion Applications Upgrade and Restoring From Backup

To cancel the upgrade and restore the system, first terminate orchestration by
following the steps in Section 6.4, "Terminate Upgrade Orchestration". After
orchestration terminates successfully, restore the system from the backup that was
taken before starting the upgrade. In addition to restoring the environment from the
backups, perform the following steps to restore and clean up the orchestration files.

1. Directories configured for the following properties in `pod.properties` are used by
   Upgrade Orchestrator to store checkpoint files and to archive older versions of
   checkpoint files.

   - ORCHESTRATION_CHECKPOINT_LOCATION

   - ORCHESTRATION_CHECKPOINT_ARCHIVE_LOCATION

   Note that if these configured directories are shared among multiple instances then,
   orchestration would have created *POD_NAME* sub directories.

2. Run the following commands to remove any checkpoint location and its contents:

   ```
   rm -rRf ORCHESTRATION_CHECKPOINT_LOCATION/POD_NAME/*
   rm -rRf ORCHESTRATION_CHECKPOINT_ARCHIVE_LOCATION/ARCHIVE/POD_NAME/*
   ```

### 6.5.1 Confirm That Required Mount Points Exist (Oracle VM Only)

Ensure that `/u02/instance/CommonDomain_webtier_local` remains a mount point. If
you are restoring the environment from a backup, also restore the `/u02/instance`
directory by running the following commands:

```
rm -rf /u02/instance/CommonDomain_webtier_local
```

```
mkdir /u02/instance/CommonDomain_webtier_local
```

```
su
```

```
mount | grep u01
```

The mount command finds the device that contains the /u01 directory. An example of
the output from this command follows:

```
host_name:/export/fusion_imf/appohs_imf/u01 on /u01 type nfs
(rw,addr=11.222.333.444)
```

Use the device name returned by the mount command, and run the following
command:

```
mount -t nfs device_name
```

An example of this command follows:

```
mount -t nfs host_name:/export/fusion_imf/appohs_imf/u02/instance/CommonDomain_
webtier_local /u02/instance/CommonDomain_webtier_local
```

```
exit
```

The following command provides an example for copying files from the backup instance to the active instance directory:

```
cp -rf /u02/instance_backup_location/CommonDomain_webtier_local
/u02/instance/CommonDomain_webtier_local
```

# 6.6 Troubleshooting Specific Upgrade Orchestrator Scenarios

This section describes the following specific Upgrade Orchestrator troubleshooting scenarios:

- Orchestration Failure With Checkpoint Location
- Safely Exit Upgrade Orchestrator
- Unable to Find the Orchestrator Upgrade Report After Failure
- Orchestration Fails to Generate Report With an Out Of Memory Error
- Invalid property: must specify ORCHESTRATION_CHECKPOINT_LOCATION
- Phase in Error Status, All Tasks Were Successful
- Orchestrator Fails With an Update Status Error
- Emails Are Not Being Sent Upon Failure
- Upgrade Orchestrator Does Not Use a Value in the Properties File
- Stale NFS File Handle Error
- Cannot Remove Snapshot File Error
- Informatica Identity Resolution (IIR) Does Not Come Up After the Upgrade
- Error Reported in CREATING_MIDDLEWARE_SCHEMAS Log

## 6.6.1 Orchestration Failure With Checkpoint Location

### Problem

When orchestration is relaunched due to any reason, there could be an error loading checkpoint files to the appropriate location. In this case, Upgrade Orchestrator exits with the following errors.

```
Unable to upload orchestration checkpoints under
/fsnadmin/upgrade/fusionChangeOps/11.1.7.0.0/orchestration/bin/../checkpoint.
Corrective Action: Remove any existing files from older Orchestration run in
/fsnadmin/upgrade/fusionChangeOps/11.1.7.0.0/orchestration/bin/../checkpoint
before you proceed.
```

### Solution

Perform the required corrective action suggested in the error message and then resume Upgrade Orchestrator to proceed with the upgrade.

## 6.6.2 Safely Exit Upgrade Orchestrator

### Problem

Orchestration hangs during the `preDowntime` or `downtimeFA` phase, or you need to exit Upgrade Orchestrator in the middle of an upgrade for any valid reason.

**Solution**

Run the `exitOrchestration` command from another console, on any host in the pod, to gracefully exit orchestration. Then run `clearExitOrchestration`. For more information, see Section 6.4, "Terminate Upgrade Orchestration".

The `exitOrchestration` command terminates the upgrade on all hosts. Therefore, after you resolve the issue, rerun orchestration on all hosts where orchestration was previously running.

### 6.6.3 Unable to Find the Orchestrator Upgrade Report After Failure

**Problem**

After Upgrade Orchestrator fails, the console reports the following example information:

```
Fusion Applications Orchestrator Upgrade Report:
/u01/orchestration/orchreports/FAOrchestrationUpgradeReport_release_hosttype_
hostname_timestamp.html
```

This html file does not exist in the `/u01/orchestration/orchreports` directory.

**Solution**

As the upgrade progresses, the Orchestrator Upgrade report is archived after the failure or completion of each task. You can find the output in the following directory, based on the example.

```
/u01/orchestration/orchreports/ARCHIVE/11.1.6.0.0/2013-05-13_11_
38-48AM/FAOrchestrationUpgradeReport_release_hosttype_hostname_timestamp.html
```

### 6.6.4 Orchestration Fails to Generate Report With an Out Of Memory Error

**Problem**

Upgrade Orchestrator fails while generating the Upgrade Orchestrator report with the following error:

```
"Java.lang.OutOfMemoryError: PermGen space
```

**Solution**

Increase the `ORCH_JVM_OPTION` value in `pod.properties` to allocate more memory for both the startup of JVM and the total size of `permgen`, as shown in the following example:

```
ORCH_JVM_OPTION=-Xmx2048m -XX:PermSize=256M -XX:MaxPermSize=512M
```

### 6.6.5 Invalid property: must specify ORCHESTRATION_CHECKPOINT_LOCATION

**Problem**

Property validation fails during the `PreDowntime` phase with the following error:

```
Invalid property: must specify ORCHESTRATION_CHECKPOINT_LOCATION in orchestration
properties file ./../config/pod/pod_properties.
```

No log file or HTML file is generated.

#### Solution

Populate the `ORCHESTRATION_CHECKPOINT_LOCATION` mandatory property in the `pod.properties` file. Note that no logs are generated for this type of failure by design.

### 6.6.6 Phase in Error Status, All Tasks Were Successful

#### Problem

You ran the `updateStatus` command to manually set the status of a failed `task_id` on the primordial host to "success" for the `PreDowntime` phase. After you resume orchestration on the IDM host, it fails with the following error:

```
Wait for peer phase: PRIMORDIAL:PreDowntime on host.mycompany.com
Found peer phase: PRIMORDIAL:PreDowntime on host.mycompany.com Error.
```

The results of `getStatus` on the pod shows that all tasks were successful but the `PreDownTime` phase was in error status.

#### Solution

Setting a task status to "success" does not resolve a "Wait for peer phase" error, because a phase level status cannot be updated by the `updateStatus` command. The only way to resolve a "Wait for peer phase" issue is to resume orchestration so that it can verify that all tasks in the phase were successful.

### 6.6.7 Orchestrator Fails With an Update Status Error

#### Problem

An orchestration task is no longer running and the following error is reported:

```
Orchestration step: DowntimePreFA DeploySoaShared Running
Unable to update task status from Running to Success

Oracle Fusion Applications Release Upgrade Orchestration failed.
```

#### Solution

Before performing the step in this solution, confirm that there are no orchestration processes running. Then run the `updateStatus` command to change the status of the task specified in the error message to error and then resume Upgrade Orchestrator.

Upgrade Orchestrator supports only the following status transitions:

- Error to Success
- Running to Error
- ManualStep to Success
- Success to Error

### 6.6.8 Emails Are Not Being Sent Upon Failure

#### Problem

The emails that Upgrade Orchestrator sends upon failure are not being received.

#### Solution

Perform the following steps to check if your mail server is configured properly:

1. You can check if your mail server is configured properly by running the following command:

   ```
   "echo hello | /usr/sbin/sendmail <email_addr>"
   ```

2. If emails are not being sent, restart the mail server and test again.

   ```
   /etc/init.d/sendmail restart
   ```

3. Ensure that all properties related to email are populated with the correct values in the pod.properties file. For more information, see Table B–1, " pod.properties".

## 6.6.9 Upgrade Orchestrator Does Not Use a Value in the Properties File

### Problem

Upgrade Orchestrator is not using a value that was recently added to one of the properties files.

### Solution

If you updated the properties file after launching Upgrade Orchestrator, follow the steps to safely exit orchestration in Section 6.6.2, "Safely Exit Upgrade Orchestrator" and then relaunch orchestration.

## 6.6.10 Stale NFS File Handle Error

### Problem

While running various commands for Upgrade Orchestrator, the following error is reported:

```
Stale NFS file handle
```

### Solution

If the Stale NFS file handle error is reported while running any of the plug-ins in orchestration or the getStatus or updateStatus commands, verify that all mount points provided in the various property files are actually accessible. For more information, see Appendix B, "Upgrade Orchestrator Properties Files".

## 6.6.11 Cannot Remove Snapshot File Error

### Problem

The following error causes Upgrade Orchestrator to fail:

```
rm: cannot remove
`/u01/ORCH/orchestration/INIT/mycompany.com/IDM/INIT/snapshot/.nfs00000000015595b3
0000004b': Device or resource busy

Oracle Fusion Applications Release Upgrade Orchestration failed.
```

### Solution

Remove the file that is causing the error and restart Upgrade Orchestrator.

### 6.6.12 Informatica Identity Resolution (IIR) Does Not Come Up After the Upgrade

**Problem**

IIR does not come up after following the steps to start IIR as part of the Start External Servers Pause Point Post Upgrade step.

**Solution**

Follow the steps in "Troubleshooting Informatica Identity Resolution and Data Quality Setup" in the "Define Data Quality" chapter of the *Oracle Fusion Applications Customer Data Management Implementation Guide* to manually check for files that need to be cleaned up and to retry the steps to start the server.

### 6.6.13 Error Reported in CREATING_MIDDLEWARE_SCHEMAS Log

**Problem**

The following error is reported:

```
[apps] [ERROR] [] [oracle.apps.ad.rupconfig.Creating_Middleware_Schemas] from
oracle.security.audit.config.dynamic.persistence.internal.ldap.AuditStoreDataManag
er searchFilterPresets
```

**Solution**

This error can be ignored.

## 6.7 Troubleshooting RUP Installer Failures

This section provides information about the following RUP Installer failures:

- General Troubleshooting During the Configuration Phase in GUI Mode
- General Troubleshooting During the Configuration Phase in Silent Mode
- RUP Installer Fails
- RUP Installer or InstallFaSaaSLcmTools Fails Due To Thread Calls
- RUP Installer or InstallFaSaaSLcmTools Fails With Internal Error
- RUP Installer Part 1 Fails on Primordial Host
- Installer Requirement Checks Fail
- Recovering From an Installer Session That Was Shut Down
- Failure During Importing Oracle Data Integrator Repositories
- Deploying New Application Configuration Fails with a "NumberFormatException"
- Failure During the Extending Certificate Validity Phase
- Failure During Importing Group Space Templates
- Configuration Assistant Fails With "Could not create credential store instance"
- Failure During Starting All Servers or Restarting SOA Servers

## 6.7.1 General Troubleshooting During the Configuration Phase in GUI Mode

This section describes the following troubleshooting scenarios related to the configuration phase in GUI mode:

- Restart a Failed Installer Session

- Troubleshoot Failures While Parallel Tasks Are Running

- The Next Button Is Not Enabled During Configuration Assistants

- The OPSS Security Store Goes Down While the Installer is Running

- Failure During Opening of Wallet Based Credential Store

### 6.7.1.1 Restart a Failed Installer Session

The installer can be restarted to rerun all failed configuration assistants as well as those configuration assistants that were not started from the previous session. When a configuration assistant or step fails, the Configuration Progress screen displays the location of the log file and the exception that caused the failure. You can also view the content of the log files that appear at the bottom of the screen to obtain detailed information to assist in diagnosing the cause of the failure.

If one or more failures occur during the configuration phase, after the final configuration assistant is complete, the following message displays:

**Configuration is completed with errors, exit the installer by clicking the 'Cancel' button and retry the failed configurations**.

Perform the following steps to rerun the installer and retry the failed configuration assistants:

1. Click **Cancel** to exit the installer.

2. Resolve the issues that caused the failure.

3. Start the installer using the same command syntax that you used for the previous incomplete installation.

4. A pop up dialog displays, asking if you want to continue the previous incomplete installation. Select **Yes** to continue running the previous session. If you select **No**, the installer starts from the beginning and it will fail, indicating that a release cannot be installed again in the same environment. You would then need to restore from your backup and restart the installer.

5. The Configuration Progress screen displays only the failed and remaining configuration assistants, and then runs these configuration assistants.

6. Assuming all configuration assistants complete successfully, click **Next** to go to the Installation Complete screen and then click **Finish** to end the session. If a configuration assistant fails again and you want to attempt to run the session again, click **Cancel** to save the session. If all configuration assistants were successful for the first installer, the second installer launches automatically. If all configuration assistants completed successfully, click **Finish** to end the session.

   Note that Language Pack runs only one installer.

### 6.7.1.2 Troubleshoot Failures While Parallel Tasks Are Running

If one or more tasks in a group fail, you can select the failed tasks in any combination, and the **Abort**, **Retry**, and **Continue** buttons are enabled as appropriate for the selected tasks. For example, if two tasks in a group fail, and the first task allows you to

select **Continue**, but the other task does not, then the **Continue** button is not enabled if you select both tasks.

You can process one or more failed tasks at a time. For example, if three tasks fail, you can retry one of them, and while it is running, you can abort the second task. Then you can retry the third task. When the first and third tasks finish processing, the next step depends on whether the second task is mandatory. If it is a mandatory task, the installer stops, and if it is non-mandatory the installer continues with the next task after the group. You can also pick two out of three or all three tasks and select **Retry**, **Abort,** or **Continue**, based on which buttons are enabled.

Note that all tasks in a group must either fail or complete successfully before the **Cancel** button is enabled.

The following example depicts a group of four configuration tasks that are running in parallel and three of the four tasks fail.

1. Four tasks were running in parallel. Three tasks fail and the remaining task is successful. Note that the **Abort**, **Retry**, and **Continue** buttons are not enabled because the check boxes for the failed tasks are not checked. In the case of failure, the check boxes are enabled for failed tasks only after all tasks in the group have either failed or completed successfully.
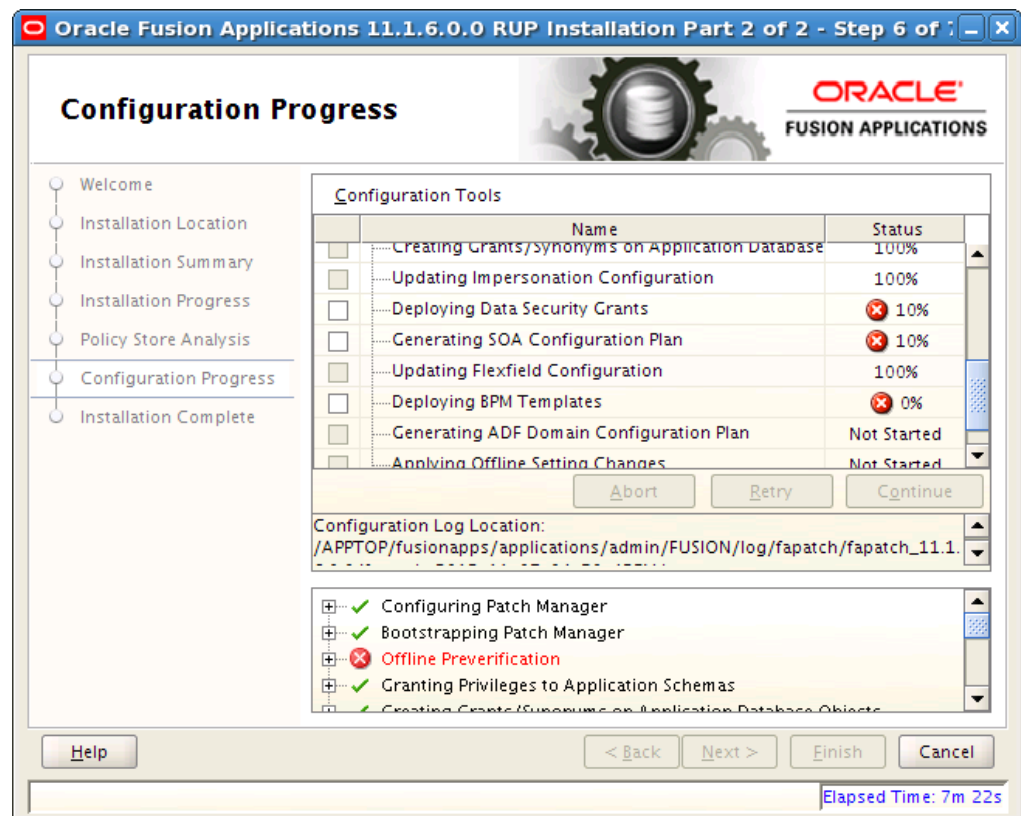


2. After you select the failed tasks, the **Abort**, and **Retry** buttons are enabled. The **Continue** button is not enabled because the failed tasks are mandatory.
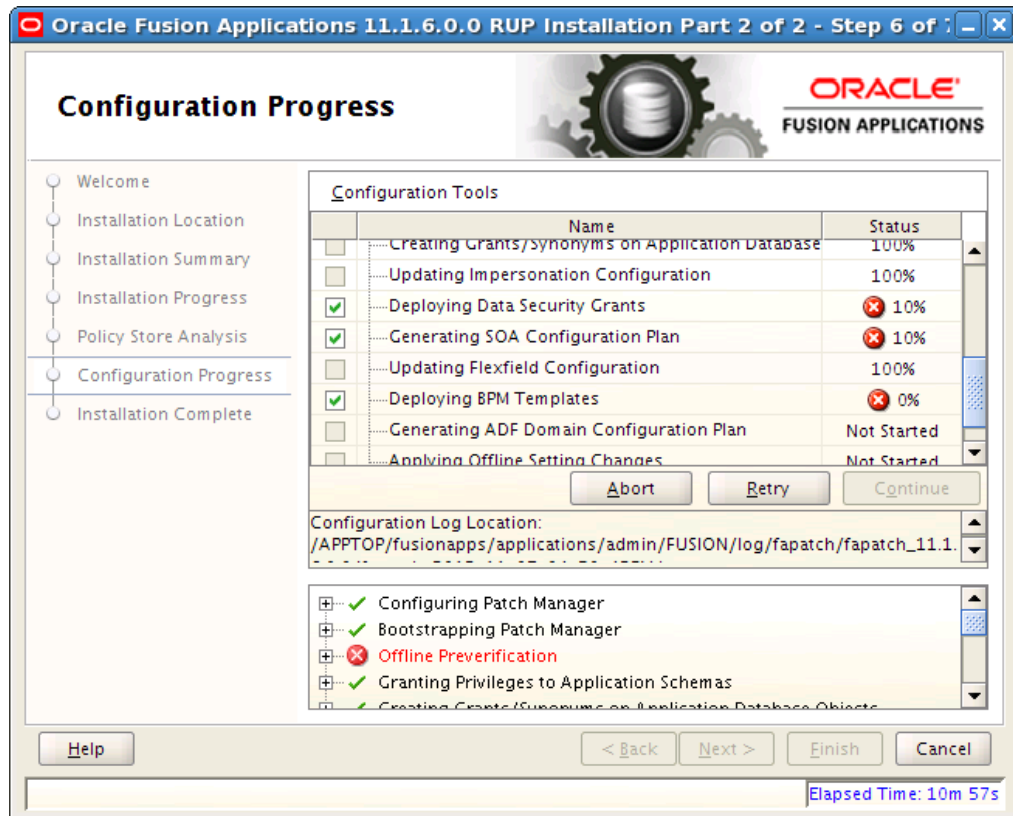
3. After you resolve the cause of the failure and click **Retry,** the three failed tasks run in parallel again.

### 6.7.1.3 The Next Button Is Not Enabled During Configuration Assistants

**Problem**

On the Configuration Progress page of the installer, the **Next** button is enabled only when all configuration assistants are successful.

If you see that all your configurations are complete, and the **Next** button is not enabled, you encountered a configuration failure and continued to the next configuration assistant.

**Solution**

In this case, you must retry the failed configuration assistants by following these steps:

1. On the Configuration Progress page of the installer, click **Cancel**.

2. Restart the installer. All failed configuration assistants or steps rerun upon restart. For more information, see Section 6.7.1.1, "Restart a Failed Installer Session".

As long as a configuration assistant is not successful, the **Next** button remains disabled. It may be necessary to repeat the cancel and retry procedure until all configuration assistants are successful.

### 6.7.1.4 The OPSS Security Store Goes Down While the Installer is Running

**Problem**

The OPSS Security Store goes down while the installer is running.

**Solution**

Configuration tasks that are related to the OPSS Security Store will fail if the store goes down. Perform the following steps to recover:

1. Abort the failed configuration task.

2. Select **Cancel** to end the installer session.

3. Start the OPSS Security Store. For more information, see Section E.7, "Starting and Stopping Oracle Internet Directory".

4. Start a new installer session. The installer resumes with the remaining tasks because you selected **Cancel**, which saves the session

### 6.7.1.5 Failure During Opening of Wallet Based Credential Store

**Problem**

The following error occurs during the configuration phase.

```
Reason:oracle.security.jps.service.credstore.CredStoreException: JPS-01050:
Opening of wallet based credential store failed.
Reason java.io.IO Exception: PKI-02002: Unable to open the wallet. Check password.
```

**Solution**

After you resolve the cause of the failure, or cancel the installation and then restart the installer. If the failure still occurs, refer to "Server with NFS-Mounted Domain Directory Fails to Start" in the *Oracle Fusion Middleware Application Security Guide* to further diagnose the failure.

## 6.7.2 General Troubleshooting During the Configuration Phase in Silent Mode

The installer can be restarted to rerun all failed configuration tasks as well as those tasks that were not started from the previous session. When a mandatory configuration task or step fails in silent mode, the installer exits. After you resolve the issue that caused the failure, restart the installer using the same command you used to start it. When the installer restarts, it restarts from the first failed task.

If any non-mandatory tasks fail in silent mode, the installer continues with the next configuration task and does not exit. You must review the logs to find any non-mandatory tasks that failed and then rerun the installer until all tasks complete successfully.

If you decide to run the installer in GUI mode, you must start it from the *REPOSITORY_LOCATION*/installers/farup/Disk1/ directory.

## 6.7.3 RUP Installer Fails

RUP Installer is one of the tasks performed by Upgrade Orchestrator. In the case of a failure, information in Section 6.1, "General Troubleshooting for an Upgrade Orchestrator Failure" applies. In addition to the Upgrade Report and log location, the RUP Installer Report location is also included as part of the notification that is sent. For more information, see Section 5.2, "Review the Post RUP Installer Report".

### 6.7.4  RUP Installer or InstallFaSaaSLcmTools Fails Due To Thread Calls

**Problem**

RUP Installer fails due to thread calls and reports errors similar to the following example:

```
"Thread-11" id=29 idx=0x98 tid=25751 prio=5 alive, native_blocked
    at java/io/UnixFileSystem.getBooleanAttributes0(Ljava/io/File;)I(Native
 Method)
    at java/io/UnixFileSystem.getBooleanAttributes(UnixFileSystem.java:228)
    at java/io/File.exists(File.java:733)
```

**Solution**

Restart Orchestrator to proceed with upgrade. If it fails again, contact Oracle Support.

### 6.7.5  RUP Installer or InstallFaSaaSLcmTools Fails With Internal Error

**Problem**

RUP Installer or `InstallFaSaaSLcmTools` fails with the following message:

```
Internal Error: File Copy failed. Aborting Install
```

**Solution**

Restart Orchestrator to proceed with upgrade. If it fails again, contact Oracle Support.

### 6.7.6  RUP Installer Part 1 Fails on Primordial Host

**Problem**

Because of intermittent issues, RUP Installer Part 1 fails on the primordial host due to the following error:

```
/exception in /u01/instance/lcm/log/11.1.7.0.0/RUP/fapatch_Applying_Middleware_
Patchsets_timestamp.log.

{{Internal Error: File Copy failed. Aborting Install

ERROR: Failed Job ID 12

ERROR: jobs failed during Applying Middleware Patchsets}}
{{ERROR: CFGEX-00090 : Applying Middleware Patchsets failed.Action : See log file
for details. java.lang.Exception: CFGEX-00090 : Applying Middleware _Patchsets
failed. at_ _oracle.as.install.fatechpatchconfig.MWPatchset.doExecute

(MWPatchset.java:53) a{}t_ oracle.as.install.engine.modules.configuration.client.

ConfigAction.execute(ConfigAction.java:375)}}
```

In addition to the preceding error, the following message is in Installer logs using the timestamp above under
`/u01/inventory/admin-apps.oracleoutsourcing.com/oraInventory/logs`:

```
OUI exception. oracle.sysman.oii.oiic.OiicInstallAPIException: OUI-10022:The
target area_
/u01/oim/oraInventory cannot be used because it is in an invalid state.
```

**Solution**

Resume Upgrade Orchestrator on the primordial nodes to proceed with the upgrade.

### 6.7.7 Installer Requirement Checks Fail

**Problem**

The installer fails with the following type of errors:

```
Starting Oracle Universal Installer...
Checking if CPU speed is above 300 MHz.
Checking Temp space: must be greater than 4096 MB. Actual 9177 MB Passed

Checking swap space: 3915 MB available, 4000 MB required. Failed <<<<
Some requirement checks failed. You must fulfill these requirements before
continuing with the installation,
```

**Solution**

Manually increase the requirement that failed, in this example, the swap space. Then resume orchestration.

### 6.7.8 Recovering From an Installer Session That Was Shut Down

**Problem**

An installer session was shut down during the upgrade.

**Solution**

If orchestration or tasks spawned by orchestration, such as RUP Installer, are killed in the middle of any process, the system may not be in a recoverable state and the state should be carefully reviewed by contacting Oracle Support before proceeding.

To recover from this situation, restore your backup of *APPLICATIONS_BASE* and start from the beginning of the upgrade.

### 6.7.9 Failure During Importing Oracle Data Integrator Repositories

**Problem**

RUP Installer Part 2 fails when the **Importing Oracle Data Integrator Repositories** configuration assistant is run in checkpointing mode and when the Offline Preverification step was already run in a previous session of the installer. An example of the exception message in the configuration assistant log follows:

```
odi.core.security.internal.ODIJpsHelper.createSubject Get exception. User:FUSION_
APPS_PROV_PATCH_APPID. Execption msg is:java.lang.NoClassDefFoundError:
javax/security/jacc/PolicyContext
```

**Solution**

Run the Offline Preverification step and resume Upgrade Orchestrator.

1. Back up the existing checkpoint file at /u01/inventory/*host_
   name*/oraInventory/checkpoint/farup/11.1.7.0.0/checkpoint.xml to a
   different location.

2. In the `checkpoint.xml` file, look for `<aggregate name="Offline Preverification" status="success"/>`, update the line to set the status to "fail" and save the file.

3. Resume Upgrade Orchestrator.

## 6.7.10 Deploying New Application Configuration Fails with a "NumberFormatException"

**Problem**

A `NumberFormatException` is reported when retrying "Deploying New application config" configuration assistant due to an incorrect value for `numCompletedDeployments` variable in the `checkpoint.xml` file.

**Solution**

To resolve this issue, convert the float value to an integer value for the "NumberOfSuccessfulArtifacts" attribute in the checkpoint file located at *central_inventory_location*/checkpoint/11.1.7.0.0/farup/checkpoint.xml.

The following example shows the value to be updated in bold:

```
<aggregate name="Deploying New Applications" status="fail">
      <property name="NumberOfSuccessfulArtifacts" value="2.0"/>
      ...
   </aggregate>
```

The following example shows the updated value in bold.

```
<aggregate name="Deploying New Applications" status="fail">
      <property name="NumberOfSuccessfulArtifacts" value="2"/>
      ...
   </aggregate>
```

## 6.7.11 Failure During the Extending Certificate Validity Phase

**Problem**

RUP Installer fails during the Extending Certificate Validity phase when upgrading from Release 5 to Release 7 in a chained upgrade on an FSCMH environment. The Release 6 upgrade first installer fails at Extending Certificate Validity because DSS has an untrusted `.jks` file. RUP Installer failed to execute the command:

```
 /u01/APPLTOP/fusionapps/jdk6/bin/keytool -delete -alias *ca_fusion
-keystore fusion_trust.jks with keytool error: java.lang.Exception: Alias
*ca_fusion does not exist.
```

**Solution**

Rename the file to a format that is different from `_fusion_identity.jks` and resume Upgrade Orchestrator.

## 6.7.12 Failure During Importing Group Space Templates

**Problem**

The import of Group Space Templates fails with the following error:

```
Another application named "webcenter" exists. Specify the Server on which your
application is deployed. Use: server= "YourServerName ".
```

**Solution**

There are multiple applications with the same name in the domain in which you are trying to register your application. This usually happens in a cluster environment, where the same application is deployed to multiple managed servers. If this is the case, specify the name of the server in which you are trying to register this application. For example, run the `registerWSRPProducer` WLST command with the server argument:

```
registerWSRPProducer(appName='myApp',
name='MyWSRPSamples',url='http://host:port/application_name/portlets/wsrp2?WSDL',
server=server_name)
```

**Related Links**

The following document provides additional information related to the subject discussed in this section:

- For command syntax and examples, see "registerWSRPProducer" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

## 6.7.13 Configuration Assistant Fails With "Could not create credential store instance"

**Problem**

A configuration assistant fails with the following error:

```
JPS-01055: Could not create credential store instance.
Reason: oracle.security.jps.JpsException: JPS-00071: Ldap bootstrap credential
retrieval failed.
Reason:oracle.security.jps.service.credstore.CredStoreException:
JPS-01050: Opening of wallet based credential store failed.
Reason java.io.IO Exception:PKI-02002: Unable to open the wallet. Check password.
```

**Solution**

Restart Upgrade Orchestrator.

## 6.7.14 Failure During Starting All Servers or Restarting SOA Servers

**Problem**

During the upgrade, RUP Installer reports the following errors while running the `StartAllServers` task, or when starting SOA servers:

```
[oracle.apps.startstop.execution.executor.StartStopTaskHelper: createMBeanSO.2053]
[tid:621] SSUTIL011
java.lang.IllegalStateException: Cannot register two instances of
WorkContextAccessController
at
weblogic.workarea.spi.WorkContextAccessController.<init>(WorkContextAccessControll
er.java:24)
at
weblogic.workarea.spi.WorkContextAccessController$1.<init>(WorkContextAccessContro
ller.java:65)
at
weblogic.workarea.spi.WorkContextAccessController.getAccessController(WorkContextA
ccessController.java:65)
```

**Solution**

Resume Upgrade Orchestrator to retry the failed step.

## 6.8 Troubleshooting Failures During the Installation Phase

Perform the following steps when an error occurs during the RUP Installer or Language Pack Installer installation phase:

1. Click **Cancel** to exit out of the installer.

2. Review the log files to determine the cause of the failure. The log files reside in `oracle_inventory/logs/installtimestamp.log`.

3. Resolve the cause of the failure.

4. Start the installer using the same command syntax that you used for the previous incomplete installation. After canceling the previous installation and starting again, you must choose to continue with the previously failed installation by clicking **Yes** on the Checkpoint Dialog. If the error is not recoverable, you can restore and restart from backup.

5. If you choose to continue with the failed installation, the installer opens at the screen where it was canceled. When canceled during the copy action, it relaunches in the Installation Summary screen. Click **Next** to navigate through the Installation Summary screen. When the Installation Progress screen displays, click **Install** to start the installation again.

Troubleshooting steps are described for the following specific failures that may occur during the installation phase:

- CFGLOG-00056: Exception caught while getting node-manager homes
- Invalid Oracle Home
- Error in Writing to File, Text File Busy
- Inventory Pointer File is Empty

### 6.8.1 CFGLOG-00056: Exception caught while getting node-manager homes

**Problem**

Within a few seconds of starting the installer, you receive the following messages:

In the log file:

```
SEVERE: CFGLOG-00056 : Exception caught while getting node-manager homes
```

In the user interface:

```
CFGLOG-00052 : Error occurred while moving instance specific files
```

**Solution**

This failure is the result of having an incompatible version of OPatch in FA_ORACLE_HOME. To resolve the issue, download and apply patch 14044793, which contains the compatible version of OPatch.

### 6.8.2 Invalid Oracle Home

**Problem**

In the Installation Location page, you receive a message about entering an invalid Oracle home, even though the location displayed on the page is correct. The installer reads `/etc/oraInst.loc` to determine the location of the central inventory.

**Solution**

To resolve this problem:

- Ensure that the `/etc/oraInst.loc` file on the machine where you are running the installer is pointing to the correct central inventory location.

- Ensure that the *FA_ORACLE_HOME* matches the values provided during provisioning. If a `/net/location` was provided as the Oracle home location during provisioning, the same `/net/location` that corresponds to *FA_ORACLE_HOME* should be provided during the installation. You can find this location by following these steps:

  - Open /etc/oraInst.loc and find the path to oraInventory, which is the central inventory, for example, `server01/appmgr/APPTOP/oraInventory`.

  - Change directory to the ContentsXML directory under the central inventory, for example, `server01/appmgr/APPTOP/oraInventory/ContentsXML`.

  - Open the `inventory.xml` file to find the correct directory path to *FA_ORACLE_HOME*.

## 6.8.3 Error in Writing to File, Text File Busy

**Problem**

During the installation phase of RUP Installer, you receive the following message on a UNIX platform.

```
Error in writing to file
'/server01/APPLICATIONS_BASE/fusionapps/applications/lcm/ad/bin/adctrl'
(Text file busy)
```

**Solution**

To resolve this issue, perform the following steps.

1. Run the `lsof` command using the full directory path of the file that is busy.

   `/usr/bin/lsof full_path_to_file`

2. You should receive a list of process ids that are using the file. Kill each process using the appropriate command for your operating system.

3. After all processes are no longer running, resume Upgrade Orchestrator.

## 6.8.4 Inventory Pointer File is Empty

**Problem**

After running the installer, the contents of `oraInst.loc` were removed.

**Solution**

The installer always tries to copy the inventory pointer file specified by the `-invPtrLoc` option to the Oracle home on which the release is to be installed. If you specify an incorrect path for the `-invPtrLoc` file, the inventory pointer file could result in being an empty file. Review the following possible solutions for this issue:

- For best results, if you are using the `-invPtrLoc` option, use it with this value: *FA_ORACLE_HOME*/oraInst.loc. This avoids a situation where you may inadvertently exclude part of the directory path to the file, as in the case of using a mapped

drive. For example, if Oracle home is registered in inventory with a /net path, such as /net/home/oraInst.loc, and you provide /home/oraInst.loc to the invPtrLoc option, the installer interprets the two paths as different. The end result is an empty inventory pointer file.

- If *FA_ORACLE_HOME* is registered in central inventory with a /net path, then you must include /net when specifying the location of the inventory pointer file with the -invPtrLoc option, for example, -invPtrLoc /net/*directory_path*/oraInst.loc.

- Restore from a backup copy of your oraInst.loc file in case the original file is damaged. You can find this in /etc/oraInst.loc.

- You can recover from this error by creating a new oraInst.loc. See the "Creating the oraInst.loc File" section in the relevant Oracle Database installation guide, for example, *Oracle Database Installation Guide, 11g Release 2 (11.2) for Linux*.

  Then resume Upgrade Orchestrator.

## 6.9 Troubleshooting Node Manager and OPMN Failures

This section provides information about the following failures:

- Verifying Node Manager and OPMN Status Fails Due to Bad Certificate Issue
- Exception During Stopping OPMN Processes
- Troubleshooting Failure During Verifying Node Manager and OPMN Status
- Node Manager Did Not Start Between First and Second Installer

### 6.9.1 Verifying Node Manager and OPMN Status Fails Due to Bad Certificate Issue

**Problem**

Verifying Node Manager and OPMS Status fails with the following error:

```
WLSTException: Error occured while performing nmConnect :
Cannot connect to Node Manager. :
[Security:090542]Certificate chain received from <hostname> - <host IP address>
was not trusted causing SSL handshake failure.
```

**Solution**

The issue can occur when the host associated with a node manager is explicitly bounced in the middle of the upgrade, and if Upgrade Orchestrator expects the node manager to be in a shutdown state at that time. Node manager on the host may be configured to automatically start up as part of the system boot process and could cause various issues depending on which upgrade step was being performed when the host was restarted. To resolve this issue, stop and restart node manager on the host where the issue was reported.

### 6.9.2 Exception During Stopping OPMN Processes

**Problem**

Upgrade Orchestrator fails to stop OPMN processes with and error similar to either of the following errors:

- ```
  Exception: OPMN could not be stopped. Script will exit. Please stop
  OPMN manually before re-running the script.
  ```

■  /APPLICATIONS_BASE/webtier_mwhome/oracle_
   common/jdk/jre/lib/fonts/ALBANWTJ.ttf - No such file exists.

**Solution**

This issue can occur due to an incompatible version of JDK being used during the process. To resolve the issue, perform the following steps.

1.  cd */APPLICATIONS_BASE/*webtier_mwhome/webtier

    mv jdk_backup_existing_version jdk

2.  cd */APPLICATIONS_BASE/*webtier_mwhome/oracle_common

    rm -rf jdk

    cp -Rp jdk_bkp_130320_1250 jdk

3.  Resume Upgrade Orchestrator.

## 6.9.3 Troubleshooting Failure During Verifying Node Manager and OPMN Status

**Problem**

The **Verifying Node Manager and OPMN Status** configuration assistant fails.

**Solution**

Do not exit out of Upgrade Orchestrator in response to this configuration assistant failure. Perform the following steps to recover:

1.  Review the node manager log files to determine the cause of the failure:

    *APPLICATIONS_CONFIG*/nodemanager/host_name/

    Note that the *APPLICATIONS_CONFIG* value can be obtained from the *APPLICATIONS_BASE*/fusionapps/faInst.loc file.

2.  After you resolve the issue that caused the failure, start the Node Manager on all hosts that are part of the Oracle Fusion Applications provisioned system. For more information, see "Task 3: Start Node Manager" in the *Oracle Fusion Applications Administrator's Guide*.

3.  Restart the OPMN server for BI, GOP (if GOP is installed), and Web Tier. If you run the Web Tier (OHS) installed with the Oracle Fusion Applications middle tier, you can start it using the following steps. If you run the Web Tier on a separate machine, you may be able to run the steps below on the other machine. In either case, ensure that Web Tier (OHS) is up at this point.

    Example for BI: (note the usage of start instead of startall)

    ```
    cd APPLICATIONS_CONFIG/BIInstance/bin
    ./opmnctl start
    ```

    Example for GOP: (note the usage of start instead of startall) Note that the OPMN server for GOP should be started from the machine that hosts the Supply Chain Management Administration Server domain. Start the OPMN server for GOP only if you have GOP installed.

    ```
    cd APPLICATIONS_CONFIG/gop_1/bin
    ./opmnctl start
    ```

    Example for Web Tier: (note the usage of start instead of startall)

    ```
    cd APPLICATIONS_CONFIG/CommonDomain_webtier/bin
    ```

```
./opmnctl start
```

For more information about the location of *APPLICATIONS_BASE* and *APPLICATIONS_CONFIG*, see Section 2.1, "Before You Begin".

The BI and Web Tier processes managed by OPMN are started by RUP Installer in the **Starting All Servers** configuration assistant. The GOP processes managed by OPMN must be started using Fusion Applications Control, as described in Section 4.4.9, "Start External Servers", after RUP Installer completes.

4.  Fix any other environment issues before resuming the upgrade. If RUP Installer exits for any reason, make sure that all node managers and OPMN processes are running. Contact Oracle Support Services to proceed out of this step if you have unresolved environment issues.

5.  After you start the services, resume orchestration to proceed to the **Starting All Servers** configuration assistant. If the starting of servers times out, see Section 6.15, "Troubleshooting Server Start and Stop Failures".

---

**Note:** If GOP is not installed, the user interface reports "Success" for GOP OPMN status, but the log file reports: `GOP is not provisioned. Skipping check for OPMN status.`

---

### 6.9.4 Node Manager Did Not Start Between First and Second Installer

This section describes two scenarios that can prevent the node manager from starting between the first and second installer.

**Problem**

The node manager was manually started before or during the **Extending Certification Validity** configuration assistant. The node manager caches the previous keystore certificates so the updated certificates are not validated and the node manager fails to start.

**Solution**

Check the node manager logs to determine if it is running and when it was last started. If the time stamp is earlier than the **Extending Certification Validity** configuration assistant execution time stamp, you must restart the node manager so that it reads the updated keystore certificates.

1.  To find out if the node manager is running for a specific host, connect to the host and run the following command. If any results are returned, the node manager is running.

```
ps -ef | grep nodemanager
```

2.  If the node manager is running, find the time of the last entry of `<Secure socket listener started on port nnnn>` in the following directory.

```
APPLICATIONS_CONFIG/nodemanager/logical_host_name/nodemanager
```

3.  To check the time stamp for the **Extending Certification Validity** configuration assistant, find the `fapatch_Extending_Certificate_Validity_XXXX` file in one of the following directories.

```
APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/RUP/configlogs
```

```
APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/RUP/ARCHIVE/timestamp/configlogs
```

The last time stamp entry is the execution time stamp.

**Problem**

The administration servers in one or more domains are running before the **Extending Certification Validity** configuration assistant runs. This prevents validation of the updated keystore certificates and fails to provide the correct status to orchestration.

**Solution**

Perform the following steps

1.  Verify whether the administration server of the domain is running by launching the administration console of the domain. If the console comes up, then the administration server is running.

2.  Verify the last time the administration server was started. Go to the *APPLICATIONS_ CONFIG*/domains/*logical_host_name*/domain_name/servers/AdminServer/logs directory. Using the command, `ls -lrt`, find the most recent the `AdminServer.log` file. In this file, find the time of the last entry that contains text similar to the following example:

```
<Channel "Default" is now listening on machine_ip:port for
protocols iiop, t3, ldap, snmp, http.>
```

## 6.10 Troubleshooting RUP Lite for OHS

The following RUP Lite for OHS troubleshooting issues are described:

■   RUP Lite for OHS Fails With Missing JDK exception

■   RUP Lite for OHS Fails With ReassociateCommonDomain Plug-in

■   RUP Lite for OHS Fails With Security Mode Errors

■   UpgradeOHSBinary Task Fails with Missing File Error

### 6.10.1 RUP Lite for OHS Fails With Missing JDK exception

**Problem**

RUP Lite for OHS fails during the `ohs.plugin.UpgradeWebtier` step due to missing the `jdk` directory.

**Solution**

Verify if there is a `jdk_backup_existing_version` directory under *WT_ORACLE_HOME*. If this directory exists, rename it to `jdk` and resume Upgrade Orchestrator.

Also, if the missing `jdk` directory is from *WT_MW_HOME*/oracle_common, check to see if there is a `jdk_backup_existing_version` directory under this directory. If so, rename it to `jdk` and resume Upgrade Orchestrator.

### 6.10.2 RUP Lite for OHS Fails With ReassociateCommonDomain Plug-in

**Problem**

RUP Lite for OHS fails with the following error:

```
Failed execution of plugin: ohs.plugin.ReassociateCommonDomain
```

**Solution**

Update the *server_name*/instance/CommonDomain_webtier_
local/config/OPMN/opmn/instance.properties file to set the registered property to
true. Then check the Administration Server on either the Common Domain or the
OSN Domain to ensure it is running. If not, bounce the server and retry RUP Lite for
OHS by resuming orchestration.

## 6.10.3 RUP Lite for OHS Fails With Security Mode Errors

**Problem**

RUP Lite for OHS reports a server side error occurs with an error message such as:

```
Server instance is not running for the security mode specified: "simple".
Try again using a different security mode. The remote registration process
did not succeed! Please find the specific error message below.
```

**Solution**

Perform the following steps.

1. Log in to the OAM administration console.

2. From the System Configuration tab, click **Server_Instances**, and double click the
   OAM server instance, such as, oam_server1.

3. Select "simple" from the Mode field in the right panel.

4. Click **Apply** to submit the changes.

5. Restart the OAM Server.

6. Restart all OHS servers in the environment.

7. Resume Upgrade Orchestrator.

> **Note:** Check the Oracle Fusion Applications OHS to ensure that SSO
> still works after the change. If it does not, you must upgrade Webgate
> manually for the Oracle Fusion Applications OHS.

## 6.10.4 UpgradeOHSBinary Task Fails with Missing File Error

**Problem**

During the Release 5 to Release 6 upgrade, the UpgradeOHSBinary task fails with an
error message similar to the following:

```
File/dir required for ruplite execution is missing: /u01/webgate/host_
name/webgate_installer_REL6/templates/webtier
```

**Solution**

Perform the following steps to resolve the issue.

1. Create the missing directory:

   ```
   mkdir /u01/webgate/hostname/webgate_installer_REL6/templates/webtier
   ```

2. Copy all of the files from
   /u01/APPLTOP/fusionapps/applications/admin/OHS/patched_

moduleconf/11.1.6.0.0 on the primordial host to the directory you created in the previous step.

3. Resume Upgrade Orchestrator.

# 6.11 Troubleshooting IDM Upgrade Failures

This section provides information about the following issues:

- Communication Exception on Primordial Console While Waiting for IDMOHS
- WLS Exception - ESS Server Does Not Respond During Start all Servers
- OAM Configuration Step Fails Due to Special Characters in Password
- Location of GRC Policies in the OAM Applications Domain

## 6.11.1 Communication Exception on Primordial Console While Waiting for IDMOHS

**Problem**

While PRIMORDIAL is waiting for IDMOHS:IDMUpgradeDone, there are communication exceptions on the PRIMORDIAL console.

**Solution**

These errors can be ignored and Upgrade Orchestrator can be resumed.

## 6.11.2 WLS Exception - ESS Server Does Not Respond During Start all Servers

**Problem**

The **Starting All Servers** configuration assistant in RUP Installer fails to start ess_server1 and reports the following error in the ess_server1.log:

```
weblogic.rmi.extensions.DisconnectMonitorUnavailableException: Could not
register a DisconnectListener
```

**Solution**

Perform the following steps to resolve this issue:

1. Open the Oracle Enterprise Manager console for the domain.

2. Navigate to following location:

    - From the console, expand the WebLogic Domain

    - Go to ESSCluster, then ess_server1

    - Right click and open System MBean browser

    - Go to ess_server1, ServerStart, select ess_server1, and click Arguments

3. Verify if -Doracle.ess.initialProcessorState=stopped is present. If it is, remove -Doracle.ess.initialProcessorState=stopped and click Apply. If it is not present, there is no action to take.

4. Restart ess_server1.

### 6.11.3 OAM Configuration Step Fails Due to Special Characters in Password

If the OAM administrator password contains special characters, such as '#' or '&', the OAM Configuration step will fail. To work around this issue, you can manually validate that the OAM Administration Server host/port and surname/password are correct. After you manually validate this information, you can proceed with the upgrade by resuming orchestration.

Perform the following steps to validate.

1. Get the OAM administrator user name and password from the credential store.

2. Run *APPLICATIONS_BASE*/fusionapps/oracle_common/common/bin/wlst.sh.

3. Run the following commands to connect to the Common Domain Administration Server and get the OAM administrator surname and password:

```
connect()
listCred(map='oracle.patching', key='FUSION_APPS_PATCH_OAM_ADMIN-KEY')
```

4. Get the OAM Administration Server host and port from the following properties in *APPLICATIONS_CONFIG*/fapatch/FUSION_prov.properties:

   - OAM_ADMIN_SERVER_HOST

   - OAM_ADMIN_SERVER_PORT

5. Use oamcfgtool.jar to confirm whether the OAM server can be invoked using the values found in the previous steps.

```
cd APPLICATIONS_BASE/fusionapps/oracle_common/modules/oracle.oamprovider_11.1.1

java -jar oamcfgtool.jar app_domain=crm web_domain=OraFusionApp
uris_file=APPLICATIONS_BASE/fusionapps/applications/crm/security/oam.conf
oam_aaa_mode=open_or_simple app_agent_password=password_for_
map="oracle.patching"
key="FUSION_APPS_PATCH_OAM_RWG-KEY"_in_credential_store
primary_oam_servers=oam_server1 oam_admin_server=http://OAM_admin_server_
host:port
oam_admin_username=username_for_FUSION_APPS_PATCH_OAM_ADMIN-KEY
oam_admin_password=password_for_FUSION_APPS_PATCH_OAM_ADMIN-KEY
oam_version=11 default_authn_scheme=FAAuthScheme
```

6. If the previous command is successful, the validation is successful and you can resume Upgrade Orchestrator.

### 6.11.4 Location of GRC Policies in the OAM Applications Domain

The location of your Governance, Risk, and Compliance (GRC) policies varies, depending on your upgrade path to Release 7. GRC polices are located in the *grc* OAM application domain if your Oracle Fusion Applications environment was originally provisioned with either version 11.1.1.5 or 11.1.2, then upgraded to version 11.1.3 and beyond. If your environment was originally provisioned with version 11.1.3 and upgraded to version 11.1.4 and beyond, your GRC policies are located in the *fs* OAM application domain.

## 6.12 Troubleshooting Applying Middleware Patches

This section provides the following troubleshooting information related to the **Applying Pre-PSA Middleware Patches** or **Applying Post-PSA Middleware Patches** configuration assistants:

- Log Files for Applying Middleware Patches
- Applying Post-PSA Middleware Patches Hangs
- Error Applying Database Client Patches
- ORA-01658: unable to create INITIAL extent for segment in tablespace
- Troubleshooting Upgrading Middleware Schema
- Troubleshooting Applying Downloaded Patches

## 6.12.1 Log Files for Applying Middleware Patches

### Problem

An error occurred during the **Applying Pre-PSA Middleware Patches** or **Applying Post-PSA Middleware Patches** configuration assistant.

### Solution

Review the log file in the relevant location to find the cause of the error:

*APPLICATIONS_ CONFIG*/lcm/logs/11.1.7.0.0/RUP/ApplyPrePSAMiddlewarePatches*timestamp*.log

*APPLICATIONS_ CONFIG*/lcm/logs/11.1.7.0.0/RUP/ApplyPostPSAMiddlewarePatches*timestamp*.log

For specific OPatch failures, go to each of the individual Oracle home directories to find the details of the OPatch errors. For example, for a SOA failure, go to *APPLICATIONS_BASE*/fusionapps/soa/cfgtoollogs/opatch.

## 6.12.2 Applying Post-PSA Middleware Patches Hangs

### Problem

The **Applying Post-PSA Middleware Patches** configuration assistant hangs.

### Solution

This problem is most likely due to adpatch hanging as the result of the java worker not getting the database connection. You can resolve this issue by following the steps in Section 6.13, "Troubleshooting Loading Database Components". Run the commands from *ATGPF_ORACLE_HOME* instead of *FA_ORACLE_HOME*.

## 6.12.3 Error Applying Database Client Patches

### Problem

The following error occurs:

```
OPatch cannot continue because it can't load library from the directory "<dbclient
Oracle Home>/oui/lib/linux64"
```

### Solution

This error may occur if the OUI version in the database client Oracle home is 11.2 while the OUI version in Oracle Fusion Applications Oracle home (FA_ORACLE_ HOME) is 11.1.

Perform the following steps to resolve this issue:

1. Go to the DB Client home.

2. Set the ORACLE_HOME environment variable to point to the database client Oracle home.

3. Apply the database client patches using the following command:

   ```
   $ORACLE_HOME/OPatch/opatch apply patch_location
   ```

4. Because the patches have now been manually applied, perform the following steps to continue with the upgrade:

   a. Go to the *FA_ORACLE_HOME*/fusionapps/applications/lcm/tp/config/RUP/FMW directory.

   b. Open the pre-psa-jobs.xml file for editing.

   c. Comment out the job with the name dbclient An example of this job follows.

   ```
   <!-- <job>
       <id>10</id>
       <target>FAMW</target>
       <component>
              <name>dbclient</name>
              <version>11.1.1.5</version>
       <component>
       <utility_name>opatch</utility_name>
       <patch_number>NA</patch_number>
       <command>%opatch% napply -silent -skip_duplicate -skip_subset
   -oh %dbclient_home% -phBaseDir %dbclient_patch% -jre %jre_loc% -invPtrLoc
   %oraInstLocFile%</command>
        <patch_location>NA</patch_location
   </job>
   ```

## 6.12.4 ORA-01658: unable to create INITIAL extent for segment in tablespace

**Problem**

The following error is reported:

```
ORA-01658: unable to create INITIAL extent for segment in tablespace FUSION_TS_
SEED.
```

**Solution**

The standard output from the ORA-1658 error follows:

```
ORA-01658: unable to create INITIAL extent for segment in tablespace string
    Cause: Failed to find sufficient contiguous space to allocate
    INITIAL extent for segment being created.
    Action: Use ALTER TABLESPACE ADD DATAFILE to add additional space to
    the tablespace or retry with a smaller value for INITIAL
```

For more information, refer to Oracle Database documentation.

## 6.12.5 Troubleshooting Upgrading Middleware Schema

**Problem**

An error occurred during the **Upgrading Middleware Schema** configuration assistant.

**Solution**

Review the log file in this location to find the cause of the error:

```
fusionapps/oracle_common/upgrade/logs/psatimestamp.log
```

**Problem**

The **Upgrading Middleware Schema** configuration assistant fails because *JAVA_HOME* cannot be found.

**Solution**

Set the *JAVA_HOME* and then manually run the upgrade for the failed schema, as shown in the following example:

```
export JAVA_HOME=/u01/APPLTOP/fusionapps/jdk6
/u01/APPLTOP/fusionapps/oracle_common/bin/psa -response
/u01/APPLTOP/fusionapps/applications/admin/FUSION/oui_resp/psa_response_crm.txt
```

### 6.12.6 Troubleshooting Applying Downloaded Patches

**Problem**

The **Applying Downloaded Patches** configuration assistant failed with the following error:

```
Stack Description: java.lang.RuntimeException:
PatchObject constructor: Input file
"/net/server01/Downloaded_Patches/atgpf/patch/1234567/etc
/config/inventory" does not exist.
```

**Solution**

This type of error occurs when you do not download the patches to the appropriate directory. To resolve this issue, copy the patches to the correct directory and resume Upgrade Orchestrator.

## 6.13 Troubleshooting Loading Database Components

This section contains information about troubleshooting issues that may occur during the **Loading Database Components** configuration assistant. Depending on the type of failure, you may need to review one or more of the log files in the following locations:

- *APPLICATIONS_CONFIG*/lcm/logs/11.1.7.0.0/RUP/PatchManager_DBPatch/

  - FAPatchManager_apply_*timestamp*.log

  - adpatch_apply_*timestamp*.log

  - adpatch_apply_*timestamp*_worker*num*.log

- *ATGPF_HOME*/admin/FUSION/log

The following troubleshooting issues are described in this section:

- Error While Loading Database Components Using Orchestration

- Error While Loading Database Components Using RUP Installer in GUI Mode

- Database Failure While Loading Database Components

- Failure During AutoPatch Validation

- [Flexfield Seed Data Upload Fails](#)
- [Failure During Granting Privileges](#)
- [Loading Database Components Configuration Assistant Fails When JDBC URL Is Null](#)
- [Orchestration Fails on Primordial Host Reporting Active FAPatchMgr Sessions](#)

### 6.13.1 Error While Loading Database Components Using Orchestration

**Problem**

You receive an email notification stating that one or more database workers failed during the **Loading Database Components** configuration assistant.

**Solution**

You receive this email notification only when the upgrade cannot progress any further and requires user intervention. In this scenario, all the workers are in a FAILED or IDLE status. The Configuration Assistant remains in a RUNNING status until all tasks in **Loading Database Components** have run. To resolve this issue, you must start AD Controller to manage the failed workers. For additional information, see "Troubleshooting Patching Sessions for Database Content" in the *Oracle Fusion Applications Patching Guide*. After you resolve the issue that caused the workers to fail, and restart the workers, Upgrade Orchestrator continues processing. No further intervention is required.

Note that the messages are displayed on the console for database component failures if you run orchestration with the -DlogLevel option set to FINEST.

There might be corner cases when you might receive an alert email indicating failed workers although the workers are still running. In such cases, you can ignore the email alert after ensuring the workers are running with no failures.

### 6.13.2 Error While Loading Database Components Using RUP Installer in GUI Mode

**Problem**

RUP Installer reports that one or more database workers failed during the **Loading Database Components** configuration assistant.

**Solution**

You must start AD Controller to manage the failed workers. After you resolve the issue that caused the workers to fail and you restart the failed worker, click **OK** in the dialog box and RUP Installer continues processing. For additional information, see "Troubleshooting Patching Sessions for Database Content" in the *Oracle Fusion Applications Patching Guide*.

### 6.13.3 Database Failure While Loading Database Components

**Problem**

Your database goes down while RUP Installer is running the **Loading Database Components** configuration assistant. If you simply bring the database up and then resume orchestration, you may encounter the following error:

```
Failed to connect to the database as fusion with error:
No more data to read from socket
```

**Solution**

Perform the following steps to recover from this error:

1. Force the database patching session to fail.

   ```
   (UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh forcefail
   (Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd forcefail
   ```

2. Start AD Controller.

   ```
   (UNIX) FA_ORACLE_HOME/lcm/ad/bin/adctrl.sh
   (Windows) FA_ORACLE_HOME\lcm\ad\bin\adctrl.cmd
   ```

   For more information, see "Starting AD Controller" in the *Oracle Fusion Applications Patching Guide*.

3. Follow this sequence of steps in AD Controller to manage the workers:

   a. Select **Tell manager that a worker failed its job** and enter **All** for all workers.

   b. Select **Tell worker to quit** and enter **All** for all workers. Note that this does not kill the workers. It sends a command to the worker to shutdown after it completes the current task.

   c. Wait for all workers to complete their tasks and shut down normally.

   d. If there are still some worker processes that do not shut down, kill those processes manually by selecting **Tell manager that a worker failed its job**. Then select **Tell manager that a worker acknowledges quit** and enter **All** for all workers.

   e. From your operating system, check for processes that are running `fapmgr`, `javaworker`, `adpatch`, `adadmin`, `sqlplus`, and `adworker`. If any exist, terminate them from your operating system.

   f. Select **Tell worker to restart a failed job** and enter **All** for all workers.

4. Resume Upgrade Orchestrator.

### 6.13.4 Failure During AutoPatch Validation

**Problem**

AutoPatch validation fails with the following message:

```
An active adpatch or adadmin session was found. Complete or terminate the
active session to allow fapmgr to proceed.
```

**Solution**

Perform the following steps to resolve this error:

1. Run the `fapmgr forcefail` command to update the patching tables.

   ```
   (UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh forcefail [-logfile log file name]
   [-loglevel level]

   (Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd forcefail [-logfile log file
   name] [-loglevel level]
   ```

2. Run the `fapmgr abort` command from *FA_ORACLE_HOME* to find out if an Oracle Fusion Applications Patch Manager session must be cleaned up.

   ```
   (UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh abort [-logfile log file name]
   ```

```
                     [-logLevel level]

                     (Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd abort [-logfile log file name]
                     [-logLevel level]
```

If this command finds no failed session, proceed to Step 3.

3. Run the following commands from *ATGPF_ORACLE_HOME* to abandon any Applications Core patching sessions or AD Administration sessions that may be running:

```
(UNIX) ATGPF_ORACLE_HOME/lcm/ad/bin/adpatch.sh abandon=y interactive=n
defaultsfile=APPLICATIONS_CONFIG/atgpf/admin/defaults.txt

(UNIX) ATGPF_ORACLE_HOME/lcm/ad/bin/adadmin.sh abandon=y interactive=n
defaultsfile=APPLICATIONS_CONFIG/atgpf/admin/defaults.txt

(Windows) ATGPF_ORACLE_HOME\lcm\ad\bin\adpatch.exe abandon=y interactive=n
defaultsfile=APPLICATIONS_CONFIG\atgpf\admin\defaults.txt

(Windows) ATGPF_ORACLE_HOME\lcm\ad\bin\adadmin.cmd abandon=y interactive=n
defaultsfile=APPLICATIONS_CONFIG\atgpf\admin\defaults.txt
```

## 6.13.5 Flexfield Seed Data Upload Fails

### Problem

When multiple seed data files are uploaded for the same flexfield but for different flexfield contexts, the upload tasks can fail due to locking issues. The failed tasks appear in the log file as the following error:

```
Loading failed with a JboException: JBO-25014: Another user has changed the
row with primary keyoracle.jbo.Key ...
```

### Solution

AutoPatch defers any failed tasks to the end of the phase and reattempts the failed tasks only after attempting all tasks in the phase at least once. Usually the flexfield seed data tasks that failed due to the locking issue succeed on subsequent attempts. You can ignore these errors if the flexfield seed data task succeeds on the retry. If the task remains in a failed state, you must use the AD Controller utility to retry the failed task.

For more information, see "Restarting a Failed Worker" in the *Oracle Fusion Applications Patching Guide*.

## 6.13.6 Failure During Granting Privileges

### Problem

A failure occurred during either the **Grant Privileges to Application Schemas** or the **Creating Grants/Synonyms on Application Database Objects** configuration assistant.

### Solution

You can find the cause of the failure by running the script manually as the SYSDBA user, using SQL*Plus or SQL*Developer. After you resolve the issue, resume orchestration.

## 6.13.7 Loading Database Components Configuration Assistant Fails When JDBC URL Is Null

**Problem**

The **Loading Database Components** configuration assistant fails with the following exception in the `FAPManager` log file.

```
Exception
[2013-11-20T06:01:53.280+00:00] [] [ERROR] [] [] [tid: 34]
[ecid:0000K9o6OHX6qI25Rrt1id1IZ4Pl00000d,0] java.lang.NullPointerException: Schema
@ name/password/
jdbc url cannot be null[[
at
oracle.apps.ad.common.db.ADDatabaseConnection.
createConnection(ADDatabaseConnection.java:529)
at
oracle.apps.ad.common.db.ADDatabaseConnection.
getConnectionWithCluster(ADDatabaseConnection.java:444)
at
oracle.apps.ad.common.db.ADDatabaseConnection.
getConnectionWithCluster(ADDatabaseConnection.java:446)
at
oracle.apps.ad.common.db.ADDatabaseConnection.
getConnectionWithCluster(ADDatabaseConnection.java:446)
......................................................
[2013-11-20T06:01:59.568+00:00] [apps] [ERROR] []
[oracle.apps.ad.rupconfig.Loading_Database_Components]
[tid: 34] [ecid:0000K9o6OHX6qI25Rrt1id1IZ4Pl00000d,0]
[[java.lang.StackOverflowError]]
```

**Solution**

Run the following command:

*FA_ORACLE_HOME/*lcm/ad/bin/fapmgr.sh forcefail

Resume Upgrade Orchestrator.

## 6.13.8 Orchestration Fails on Primordial Host Reporting Active FAPatchMgr Sessions

**Problem**

In a scenario where `fapmgr` applies patches using the multi-apply feature, and any patch validation fails, the status is set to 'SUCCESS'. This new status is treated as an active session by Health Checker and it fails, causing an orchestration failure with the error message as shown in the following example:

```
[ERROR]: Plugin 'PatchSessionsAndProcessesCheck': HC-PATCHSP-00004 : Check

#1: Found active FAPMgr sessions. Review log files for details on which Sessions
exist. (Pre-Upgrade Checks)
```

**Solution**

Run the following SQL*Plus command in the fusion schema:

```
update AD_PATCH_UTIL_SESSIONS set status='COMPLETED_WITH_WARNINGS' where
status='SUCCESS';
```

Resume orchestration.

## 6.14 Troubleshooting Deployment of Applications Policies

This section contains information about the following troubleshooting issues that may occur during the **Deploying Application Policies** configuration assistant:

- Log Files for Deploying Application Policies
- Failure During Analysis of Applications Policies
- Failure During Deploying Applications Policies
- Warning During Deploying Applications Policies
- Warning during Migrate Security Store
- IDM Server Failure During Deployment of Applications Policies

### 6.14.1 Log Files for Deploying Application Policies

Log files for this configuration assistant may be found in this location:

```
APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/RUP/configLogs/fapatch_Deploying_
Applications_Policies_(jazn-data.xml)_timestamp.log
```

### 6.14.2 Failure During Analysis of Applications Policies

**Problem**

A failure occurs during applications policy analysis.

**Solution**

Review the log file that is generated by each stripe. The log files are located under the main log directory, `APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/RUP` and are named as follows:

- `fapatch_CRMJaznAnalysis_timestamp.log`
- `fapatch_FSCMJaznAnalysis_timestamp.log`
- `fapatch_HCMJaznAnalysis_timestamp.log`
- `fapatch_OBIJaznAnalysis_timestamp.log`
- `fapatch_SOAJaznAnalysis_timestamp.log`
- `fapatch_UCMJaznAnalysis_timestamp.log`
- `fapatch_BPMJaznAnalysis_timestamp.log`

After you resolve the JAZN analysis error, retry the analysis for the failed stripe to confirm the issue is resolved.

### 6.14.3 Failure During Deploying Applications Policies

**Problem**

A failure occurs during **Deploying Application Policies**.

**Solution**

When a failure occurs during **Deploying Application Policies**, you must restore only the stripe or system policy that has failed, from your backup. Use the OPSS `migrateSecurityStore` command with the appropriate source and destination

arguments to perform the restore. Do not restore a stripe that has not failed. Review the JAZN deployment log file to determine the cause of the failure, `fapatch_Deploying_Applications_Policies_(jazn-data.xml)_timestamp.log`.

After you resolve the issue, resume Upgrade Orchestrator.

For more information, see "Migrating with the Script migrateSecurityStore" in the *Oracle Fusion Middleware Application Security Guide*.

## 6.14.4 Warning During Deploying Applications Policies

### Problem

The following warning occurs during **Deploying Application Policies**:

```
WARNING: Failed to validate the xml content. cvc-complex-type.2.4.a: Invalid
content was found starting with element 'property'. One of
'{"http://xmlns.oracle.com/oracleas/schema/11/jps-config-11_1.xsd":propertySetRef,
"http://xmlns.oracle.com/oracleas/schema/11/jps-config-11_1.xsd":extendedProperty,
"http://xmlns.oracle.com/oracleas/schema/11/jps-config-11_
1.xsd":extendedPropertySetRef,
"http://xmlns.oracle.com/oracleas/schema/11/jps-config-11_
1.xsd":serviceInstanceRef}'
is expected. Location: line 165 column 96.
WLS ManagedService is not up running. Fall back to use system properties for
configuration.
```

### Solution

You can safely ignore this message as there is no functional impact of this warning and the deployment is successful.

## 6.14.5 Warning during Migrate Security Store

### Problem

The following warning occurs during **Deploying Application Policies**:

```
FINE: Application policies already exists for application: fscm
oracle.security.jps.service.policystore.PolicyObjectAlreadyExistsException:
Cannot create application policy context "fscm".
        at
oracle.security.jps.internal.policystore.ldap.LdapPolicyStore.unsync_createApp
licationPolicy(LdapPolicyStore.java:833)
        at
oracle.security.jps.internal.policystore.ldap.LdapPolicyStore.createApplicatio
nPolicy(LdapPolicyStore.java:753)
        at
oracle.security.jps.internal.tools.utility.destination.apibased.JpsDstPolicy.c
lone(JpsDstPolicy.java:805)
```

### Solution

You can safely ignore this message as there is no functional impact of this warning and the deployment is successful.

### 6.14.6 IDM Server Failure During Deployment of Applications Policies

**Problem**

The IDM Server goes down during **Deploying Application Policies** and the deployment fails.

**Solution**

Upgrade Orchestrator does not allow a retry after this type of failure. You must instead exit orchestration and restore from your IDM backup. Then resume Upgrade Orchestrator.

## 6.15 Troubleshooting Server Start and Stop Failures

This section includes the following troubleshooting topics:

- General Server Failure Due to Time Out Failures

- Failure to Start BIServer

- Startup Failed for CommonDomain: OHSComponent (Oracle VM Only)

- EditTimedOutException Error During Online Preverification

- The SOA-infra Application is in a Warning State

- The SOA-infra Application is in a Warning State on All Domains

### 6.15.1 General Server Failure Due to Time Out Failures

**Problem**

A failure during the **Starting All Servers** configuration assistant typically happens when one of the servers times out and fails to start due to resource issues or application specific issues.

**Solution**

Various platforms and environment configurations can impact how long it will take all servers to actually start during the **Starting All Servers** configuration assistant. Although RUP Installer waits an average amount of time for this configuration assistant to complete before it is marked as **Failed**, different platforms may require more time. It is not unusual to receive timeout errors in the log files if the starting of all servers for your environment requires more time than RUP Installer allows. If this configuration assistant fails, follow these steps:

1. Monitor the status of the servers by reviewing the messages in the server log files or on the console. The log file, *APPLICATIONS_ CONFIG*/lcm/logs/11.1.7.0.0/RUP/StartStop/fastartstop_*timestamp*.log, indicates which server started and failed to start.

   An example of messages for a server that timed out follows.

   ```
   Time out while performing Start for domain SCMDomain. Waited for 2400 seconds
   [2011-10-21T03:57:52.052--8:00] [fastartstop] [NOTIFICATION:1] [UTIL]
   [oracle.apps.startstop.util.MbeanUtil: runSSCommandOnDomain.868] [tid:37] Start
   operation is completed for domain SCMDomain. Please see SCMDomain.log for
   details.

   [2011-10-21T03:57:52.052--8:00] [fastartstop] [NOTIFICATION:1] [UTIL]
   [oracle.apps.startstop.invoke.StartStopTask: call.221] [tid:37] StartStopTask
   ```

```
over for domain SCMDomain

[2011-10-21T03:57:52.052--8:00] [fastartstop] [NOTIFICATION:1] [SST]
[oracle.apps.startstop.invoke.StartStopTask: call.223] [tid:37] Finished the
task for the Domain SCMDomain
```

2. Review the log files at the domain level to see a summary of the server status for that domain: *APPLICATIONS_ CONFIG*/lcm/logs/11.1.7.0.0/RUP/StartStop/*domain name_timestamp*.log.

3. Review the corresponding server logs for the failed servers under the following directory: *APPLICATIONS_CONFIG*/domains/*hostname*/*domain name*/servers/*server name*/logs.

4. After you determine and resolve the cause of the failure, restart Upgrade Orchestrator.

## 6.15.2 Failure to Start BIServer

**Problem**

The following exception during the **Starting all Servers** configuration action indicates a failure in starting the BIServer:

```
Start all servers fails to start
Start operation on the component :coreapplication_obips1:, for the instance
:BIInstance: - FAILED
```

The coreapplication_obips1 server log file reports the following error:

```
ecid:]]
[2012-04-10T00:22:20.000-07:00] [OBIPS] [ERROR:16] []
[saw.security.odbcuserpopulationimpl.initialize] [ecid: ] [tid: ] Unable to
create a system user connection to BI Server during start up. Trying again.[[
File:odbcuserpoploaderimpl.cpp
Line:325
Location:
saw.security.odbcuserpopulationimpl.initialize
saw.catalog.local.loadCatalog
saw.subsystems.catalogbootstrapper.loadcatalog
saw.webextensionbase.init
saw.sawserver
ecid:]]
[2012-04-10T00:22:25.000-07:00] [OBIPS] [NOTIFICATION:1] [] [saw.sawserver]
[ecid: ] [tid: ] Oracle BI Presentation Services are shutting down.[[
File:sawserver.cpp
Line:706
Location:
saw.sawserver
ecid:
```

**Solution**

Perform the following steps to work around this issue.

1. Resume Upgrade Orchestrator, which shuts down and starts bi_server1.

2. Monitor the fastartstop log files and the state of bi_server1(BIDomain).

3. As soon as bi_server1 restarts, as indicated by a RUNNING status, start the component coreapplication_obiccs1 or all the components of type OracleBIClusterControllerComponent using opmnctl.

Example syntax follows:

```
*/BIInstance/bin/opmnctl startproc ias-component=coreapplication_obiccs1
```

### 6.15.3 Startup Failed for CommonDomain: OHSComponent (Oracle VM Only)

**Problem**

The OHS diagnostic log contains the following error message:

```
No such file or directory:  Couldn't create accept lock
```

**Solution**

This issue could be the result of the hypervisors going down, resulting in bringing the Oracle VM servers down. Perform the following steps to resolve the error:

1. Find the entry for the lock file in httpd.config, for example:

   ```
   LockFile "/u101/ohs_inst1/diagnostics/logs/OHS/ohs1/http_lock"
   ```

2. Confirm whether the directory that contains the lock file exists.

3. Assuming this directory does not exist, create the directory.

### 6.15.4 EditTimedOutException Error During Online Preverification

**Problem**

The following error is reported during Online Preverification:

```
weblogic.management.mbeanservers.edit.EditTimedOutException
```

**Solution**

You may have to manually release the edit session. For more information, see "Resolving an EditTimedOutException Error" in the *Oracle Fusion Applications Patching Guide*.

### 6.15.5 The SOA-infra Application is in a Warning State

**Problem**

After the upgrade, the following error displays after you log in to the WLS Console of CommonDomain. and navigate to Deployments:

```
soa-infra application is in WARNING state.
```

**Solution**

You can ignore this error as there is no functional impact for SOA users due to this error. To resolve the issue, see "Updating the soa-infra Application in Warning State" in the *Oracle Fusion Middleware Patching Guide*.

### 6.15.6 The SOA-infra Application is in a Warning State on All Domains

**Problem**

The soa-infra app is in a warning state in all domains and errors are reported related to "jms/bpm/CaseEventQueue".

**Solution**

This error can be ignored.

# 6.16 Troubleshooting SOA Composite Deployment Failures

This section describes how to recover from failures during the **Deploying SOA Composites** configuration assistant. The following topics are described:

- SOA Composite Log Files
- SOA Composite Failure Does Not Recover
- Wsm-pm Application is not Running in Domain (Solaris Only)
- Manually Deploying SOA Composites
- Invoke an Instance of SOA Composite
- Merging SOA Composite JDeveloper Customizations During SOA Preverification

## 6.16.1 SOA Composite Log Files

The following log files are generated by the deployment of SOA composites:

- Client side log files where individual domain logs reside: *APPLICATIONS_ CONFIG*/lcm/logs/11.1.7.0.0/RUP/soalogs

- Log files for the failed domain:

  - *APPLICATIONS_CONFIG*/domains/*hostname*/*domain name*/servers/*server name*/logs/soa_server1.log

  - *APPLICATIONS_CONFIG*/domains/*hostname*/*domain name*/servers/*server name*/logs/soa_server1.out

  - *APPLICATIONS_CONFIG*/domains/*hostname*/*domain name*/servers/*server name*/logs/soa_server1-diagnostic.log

  - *APPLICATIONS_CONFIG*/domains/*hostname*/*domain name*/servers/*server name/*logs/AdminServer.log

## 6.16.2 SOA Composite Failure Does Not Recover

**Problem**

Normally, a failed SOA composite is undeployed by RUP Installer. However, if the failure of the deployment is due to an issue such as SOA servers running out of memory, then RUP Installer does not recover until you resume Upgrade Orchestrator.

Examples of error messages related to SOA Composite failures follow:

```
CFGLOG-00380: SOA composite "composite_name" patch failed for server "server_
name".
Recovery process also failed with an unknown reason. If the SOA composite
patch exists on the server, it will be automatically undeployed during retry
or a checkpoint run. Also if the base composite is not the default composite,
it will be automatically set as default.

CFGLOG-00327: SOA composite "composite_name" patch failed for server "server_
name".
Recovery process also failed, and the composite patch is not undeployed.
The patch will be automatically undeployed during retry or a checkpoint run.
```

```
CFGLOG-00328: SOA composite "composite_name" patch failed for server "server_
name".
Recovery process also failed, and the base composite is not set as the
default composite. The base composite will be automatically set as default
during retry or a checkpoint run.
```

Examples of report exceptions follow:

```
CFGEX-00087: SOA composite "composite_name" patch failed for server "server_name".
Recovery process also failed. Recovery will be done automatically during retry or
a checkpoint run.
Action : No action required.

CFGEX-00073: SOA composite "composite_name" patch failed for server "server_name".
Action : See logs for details.
```

**Solution**

When patching existing SOA composites, RUP Installer automatically recovers any partially deployed SOA composites after failure when you restart Upgrade Orchestrator. The following actions can be performed by Upgrade Orchestrator:

■ Undeploy the partially deployed SOA composite revision if it is still present.

■ Set as default the same SOA composite revision that was default before the patching was attempted, if it's not already set as default.

If the failure was caused by an environment issue, such as running out of memory, resolve the cause of the failure before you restart RUP Installer.

## 6.16.3 Wsm-pm Application is not Running in Domain (Solaris Only)

**Problem**

The following error is reported during SOA Composite deployment on a Solaris platform:

```
CFGEX-00079 : Wsm-pm application is not running in domain "domain name"
```

You have already confirmed that the `wsm-pm` application is running on this domain.

**Solution**

Perform the following steps:

1. Log in to the failed domain and check the health of all managed servers and deployed applications.

2. Bounce all managed servers of the failed domains.

3. Exit Upgrade Orchestrator.

4. Restart Upgrade Orchestrator.

## 6.16.4 Manually Deploying SOA Composites

If a customized SOA composite deployment fails during the upgrade, you must manually deploy this composite using WLST commands.

**To apply a SOA composite manually after a deployment failure**

In the following steps, the example composite, `FinAp`, is patched from revision 1.0 to revision 2.0 and the SAR file of revision 2.0 is in *FA_ORACLE_HOME*/crm/deploy/sca_ FinAp_rev2.0.jar.

Note that the parameters are for illustration purposes only.

1. Refer to the Diagnostics report to find the name and location of the sca_*.jar file that was copied to *FA_ORACLE_HOME* by Oracle Fusion Applications Patch Manager. For more information, see "Diagnostics Report" in the *Oracle Fusion Applications Patching Guide*.

2. If the previous revision contained JDeveloper customizations, ensure that you deploy the patched revision with the merged JDeveloper customizations. Using the sca_*.jar file from Step 1, follow the JDeveloper customization merge instructions that are described in Section 6.16.6, "Merging SOA Composite JDeveloper Customizations During SOA Preverification". Then use the merged sca_*.jar for Step 3.

3. Deploy the patched composite using the single patch composite command.

    ```
    sca_patchComposite('SOA-Infra URL', user, password,
    '/FA_ORACLE_HOME/crm/deploy//sca_FinAprev2.0.jar',
    mergeLogFile='/tmp/merge-log.txt')
    ```

## 6.16.5 Invoke an Instance of SOA Composite

You must run the `UpdateSOAMDS` SOA composite on every domain if you made any flexfield changes, by following the steps described in "Task: Synchronizing Customized Flexfields in the MDS Repository for SOA" in the *Oracle Fusion Applications Extensibility Guide for Developers*.

## 6.16.6 Merging SOA Composite JDeveloper Customizations During SOA Preverification

If you performed JDeveloper customizations to a SOA composite and you deployed the composite to the SOA runtime, RUP Installer reports an error during **SOA Preverification**, which instructs you to take the newer version of the composite that is in the release. You must then merge your customizations by performing the following steps.

1. If any customizations are detected, the SOA Preverification results display the SOA composite name, its location in the *FA_ORACLE_HOME*/*stripe*/deploy directory, and the requirement for you to merge JDeveloper customizations into the sca_*.jar file in *FA_ORACLE_HOME* before proceeding with RUP Installer. The *stripe* in the directory path refers to crm, hcm, fscm, and so on.

2. Open the custom SOA workshops and the customized version of the Fusion Applications SOA composite in JDeveloper using "Oracle Fusion Applications Developer". For more information, see "Customizing SOA Composite Applications with JDeveloper" in the *Oracle Fusion Applications Extensibility Guide for Developers*.

3. Import the composite sca_*.jar file from *FA_ORACLE_HOME*/*stripe*/deploy into the project, for example revision 11.1.7.0.0, in JDeveloper. Make note of this revision number in the deployment window because you will need it in Step 8.

4. Restart JDeveloper in the Oracle Fusion Applications Administrator Customization role.

5. Verify that there are no errors in JDeveloper.

6. Verify that the changes introduced in both the customized version and the patched version are present.

7. Right-click the composite project in the Application Navigator, select **Deploy**, select the composite, click **Deploy to SAR**, and click **Next**.

8. Manually change the value in **New Revision ID** to the revision from Step 3, for example, 11.1.7.0.0, and click **Finish**.

9. If the deployment folder is set to a location different from that of the *FA_ORACLE_HOME*/*stripe*/deploy directory, copy and replace the JAR in the location mentioned in the error message of this SOA Composite. If your file name is different, rename it to the original name. You must copy the jar in the correct format to *FA_ORACLE_HOME*/*stripe*/deploy. For example if you have sca_ContractsDeliverablePurchaseDocAttrReadComposite_rev11.1.7.0.0.jar in JDeveloper, then you must copy it back to the *FA_ORACLE_HOME*/*stripe*/deploy directory as sca_ContractsDeliverablePurchaseDocAttrReadComposite.jar.

10. To proceed with the installation, use the same command you used to start Upgrade Orchestrator.

For more information about customizing SOA composites, see "Customizing and Extending SOA Components" in the *Oracle Fusion Applications Extensibility Guide for Developers*.

# 6.17 Troubleshooting RUP Lite for OVM

Review the /u01/lcm/rupliteovm/output/logs/ruplite.log file to confirm there are no errors. You can also check rehydration framework logs under /assemblybuilder/logs or /var/log for any errors.

The following troubleshooting issues are also described in this section:

- RUP Lite for OVM Plug-in Failures

- RUP Lite for OVM Validation Fails

- RUP Lite for OVM in Offline Mode or Online Mode Hangs

- RupLiteOvmValidatePlugin Hangs

- RUPLite for OVM in Offline Mode Fails on ovm.plugin.DisableWebchat

- RUP Lite for OVM in Offline Mode Fails With Offline Data Files Issue

- RUP Lite for OVM in Post-Root Mode Fails With Property Issues

- RUP Installer Fails During Apply Pre-PSA Due to Smart Patch Conflict (Oracle VM Only)

## 6.17.1 RUP Lite for OVM Plug-in Failures

Review the following troubleshooting information for specific plug-ins:

- **UpdateSESDBConnection:** This plug-in is rerunnable. The rehydration command this plug-in calls requires that all database schema passwords be registered in the credentials store. The credential store must contain a entry for FUSION_DISCUSSIONS_CRAWLER. The following error message appears in the ruplite.log file if this entry is missing:

```
Executing Task:
oracle.apps.fnd.provisioning.ovm.rehydratefw.cli.cmd.fasec.UpdateSESDBConnectio
nCmd ... FAILED. [0m31s]
```

```
An error occurred: An error occurred during command execution: A password could
not be retrieved because:
The deploy property 'credential.FUSION_DISCUSSIONS_CRAWLER.password' does not
have a value.
A value from the credential store could not be read or does not exist. A
reference property was not provided.
```

The Register Database Schema tool populates the credentials store with database schema passwords. For more information, see Section 2.4.2.3, "Prepare to Register Database Schema Information".

Perform the following steps to verify this plug-in was successful:

1. Open the Oracle Secure Enterprise Search administration page.

2. Go to the **Sources** tab.

3. Edit the **Announcements** data source.

4. Verify that **Source Configuration - Database Connection String** and **Authorization - Authorization Database Connection String** reflect the values for host, port, and service name from `ovm-ha-deploy.properties`. If the `faovm.ha.fusiondb.new.is.rac` property is set to false, the non-RAC port values will be used. If this property is set to true, the RAC port values will be used.

- **DeployECSF**: This plug-in is rerunnable. If your environment was originally provisioned before Release 5, you can verify that this plug-in was successful by confirming that the help object, schedule and group being deployed are reported in the log file. You can also use Fusion Applications Control to connect to the Administration Server that hosts the search application and confirm that the Help instance artifacts are deployed.

- **DisableWebchatConnections:** This plug-in is rerunnable. If your environment has WebChat enabled this plug-in does not disable the connection.

- **ValidateEnvironment**: If this plug-in fails, RUP Lite for OVM stops. You must resolve any errors reported in the log file and then run RUP Lite for OVM again.

- **SetupCredentials:** If this plug-in fails, RUP Lite for OVM stops. Typical causes of failure are an incorrect key for an existing wallet, or specifying a key for a new wallet that does not meet Oracle's minimum standards. You must resolve any errors reported in the log file and then run RUP Lite for OVM again.

  Note that you are prompted for the password twice and that both responses must be identical. If you need to change the password in the wallet, set the `ovm.plugin.SetupCredentials.enable_password_update property` to true. If this property is enabled, when the `SetupCredentials` plug-in reruns, you are given the option to overwrite the existing password for a particular plug-in, in the wallet. By default this feature is disabled.

- **UpdateResolvConf:** This plug-in is rerunnable. If a value already exists in the `/etc/resolv.conf` file, it will not be added again. If you remove a property value from `metadata/env.properties`, the value is not removed from `/etc/resolve.conf` by running the plug-in again.

- **ApplyMemorySettings**: Check the `fusionapps_start_params.properties` files in the environment, which are located under the `bin` directory of each domain. Ensure that the `minmaxmemory` settings in the files are at least as high as the settings in the template under the `ovm/metadata` directory that corresponds to the environment's topology.

- **GenerateOptimizedQueryPlans:** This plug-in is rerunnable. Verify this plug-in was successful by connecting to the database as **fusion_mds** and running the following command:

```
SELECT TO_CHAR(last_analyzed, 'yyyy/mm/dd hh:mi:ss am') as last_analyzed FROM
user_tables;
```

The results should show that the tables were just analyzed.

- **DisableSearchUI:** This plug-in is rerunnable. Verify this plug-in was successful by connecting to the database as **fusion** and running the following command:

```
select fnd_profile.value('FUSION_APPS_SEARCH_ENABLED') from DUAL;
```

The result should be "N".

- **UpdateFusionIIRDiag**: This plug-in is rerunnable. Verify this plug-in was successful by confirming that the fusioniirdiag.sh script in the *APPLICATIONS_ BASE*/InformaticaIR/bin directory is the updated version and the permissions and ownership of this script match those of the other scripts in the same directory. You can verify the version by noting the date and size of the file.

- **DisableWebchat:** Verify this plug-in was successful by confirming that the following SQL*Plus queries return no rows:

```
SELECT username FROM all_users WHERE username LIKE '%BEE%';
SELECT tablespace_name FROM dba_tablespaces WHERE tablespace_name LIKE '%BEE%';
```

Also verify that the beehivereadonlyuser user does not exist in LDAP and that the WebChat Oracle VM is shut down.

## 6.17.2  RUP Lite for OVM Validation Fails

If RUP Lite for OVM validation fails, the cause of the failure could be that a non-application user, such as root, was used to create the RUP Lite for OVM wallet. If this is the case, perform the following steps to resolve the issue.

1. Copy the Release 6 pre-upgrade rupliteovm to the share.

2. Edit env.properties to enable the CreateEMFAWallet property and set CUSTOM_ WALLET_DIR to the absolute path of the output/wallet directory of rupliteovm.

3. Run RUP Lite for OVM in wallet mode to create the wallet.

4. Run RUP Lite for OVM in validate mode from that primordial host as the correct applications user, not as root.

## 6.17.3  RUP Lite for OVM in Offline Mode or Online Mode Hangs

**Problem**

 RUP Lite for OVM runs for a long time during domain configuration.

**Solution**

Perform the following steps to resolve this issue:

1. Ensure that the IDM host is accessible and responding.

2. Ensure that the database is accessible and responding.

3. If either the IDM host or the database is not responding, update the status of the orchestrator task that runs RUP Lite for OVM to "Error", using the following command:

```
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype host_type -hostname
host_name -release release_number -phase phase_name -taskid plugin_name
-taskstatus Error
```

Fix the issue with the IDM host or the database and resume Upgrade Orchestrator.

4. If none of the above steps solve the problem, contact Oracle Support with detailed log information.

## 6.17.4 RupLiteOvmValidatePlugin Hangs

**Problem**

During the `PreDowntime` phase, the `RupLiteOvmValidatePlugin` hangs.

**Solution**

The plug-in, `RupLiteOvmValidatePlugin`, creates a log with the lock file, `ruplitevalidate.log.lck`.

Perform the following steps to resolve this issue:

1. Verify if your Shared directory is mounted with the `nolock` option. If the Shared directory is mounted with the nolock option then remove the .lck file and proceed with ruplite validate. If this is not the case, then create the mount point of the Shared directory with nolock with the following command:

```
mount -o nolock host_name:directory_path_to_which_directory
```

2. Remove the .lck file.

```
rm ruplitevalidate.log.lck
```

3. Run ruplite from the mount point used in Step 1:

```
bin/ruplite.sh validate
```

## 6.17.5 RUPLite for OVM in Offline Mode Fails on ovm.plugin.DisableWebchat

**Problem**

RUPLite for OVM can fail on `ovm.plugin.DisableWebchat` if there are guaranteed restore points in the database.

**Solution**

Perform the following steps to drop the restore points and resume Upgrade Orchestrator

1. Connect as SYS user.

2. Run the following SQL*Plus query:

```
SELECT NAME, SCN, TIME, DATABASE_INCARNATION#,GUARANTEE_FLASHBACK_
DATABASE,STORAGE_SIZE FROM
V$RESTORE_POINT WHERE GUARANTEE_FLASHBACK_DATABASE='YES';
```

3. If the query returns any restore points, drop the restore points using the following command:

```
DROP RESTORE POINT restore_point_name;
```

4. Resume Upgrade Orchestrator.

## 6.17.6 RUP Lite for OVM in Offline Mode Fails With Offline Data Files Issue

**Problem**

During the RUP Lite for OVM Offline task, a failure with a message "RUP Lite for OVM in offline mode task failed" is reported.

**Solution**

Check the log file to see if an error exists as shown in the following example:

```
ORA-01191: file 28 is already offline - cannot do a normal offline
ORA-01110: data file 28: '+DATA/prtff/datafile/bee_data.dbf
```

If this error is reported, perform the following steps.

1. Connect to the database as SYSDBA and run the following SQL*Plus query to determine if the data file is offline.

```
select FILE_NAME,ONLINE_STATUS from dba_data_files where ONLINE_
STATUS<>'ONLINE';
```

An example of a data file that is offline follows:

```
DATA/prtff/datafile/bee_data.dbf, OFFLINE
```

2. If there are offline files, run the following command as SYSDBA:

```
alter database datafile 'PATH_TO_DATAFILE' online
```

The *PATH_TO_DATAFILE* is the path that was returned by the previous query.

3. Resume Upgrade Orchestrator.

## 6.17.7 RUP Lite for OVM in Post-Root Mode Fails With Property Issues

**Problem**

RUP Lite for OVM in the post-root mode fails with the following error:

```
"Property faovm.topo.type not found in context file"
```

**Solution**

Rerun RUP Lite for OVM in the post-root phase, and if the issue persists, contact Oracle Support.

## 6.17.8 RUP Installer Fails During Apply Pre-PSA Due to Smart Patch Conflict (Oracle VM Only)

**Problem**

For the CRM stripe on an Oracle VM environment during the Release 6 to Release 7 upgrade, RUP Installer fails during the Apply Pre-PSA Middleware Patches

configuration assistant, due to a smart patch conflict. The following exception is reported:

```
"Conflict(s) detected - resolve conflict condition and execute patch
installation again.

Conflict condition details follow:

SEVERE: Conflict(s) detected - resolve conflict condition and execute patch
installation again

Patch HYKC is mutually exclusive and cannot coexist with patch(es):
3BBT,SZXM,7YZB,6D9T,56MM,F89C,9264,9887,S39F,7AAZ,JZED,E9FL,IH4D,YJTB

SEVERE: Patch HYKC is mutually exclusive and cannot coexist with patch(es):
3BBT,SZXM,7YZB,6D9T,56MM,F89C,9264,9887,S39F,7AAZ,JZED,E9FL,IH4D,YJTB"
```

**Solution**

Manually roll back all conflicting WLS patches and rerun orchestration.

## 6.18  Troubleshooting Health Checker Issues

- Resolving JAZN Conflicts Found by Health Checker
- Verifying OS Attributes Health Check Failed
- Health Checker Fails Due to Active ODI Sessions
- Health Checker Fails During Default Keystore Size Check
- Troubleshooting Hanging Issue for Health Checker

### 6.18.1  Resolving JAZN Conflicts Found by Health Checker

Health Checker checks the JAZN Analysis reports for potential conflicts and deletions that are not patched automatically by RUP Installer. The reports are located in this directory:

**Release 7 location:**

*APPLICATIONS_
CONFIG*/lcm/admin/11.1.7.0.0/fapatch/JAZN/*stripe*/delta/report.txt

**Release 6 location:**

*APPLICATIONS_
BASE*/fusionapps/applications/admin/JAZN/*stripe*/delta/report.txt

The *stripe* is crm, fscm, hcm, obi, soa, ucm or bpm.

Review the Modification section of the report to see the roles that RUP Installer did not update. For each conflict that displays in this report, you must evaluate and manually patch the role by using Oracle Authorization Policy Manager (APM). For more information, see "Upgrading Oracle Fusion Applications Policies" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*.

The following example shows a typical Application Role conflict that has been modified by both the patch and production, therefore it is not applied by RUP Installer.

```
MODIFICATION CONFLICTS
```

```
Artifact type: Application Role
Artifact Name: OBIA_PARTNER_CHANNEL_ADMINISTRATIVE_ANALYSIS_DUTY
Description: This artifact is modified at attribute level in patch version and
also in production.
```

Note the location of the following files for reference when using APM:

- Location of baseline files, where stripe is crm, fscm, hcm, obi, soa, ucm or bpm:

  *FA_ORACLE_HOME*/admin/JAZN/*stripe*/baseline

- Location of patch files for fscm, crm, and hcm stripes:

  *FA_ORACLE_HOME/stripe*/deploy/system-jazn-data.xml

- Location of patch files for the obi, soa, ucm or bpm stripes:

  *FA_ORACLE_HOME*/com/acr/security/jazn/bip_jazn-data.xml

## 6.18.2  Verifying OS Attributes Health Check Failed

### Problem

Health Checker reports the following error when running the Verifying OS Attributes check:

```
[ERROR]: Plugin 'OsCheck': HC-OS-00002 : OS Support Check failed.Error(s):
OS version is not supported(Check for OS name ,arch and version
support)(Pre-Downtime Checks)
```

### Solution

If you are using Red Hat Enterprise Linux Server release 5.* (Tikanga), a manual verification of OS platform is required to determine if this validation error can be ignored. To perform the manual validation, run the osarch.sh script, which is located under *SHARED_LOCATION/ORCH_LOCATION/*util. Verify that the PLATFORM_TYPE=Linux, the OS_ARCH=x86_64, and the PLATFORM_VERSION is any sub-version of version 5 (Tikanga) of RHEL Server. If all of the above requirements are satisfied, the error is safe to ignore. Otherwise, refer to the suggested corrective actions provided by Health Checker. Sample output from the osarch.sh script follows:

```
PLATFORM_TYPE=Linux
OS_ARCH=x86_64
PLATFORM_VERSION=Enterprise Linux Server release 5.6 (Tikanga)
```

## 6.18.3  Health Checker Fails Due to Active ODI Sessions

### Problem

Health Checker fails during pre-down time or down time because of finding active ODI sessions.

### Solution for Failure During Pre-Down Time

Ignore the failure and proceed.

### Solution for Failure During Down Time

Run the following update statement and resume Upgrade Orchestrator.

```
UPDATE FUSION_ODI.SNP_SESSION SET SESS_STATUS='E' WHERE SESS_STATUS IN ('W', 'R',
'Q');
```

### 6.18.4 Health Checker Fails During Default Keystore Size Check

**Problem**

Health Checker reports the following error during the Default Keystore Size Check:

```
[ERROR]: Plugin 'DefaultKeystoreSizeCheck': HC-DKS-0002 : Following domain's
default keystore file size is different from CommonDomain domain's default
keystore file located at
/u01/APPLTOP/instance/domains/admin-apps.oracleoutsourcing.com/CommonDomain/co
nfig/fmwconfig/default-keystore.jks which has the size of 1,867 bytes.
List of Domains that are different are:
[Domain name: CRMDomain , File location:
/u01/APPLTOP/instance/domains/admin-apps.oracleoutsourcing.com/CRMDomain/confi
g/fmwconfig/default-keystore.jks, File size: 2658 Bytes]

Corrective action: Contact Oracle Support to resolve the issue.(Checks the
size of default-keystore.jks file in all domains)
```

**Solution**

This error can be ignored.

### 6.18.5 Troubleshooting Hanging Issue for Health Checker

**Problem**

If a health check is taking too long or if it is hanging, it can be terminated.

**Solution**

To confirm a health check is hung, make sure that there has been no logging for more than 30 minutes by comparing the current timestamp and the last timestamp in the *manifest_name*.log.lck file. Perform the following steps to terminate a hanging health checker process.

1.  Query the list of running processes for
    `oracle.healthcheckplug.core.PluginManager` using the following command:

    ```
    ps -ef | grep oracle.healthcheckplug.core.PluginManager
    ```

2.  Terminate the process id of the process returned by the previous command by using the following command:

    ```
    kill -KILL java process id
    ```

3.  After terminating the process, perform any corrective action and resume Upgrade Orchestrator.

## 6.19 Troubleshooting Other Potential Issues During the Upgrade

This section provides information about the following troubleshooting issues:

- Troubleshoot setenv PERLIB5 Version Compatibility
- Pre-Upgrade Task Fails Because SES Crawler Processes Cannot Be Stopped
- UpdateMDSSOAComposite Task Fails During DowntimePostFA
- Policy Store and Oracle Platform Security Services Versions Are Not Compatible
- Troubleshooting Bootstrapping Patch Manager

- Troubleshooting Failures During Propagating Domain Configuration
- RUP Lite for Domain Configuration Takes Too Long to Complete
- Troubleshooting Deployment of BI Publisher Artifacts
- PatchInventoryCheckPlugin Fails During Predowntime
- Failure During IPM Import
- GUI Mode Language Pack Installation Failure
- Orchestration Fails With StartAllServers Task After Language Pack Upgrade on CRM
- WLS SocketTimeoutException During Server Startup During Upgrade
- Orchestration Unable to Initialize the Checkpoint System
- Upgrade JDK in a Freshly Provisioned Release 6 Environment
- Upgrade JDK in a Freshly Provisioned Release 6 Environment (AIX)
- Ignorable Errors Reported by catbundle.sql
- Performing Installation Verification Steps

### 6.19.1 Troubleshoot setenv PERLIB5 Version Compatibility

**Problem**

While downloading patches, as described in Section 2.3.5.2 or Section 2.3.6.3, you are setting environment variables to run the `adCreateMosPlan.pl` script. After you issue the `setenv` command for PERLLIB5, the following error occurs: `Perl lib version (v5.8.3) does not match the executable version (v5.8.8)`.

**Solution**

Run the following commands:

```
export PERL_HOME=/u01/APPLTOP/dbclient/perl
export PATH=/u01/APPLTOP/dbclient/perl/bin:$PATH
```

Then retry the `setenv` command.

### 6.19.2 Pre-Upgrade Task Fails Because SES Crawler Processes Cannot Be Stopped

**Problem**

SES crawler processes in the LAUNCHING state cannot be stopped by the pre-upgrade task, so the pre-upgrade task fails.

The following error message appears in the primordial host orchestration log. The schedule names listed in the following examples are the schedules that could not be stopped.

```
[2013-12-06T15:22:47.188+00:00] [orchestration] [NOTIFICATION] []
[oracle.orchestration] [tid: 13] ERROR: Failed to stop the following Index
Launching Schedules:

[2013-12-06T15:22:47.188+00:00] [orchestration] [NOTIFICATION] []
[oracle.orchestration] [tid: 13]

[2013-12-06T15:22:47.188+00:00] [orchestration] [NOTIFICATION] []
```

```
[oracle.orchestration] [tid: 13] Purchasing Contract Documents

[2013-12-06T15:22:47.188+00:00] [orchestration] [NOTIFICATION] []
[oracle.orchestration] [tid: 13] Purchasing Contracts

[2013-12-06T15:22:47.188+00:00] [orchestration] [NOTIFICATION] []
[oracle.orchestration] [tid: 13] References

[2013-12-06T15:22:47.188+00:00] [orchestration] [NOTIFICATION] []
[oracle.orchestration] [tid: 13] Sourcing Contracts

[2013-12-06T15:22:47.188+00:00] [orchestration] [NOTIFICATION] []
[oracle.orchestration] [tid: 13] FAILURE: SesDisableIndexSchedules failed.
```

**Solution**

Bounce the ESS server of the common domain and resume Upgrade Orchestrator.

### 6.19.3 UpdateMDSSOAComposite Task Fails During DowntimePostFA

**Problem**

The UpdateMDSSOAComposite task, which runs during the downtimePostFA phase, can cause a run time exception or stop responding for more than one hour without any updates to logs. This is an example of an exception if failure occurs:

```
java.lang.RuntimeException: javax.naming.NamingException:
Unhandled exception in lookup [Root exception is org.omg.CORBA.MARSHAL:..
```

**Solution**

> **Note:** This task, when successful, may take a long time and you should ensure that the upgrade does not respond for more than an hour without any log activity before following these steps.

Perform the following steps.

1. Look for the Java processes that are running by using command, ps -ef | grep java, and terminate the Java processes by using command, kill -9 <process ID>.

2. Execute the command, cd ORCH_LOCATION/config.

3. Back up the release manifest file. This is either rel5-7_primordial.xml for a multi- hop upgrade or rel7_primordial.xml for a single hop upgrade from Release 6 to 7.

4. In the backup file, look for the plug-in name, such as <plugin id="UpdateMDSSOAComposite>.

   Lines should be associated with the plug-in entry as shown in the following example:

   ```
   %APPLICATIONS_BASE%/fusionapps/applications/oui/jlib/
   xmlparserv2.jar;%APPLICATIONS_BASE%/fusionapps/
   wlserver_10.3/server/lib/wlclient.jar;
   %APPLICATIONS_BASE%/fusionapps/wlserver_10.3/server/
   lib/weblogic.jar"active="true"
   ```

5. Remove the `wlclient.jar` line only, and save the file. The new file looks as follows:

```
%APPLICATIONS_
BASE%/fusionapps/applications/oui/jlib/xmlparserv2.jar;%APPLICATIONS_
BASE%/fusionapps/wlserver_10.3/server/
lib/weblogic.jar"active="true"
```

6. Resume Upgrade Orchestrator on the primordial host.

## 6.19.4 Policy Store and Oracle Platform Security Services Versions Are Not Compatible

### Problem

After upgrading to Release 11.1.1.7.0, you receive the following error while connecting to ODI Studio:

```
oracle.security.jps.service.policystore.PolicyStoreIncompatibleVersionException

JPS-06100: Policy Store version 11.1.1.7.0 and Oracle Platform Security Services
Version 11.1.1.6.0 are not compatible.
```

### Solution

Upgrade or reinstall the ODI studio component from Release 11.1.1.7.0. For more information, see "Setting Up Oracle Data Integrator Studio" in the "Human Capital Management" chapter in the *Oracle Fusion Applications Post-Installation Guide* and "Installing Oracle Data Integrator" in the *Oracle Fusion Middleware Installation Guide for Oracle Data Integrator*.

## 6.19.5 Troubleshooting Bootstrapping Patch Manager

### Problem

An error occurred during the **Bootstrapping Patch Manager** configuration assistant.

### Solution

An error during **Bootstrapping Patch Manager** normally occurs only when the database is down. Ensure that the database is up and running. You can review the related log files in this location:

```
APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/RUP/FAPatchManager_bootstrap_
timestamp.log
```

## 6.19.6 Troubleshooting Failures During Propagating Domain Configuration

This section contains information about troubleshooting issues that may occur during the **Propagating Domain Configuration** configuration assistant. The following topics are discussed:

- Propagating Domain Configuration Assistant Takes Too Long to Complete
- Confirm the Configuration Assistant Was Successful
- WARs or EARs Are Not Accessible From The Primordial Host

### 6.19.6.1 Propagating Domain Configuration Assistant Takes Too Long to Complete

**Problem**

The Propagating Domain Configuration tasks is taking too long to complete.

**Solution**

This configuration assistant can take some time to complete as it is highly dependent on the environment, specifically the number of non-admin domains and the responsiveness of the file system.

You can monitor the progress of this configuration assistant by reviewing log files in this location:

```
APPLICATIONS_CONFIG/lcm/admin/version/fapatch//ruplitedomain/output/logs
```

### 6.19.6.2 Confirm the Configuration Assistant Was Successful

To confirm this configuration assistant was successful, verify that the `config/fusionapps_start_params.properties` file exists under each local or non-admin split domain. Also ensure that the `bin/setDomainEnv.sh` file under each local or non-admin split domain contains the following row:

```
POST_CLASSPATH="${COMMON_COMPONENTS_HOME}/modules/oracle.appstrace_
11.1.1/appstrace.jar${CLASSPATHSEP}${POST_CLASSPATH}"
export POST_CLASSPATH
```

### 6.19.6.3 WARs or EARs Are Not Accessible From The Primordial Host

**Problem**

The **Propagating Domain Configuration** configuration assistant fails if there are WARs or EARs installed or deployed that are not accessible from the primordial host where RUP Installer is running. An example of the error caused by this condition follows:

```
<< read domain from
APPTOP/instance/domains/server.company.com/SCMDomain
<< write template to
APPLICATIONS_
CONFIG/lcm/admin/11.1.7.0.0/fapatch/ruplitedomain/output/templates/SCMDomain.jar
>>  fail: Unable to locate file:
/fusionapps/localdomain/domains/server.company.com/SCMDomain/datalens/datalens.war
>>  fail: write template to
"APPLICATIONS_
CONFIG/lcm/admin/11.1.7.0.0/fapatch/ruplitedomain/output/templates/SCMDomain.jar"

CFGFWK-60550:  Script execution aborted. The script may contain an error.
Unable to locate file:
/fusionapps/localdomain/domains/server.company.com/SCMDomain/datalens/datalens.war
```

**Solution**

To resolve this issue, you must undeploy or uninstall the WAR or EAR, which is `datalens.war` in this example. Then resume orchestration. After the upgrade has completed successfully, you can install or deploy the WAR or EAR.

### 6.19.7 RUP Lite for Domain Configuration Takes Too Long to Complete

**Problem**

RUP Lite for Domain Configuration takes too long to complete.

**Solution**

This utility can take some time to complete as time taken to propagate domain configuration is highly dependent on the environment, specifically the number of non-admin domains and the responsiveness of the file system. Note this issue is seen only in local domain environments where the utility is run between RUP Installer Part 1 and Part 2. This is not an issue for Oracle VM environments or other environments with shared domains.

### 6.19.8 Troubleshooting Deployment of BI Publisher Artifacts

**Problem**

The following error occurs if the BI Presentation servers are running during the deployment of BI Publisher artifacts:

```
java.lang.RuntimeException: Webcat patch file creation failed!
```

**Solution**

If you upgrade to a release that contains BI Publisher artifacts, the BI Presentation servers must not be running. To resolve this issue, shut down the BI Presentation servers to release locks on the Oracle BI Presentation Catalog. For more information, see "fastartstop Syntax" in the *Oracle Fusion Applications Administrator's Guide*.

### 6.19.9 PatchInventoryCheckPlugin Fails During Predowntime

**Problem**

On the primordial host, orchestration may fail while running the general system checks as part of predowntime checks.

**Solution**

Perform the following steps to comment out the check.

1. Open the manifest file located at *APPLICATIONS_ BASE*/fusionapps/applications/lcm/hc/config.

2. Search for `PatchInventoryCheckPlugin`.

3. Comment out the plug-in by adding <!-- before the plug in and --> after it, as shown in the following example.

```
<!--
<plugin id="PatchInventoryCheckPlugin"
description="Verify Patch Inventory in FA_ORACLE_HOME"
invoke=""
plugin.class="oracle.check.apps.PatchInventoryCheckPlugin"
class.path="$HC_LOCATION/lib/precheckplugin.jar;
$HC_LOCATION/lib/hccommon.jar"
stoponerror="false"/>
-->
```

### 6.19.10 Failure During IPM Import

**Problem**

The configuration assistant for importing IPM artifacts fails with the following error:

```
importIPMApplication() & importIPMInput() WLST commands have not run
successfully
```

**Solution**

Follow the instructions in Steps 1 through 7 in "Prerequisites for the Deployment of IPM Artifacts" in the *Oracle Fusion Applications Patching Guide*. Then resume Upgrade Orchestrator.

### 6.19.11 GUI Mode Language Pack Installation Failure

**Problem**

In GUI mode, when installing a language pack, if any configuration action fails and then succeeds on retry, and subsequently all configuration actions were successful, the installer incorrectly shows a popup with the following message:

```
Configuration is completed with errors, exit the installer by clicking the
'Cancel' button and rerun the installer to retry the failed configurations.
```

**Solution**

Perform the following steps:

1.  Cancel the installer.

2.  Relaunch the installer in checkpoint mode. The configuration screen appears, showing no configuration actions because all actions were successful earlier.

3.  Click **Next** to go to the Installation Complete screen.

4.  Click **Finish** to exit the installer.

### 6.19.12 Orchestration Fails With StartAllServers Task After Language Pack Upgrade on CRM

**Problem**

Orchestration tries to restart all servers after a Language Pack upgrade. On CRM PODs, there may be failures in starting the IIR server, which may be reported as the following error:

```
ORCH-DOWNTIME-SS-00005 : Failed to start all servers. Review log file
/u01/APPLTOP/instance/lcm/logs/11.1.7.0.0/orchestration/host_name-rel5-7_midtier_
timestamp.log for details on the failures to take appropriate corrective action.
(Bounce All Servers).
```

**Solution**

Perform the following steps.

1.  Review the orchestration log file at /u01/APPLTOP/instance/lcm/logs/11.1.7.0.0/orchestration/*hostname*-rel5-7_ midtier_*timestamp*.log, and check for any high level failures.

2.  Review all `fa_control` logs on the failed host and look for details on the server that failed.

3.  If the IIR server is the only server that failed to start, update the status of the task to Success using the following `updateStatus` command, and resume Upgrade Orchestrator. You can restart the IIR server manually after the upgrade.

    ```
    ./orchestration.sh updateStatus -pod POD_NAME -hosttype host_type -hostname
    host_name -release REL7 -phase DowntimePostLP -taskid StartSeversAfterLP
    -taskstatus success
    ```

## 6.19.13 WLS SocketTimeoutException During Server Startup During Upgrade

### Problem

As an intermittent issue, there could be WLS socket exceptions during server startup, or during any other upgrade tasks. An example of the exception is:

```
bea_wls_management_internal2/Bootstrap, user: FUSION_APPS_PROV_PATCH_APPID
java.net.SocketTimeoutException: Read timed out
at jrockit.net.SocketNativeIO.readBytesPinned(Native Method)
at jrockit.net.SocketNativeIO.socketRead(SocketNativeIO.java:32)
```

### Solution

Find the managed server or the administration server that encounters the failure, and manually restart the server. Proceed with the upgrade by resuming Upgrade Orchestrator on the failed host.

## 6.19.14 Orchestration Unable to Initialize the Checkpoint System

### Problem

An orchestration process can fail when the checkpoint system cannot be initialized with an error message as shown in the following example:

```
"Failed to load prevayler under
APPTOP/11.1.7.0.0/orchestration/bin/../checkpoint/REL7/host_
name/PRIMORDIAL/DowntimePreFA/snapshot: Chunk header corrupted."
```

### Solution

Review he log file to ensure that there is no "out of disk space" exception. If there is no "out of disk space" exception, resume orchestration on the host where the failure occurred to continue the upgrade. If there is an "out of disk space" exception, ensure that there is enough disk space and then resume orchestration.

## 6.19.15 Upgrade JDK in a Freshly Provisioned Release 6 Environment

Perform the following steps to upgrade JDK only if you are upgrading from an Oracle Fusion Applications environment that was freshly provisioned in Release 6. If you upgraded to Release 6 from Release 5, you can skip this step.

1.  Set the following environment variables, in addition to those set in Section 2.1.13, "Set Environment Variables".

    ■   `UPGRADE_JDK_PATTERN`: The version to which you are upgrading. You can get this JDK version from *REPOSITORY_LOCATION*/jdk6.

    ■   `PREVIOUS_JDK_BACKUP_PATTERN`: The current version of JD. You can get this version from *APPLICATIONS_BASE*/jdk6.

- `JAVA_HOME`: The java home directory.

2. Run the following command from *REPOSITORY_LOCATION*/installers/farup/Disk1/upgrade/bin:

```
(UNIX) upgradeJDK.sh
(Windows) upgradeJDK.bat
```

3. Review the log files for upgradeJDK which are located in the *FA_ORACLE_HOME*/admin/FUSION/log/upgradeJDK directory.

### 6.19.16 Upgrade JDK in a Freshly Provisioned Release 6 Environment (AIX)

Perform the following steps to upgrade JDK only if you are upgrading from an Oracle Fusion Applications AIX environment that was freshly provisioned in Release 6. If you upgraded to Release 6 from Release 5, you can skip this step.

1. Set the following environment variables, in addition to those set in

   Section 2.1.13, "Set Environment Variables".

   - `UPGRADE_JDK_PATTERN`: The version to which you are upgrading. You can get this JDK version from *REPOSITORY_LOCATION*/jdk6 by running the following command:

     ```
     ./java -fullversion 2>&1 | cut -d " " -f 9
     ```

   - `PREVIOUS_JDK_BACKUP_PATTERN`: The current version of JDK. You can get this version from *APPLICATIONS_BASE*/jdk6. by running the following command:

     ```
     ./java -fullversion 2>&1 | cut -d " " -f 9
     ```

   - `JAVA_HOME`: The java home directory.

2. Run the following command from *REPOSITORY_LOCATION*/installers/farup/Disk1/upgrade/bin:

   ```
   (AIX) upgradeJDK.sh
   ```

3. Review the log files for upgradeJDK which are located in the *FA_ORACLE_HOME*/admin/FUSION/log/upgradeJDK directory.

### 6.19.17 Ignorable Errors Reported by catbundle.sql

The following ignorable errors may be encountered while running the catbundle.sql script or its rollback script:

ORA-29809: cannot drop an operator with dependent objects

ORA-29931: specified association does not exist

ORA-29830: operator does not exist

ORA-00942: table or view does not exist

ORA-00955: name is already used by an existing object

ORA-01430: column being added already exists in table

ORA-01432: public synonym to be dropped does not exist

ORA-01434: private synonym to be dropped does not exist

ORA-01435: user does not exist

ORA-01917: user or role 'XDB' does not exist

ORA-01920: user name '<user-name>' conflicts with another user or role name

ORA-01921: role name '<role name>' conflicts with another user or role name

ORA-01952: system privileges not granted to 'WKSYS'

ORA-02303: cannot drop or replace a type with type or table dependents

ORA-02443: Cannot drop constraint - nonexistent constraint

ORA-04043: object <object-name> does not exist

ORA-29832: cannot drop or replace an indextype with dependent indexes

ORA-29844: duplicate operator name specified

ORA-14452: attempt to create, alter or drop an index on temporary table already in use

ORA-06512: at line <line number>. If this error follow any of above errors, then can be safely ignored.

ORA-01927: cannot REVOKE privileges you did not grant

### 6.19.18 Performing Installation Verification Steps

Perform the steps in "Verifying Installation" in the "Common" chapter in the *Oracle Fusion Applications Post-Installation Guide*.

## 6.20 Platform Specific Troubleshooting Issues

This section contains troubleshooting information for platform specific issues.

### 6.20.1 SUSE Linux Troubleshooting Issues

This section contains troubleshooting information for the following issues on SUSE Linux.

#### 6.20.1.1 OS Support Check Fails

**Problem**

The following is error is reported when the GeneralSystemHealthChecks runs.

```
Plugin 'OsCheck': HC-OS-00002 : OS Support Check failed.Error(s):  OS version
is not supported(Check for OS name,arch and version support)
```

**Solution**

Back up the *FA_ORACLE_HOME*/lcm/hc/healthchecks.xml file. Then edit this file to replace all instances of "SLES 11.*::" with "SUSE Linux Enterprise Server 11.*::".

#### 6.20.1.2 HostsCheck Fails

**Problem**

The following error is reported when the GeneralSystemHealthChecks fails on HostsCheck:

```
[oracle.healthcheckplug] [tid: 10] [ecid: ] Plugin 'HostsCheck':
HC-COMMON-00001 :Unable to perform the check: java.io.FileNotFoundException:
/etc/sysconfig/network (Is a directory)
```

Review log files for additional details to take an appropriate corrective
action(Hosts Name)

**Solution**

You can ignore this error and proceed with the upgrade.

## 6.20.2 Windows Troubleshooting Issues

This section contains troubleshooting information for the following issues on
Windows:

- DowntimePostFA Phase Fails in RemoveConflictingPatches Task
- Upgrade JDK Fails
- Update Impersonation Configuration Fails

### 6.20.2.1 DowntimePostFA Phase Fails in RemoveConflictingPatches Task

**Problem**

The `DowntimePostFA` phase of orchestration fails during the
`RemoveConflictingPatches` task on Windows with the following error:

```
RollbackSession rolling back interim patch '16569379' from OH
'c:\AT\webtier_mwhome\webtier'
Prerequisite check "CheckActiveFilesAndExecutables" failed. The details are:

Following files are active :
c:\AT\webtier_mwhome\webtier\bin\yod.dll
```

**Solution**

The cause of the failure is that the OPMN processes that is running from the BI and
GOP homes are using this `dll`. When this failure occurs, shut down the OPMN and
the OPMN-managed processes using the respective services. After making sure that
the OPMN processes are down, restart orchestration. After orchestration succeeds,
bring up the OPMN processes by using the respective services.

### 6.20.2.2 Upgrade JDK Fails

**Problem**

Upgrade JDK fails with the following error:

```
Upgrade JDK plugin command:
C:\R\installers\farup\Disk1\upgrade\bin\upgradeJDK.bat
--apptop C:\AT --repo
C:\R
[2013-07-02T14:24:34.566-06:00] [orchestration] [NOTIFICATION] []
[oracle.orchestration] [tid: 12]
[ecid: 0000JyWzVIIFW7HpIsDCif1HonA^000003,0]

Tue 07/02/2013 14:24:34.56 upgradeJDK BEGIN
[2013-07-02T14:24:34.582-06:00] [orchestration] [NOTIFICATION] []
[oracle.orchestration] [tid: 12]
[ecid: 0000JyWzVIIFW7HpIsDCif1HonA^000003,0]

Tue 07/02/2013 14:24:34.57 Output logged to file
C:\AT\fusionapps\applications\admin\FUSION\log\upgradeJDK\upgradeJDK_14243455. log
 [2013-07-02T14:24:34.610-06:00] [orchestration] [NOTIFICATION] []
```

**Solution**

Set the following environment variables:

```
set APPLICATIONS_BASE=APPLICATIONS_BASE LOCATION>
set REPOSITORY_LOCATION=C:\SHARED\11.1.7.0.0\Repository
```

Then in the same command prompt, start orchestration on the primordial node.

### 6.20.2.3 Update Impersonation Configuration Fails

**Problem**

The **Update Impersonation Configuration** configuration assistant fails on Windows.

**Solution**

Relaunch orchestration so the configuration assistant for Update Impersonation Configuration reruns.

# A

# Additional Information About Upgrade Orchestrator

This appendix provides additional information about Upgrade Orchestrator.

This appendix includes the following topics:

- Additional Information About Upgrade Orchestrator Commands
- Utilities Run by Upgrade Orchestrator

## A.1 Additional Information About Upgrade Orchestrator Commands

This section provides additional information about Upgrade Orchestrator commands. The following topics are included:

- Upgrade Orchestrator Command Arguments
- Options for the Orchestration Command When Starting Orchestration
- Options for the Orchestration updateStatus Command
- Options for the Orchestration getStatus Command
- The validatesetup Argument

### A.1.1 Upgrade Orchestrator Command Arguments

The following command arguments are available for the orchestration command to retrieve information about the status of the upgrade as well as manage the status.

- Use `updateStatus` to update the status for a specific task to either SUCCESS or FAILURE. For more information, see Section A.1.3, "Options for the Orchestration updateStatus Command."
- Use `getStatus` to retrieve the status of a specific task as well as the summary of the upgrade on a specific `POD_NAME` and `host_type` while Upgrade Orchestrator is running. For more information, see Section A.1.4, "Options for the Orchestration getStatus Command" and Section 6.3, "Monitoring Upgrade Orchestration Progress."
- Use `exitOrchestration` to terminate orchestration gracefully on all hosts on a specific pod. For more information, see Section 6.4, "Terminate Upgrade Orchestration."
- Use `clearExitOrchestration` to clear the exit status on all hosts. For more information, see Section 6.4, "Terminate Upgrade Orchestration."

- Use `getExitOrchestrationStatus` to retrieve the status of the `exitOrchestration` command.

- Use `validateSetup` to validate the shared location status and permissions. This validation is implicitly run when any of the orchestration command options are run. For more information, see Section A.1.5, "The validatesetup Argument."

## A.1.2 Options for the Orchestration Command When Starting Orchestration

The following table provides a description of the options available when using the orchestration command to start Upgrade Orchestrator.

*Table A–1    Options for the orchestration.sh command*

| Name | Mandatory | Description |
|------|-----------|-------------|
| -pod | Yes | The value of *POD_NAME* refers to the directory you created in Step 3, Section 2.4.1, "Set Up Upgrade Orchestrator on a Shared Location". |
| -hosttype | Yes | The host type. Valid values are PRIMORDIAL, MIDTIER, OHS, and IDM. For more information see Section 1.2.1, "Host Types". |
| -release | No | The release name, for example, REL5-7 or REL7. If this option is not used, all releases defined in the manifest file are executed. |
| -phase | No | Only the `PreDowntime` phase can be specified in the command line when running orchestration. |
| -checkpoint | No | Valid values are true or false. If set to false, ignore the checkpoint results and rerun. The default value is true. |
| -DlogLevel | No | The log level. Valid values are SEVERE, WARNING, INFO, CONFIG, FINE, FINER and FINEST. The default value is INFO. Note that error messages are displayed on the console for database component failures if you set the `-DlogLevel` option to FINEST. |
| -v | No | Displays the product version and exits. |
| -h | No | Displays help information and exits. |

## A.1.3 Options for the Orchestration updateStatus Command

The following table provides a description of the available options when using the orchestration command to update the status of orchestration tasks.

*Table A–2    Options for orchestration.sh updateStatus command*

| Name | Mandatory | Description |
|------|-----------|-------------|
| updateStatus | Do not use with `getStatus` | Updates the status of the selected task. |
| -pod | Yes | The name of the pod to be searched. |
| -hosttype | Yes | The host type. Valid values are: PRIMORDIAL, MIDTIER, OHS, and IDM. |
| -hostname | Yes | Host name, including domain details. |
| -release | Yes | The release name, for example, REL5-7 or REL7. If this option is not used, all releases defined in the manifest file are executed. |

*Table A–2   (Cont.)  Options for orchestration.sh updateStatus command*

| Name | Mandatory | Description |
|---|---|---|
| -phase | Yes | The phase name. Valid values are: `PreDowntime`, `DowntimePreFA`, `DowntimeDuringFA`, `DowntimePostFA`, `DowntimeDuringLP`, `DowntimePostLP`. |
| -taskid | Yes | Orchestration `task_id` that is to be updated. |
| -taskstatus | Yes | Orchestration task status. Valid values are `success` and `error`. |
| -v | No | Displays the product version and exits. |
| -h | No | Displays help information and exits. |

## A.1.4  Options for the Orchestration getStatus Command

The following table provides a description of the available options when using the orchestration command to get the status of an orchestration session.

*Table A–3    Options for orchestration.sh getStatus command*

| Name | Mandatory | Description |
|---|---|---|
| getStatus | Do not use with `updateStatus` | Retrieves the checkpoint status from the selected orchestration task. |
| -pod | Yes | The name of the pod to be searched. |
| -hosttype | Yes | The host type. Valid values are: PRIMORDIAL, MIDTIER, OHS, and IDM. |
| -hostname | Yes | Host name, including domain details. |
| -release | Yes | The release name, for example, REL5-7 or REL7. If this option is not used, all releases defined in the manifest file are queries. |
| -phase | No | You can specify the following phase names to see the status for the specific phase: `PreDowntime`, `DowntimePreFA`, `DowntimeDuringFA`, `DowntimePostFA`, `DowntimeDuringLP`, `DowntimePostLP`. |
| -taskid | No | The Orchestration `task_id` that is to be searched. If this option is used, the status for the specific task is returned. |
| -taskstatus | No | The Orchestration task status. Valid values are `success` and `error`. If this option is used, a list of all tasks that match the status is returned. |
| -v | No | Displays the product version and exits. |
| -h | No | Displays help information and exits. |

## A.1.5  The validatesetup Argument

If you run the `orchestration.sh` command with the `validatesetup` argument, the following validations occur:

- Validating SHARED_UPGRADE_LOCATION

  Successfully validated permissions of shared folder.

- Validating ORCHESTRATION_CHECKPOINT_LOCATION

  Successfully validated permissions of shared folder.

- Validating ORCHESTRATION_CHECKPOINT_ARCHIVE_LOCATION

Successfully validated permissions of shared folder.

These options are implicitly run when any of the orchestration commands run.

## A.2  Utilities Run by Upgrade Orchestrator

This section describes the utilities that are run by Upgrade Orchestrator. This is for your information only and no action is needed.The following utilities are included:

- RUP Installer
- Health Checker Utility
- RUP Lite for OVM Utility
- RUP Lite for OHS Utility
- RUP Lite for BI Utility

### A.2.1  RUP Installer

During the installation phase, RUP Installer copies all files for 11*g* Release 7 (11.1.7) to the appropriate locations, such as Oracle Fusion Middleware home and Oracle Fusion Applications Oracle home. After the file copy completes, RUP Installer calls its first installer to update Oracle Fusion Applications Patch Manager and apply Oracle Fusion Middleware patches. When the first installer completes successfully, RUP Installer calls the second installer, which performs the Policy Store Analysis. Upon successful completion of the Policy Store Analysis, RUP Installer calls Configuration Assistants to perform the remaining tasks required to update and deploy artifacts to Oracle Fusion Applications. Depending on the contents of 11*g* Release 7 (11.1.7), not all configuration assistants may run.

#### A.2.1.1  RUP Installer Configuration Assistants

All mandatory configuration assistants must complete successfully before proceeding to the next configuration assistant.

If any tasks fail during the installation phase, refer to Section 6.8, "Troubleshooting Failures During the Installation Phase" for more information.

The following table provides a list of configuration assistants that the first installer runs. The Retry Behavior and Troubleshooting column describes what RUP Installer does after a configuration assistant fails, you resolve the cause of the failure, and then resume orchestration. If available, links are provided to relevant troubleshooting sections.

***Table A–4  Configuration Assistants Run by Oracle Fusion Applications 11g Release 7 (11.1.7) RUP Installer Part 1 of 2***

| Name | Mand atory | Description | Retry Behavior and Troubleshooting |
|------|------------|-------------|-------------------------------------|
| Configure Patch Manager | Yes | Configures Oracle Fusion Applications Patch Manager. | Starts from the beginning of the task. |
| Consolidate Repository And Downloaded Patches | Yes | Consolidates patches in the repository and the patches you download in Section 2.3.6.3, "Download and Unzip Mandatory Post-Release 7 Patches". | Starts from the beginning of the task. |
| Update Patch Manager | Yes | Applies Patch Manager Patches | Applies failed patches. |

*Table A–4   (Cont.)  Configuration Assistants Run by Oracle Fusion Applications 11g Release 7 (11.1.7) RUP Installer Part 1 of 2*

| Name | Mandatory | Description | Retry Behavior and Troubleshooting |
|------|-----------|-------------|-------------------------------------|
| Reconfigure Patch Manager | Yes | Reconfigures Oracle Fusion Applications Patch Manager. | Starts from the beginning of the task. |
| Bootstrap Patch Manager | Yes | Updates the data model for Oracle Fusion Applications Patch Manager by running the `fapmgr bootstrap` command. | Starts from the beginning of the task. See Section 6.19.5, "Troubleshooting Bootstrapping Patch Manager". |
| Create Middleware Schemas | Yes | Creates Oracle Fusion Middleware schemas | Starts from the beginning of the task. |
| Apply Middleware Patch Sets | Yes | Applies Oracle Fusion Middleware patch sets, which can include upgrades, schema changes and installers. For more information, see Section A.2.1.1.1, "Middleware Installers Invoked by the Apply Middleware Patch Sets Configuration Assistant". | Installs failed patch sets. |
| Apply Pre-PSA Middleware Patches | Yes | Applies Pre-PSA Middleware Patches<br><br>For more information, see Section A.2.1.1.2, "Patches Not Supported by the Apply Pre-PSA and Post-PSA Middleware Patches Configuration Assistants". | Applies the failed patches. See Section 6.12, "Troubleshooting Applying Middleware Patches". |
| Verify Middleware PSA Schema Credentials | Yes | Verifies users and logins for schemas. | Starts from the beginning of the task. |
| Upgrade Middleware Schemas | Yes | Runs Oracle Fusion Middleware patch set assistants (PSA). | Runs failed tasks. See Section 6.12.5, "Troubleshooting Upgrading Middleware Schema". |
| Apply Post-PSA Middleware Patches | Yes | Applies Post-PSA Middleware Patches<br><br>See Section A.2.1.1.2, "Patches Not Supported by the Apply Pre-PSA and Post-PSA Middleware Patches Configuration Assistants". | Applies the failed patches. See Section 6.12, "Troubleshooting Applying Middleware Patches". |
| Restore Default Context in `JPS-CONFIG-JSE.XML` Files | Yes | Restores default context. | Checks if file is corrupted and replaces the file with a well formed XML file and Re-Try. |
| Upgrade OPSS | Yes | Upgrades the Policy Store. | Starts from the beginning of the task. |
| Extend Certificate Validity | Yes | Extends certificate validity by three years from the date of the upgrade. | Starts from the beginning of the task. |

*Table A–4    (Cont.) Configuration Assistants Run by Oracle Fusion Applications 11g Release 7 (11.1.7) RUP Installer Part 1 of 2*

| Name | Mandatory | Description | Retry Behavior and Troubleshooting |
|---|---|---|---|
| Deploy Middleware Policies (jazn-data.xml) | Yes | Deploys Middleware policies. | Starts from the beginning of the task and includes the clean up required. |
| Apply Offline BI Metadata and Configuration Updates | Yes | Performs the deployment of the updated applications policies for Oracle Business Intelligence. | Retries failed steps. |
| Apply ESSAPP Code Source Grant Changes | Yes | Adds code source grants to support auditing. | Starts from the beginning of the task. |
| Apply Domain Configuration | Yes | Applies startup parameter changes and configures `datasource` for audit service. | Retries failed steps. |
| Propagate Domain Configuration | Yes | Unzips RUP Lite for Domain Configuration into `APPLICATIONS_CONFIG`/lcm/admin/`version`/fapatch/ru plitedomain. Updates properties in the RUP Lite env.properties file and prepares RUP Lite so you can run RUP Lite for Domain Configuration. | Starts from the beginning of the task. See Section 6.19.6, "Troubleshooting Failures During Propagating Domain Configuration". |

The following table provides a list of configuration assistants that the second installer runs. The Retry Behavior and Troubleshooting column describes what RUP Installer does after a configuration assistant fails, you resolve the failure, and then resume orchestration. If available, links are provided to relevant troubleshooting sections. The second installer supports parallel processing of certain configuration assistants, which run in groups. For more information, see Section A.2.1.2.7, "Parallel Configuration Assistants".

*Table A–5    Configuration Assistants Run by Oracle Fusion Applications 11g Release 7 (11.1.7) RUP Installer Part 2 of 2*

| Name | Mandatory | Description | Retry Behavior and Troubleshooting |
|---|---|---|---|
| Configure Patch Manager | Yes | Configures Oracle Fusion Applications Patch Manager. | Starts from the beginning of the task. |
| Bootstrap Patch Manager | Yes | Updates the data model for Oracle Fusion Applications Patch Manager by running the fapmgr `bootstrap` command. | Starts from the beginning of the task. See Section 6.19.5, "Troubleshooting Bootstrapping Patch Manager". |
| Offline Preverification Pre Database Content Upload | Yes | Performs the following validation checks while all servers are shut down:<br>■ Policy Store<br>■ Number of database workers<br>■ Database Content Upload<br>■ Oracle Data Integrator (ODI) | Runs failed steps. |

*Table A–5   (Cont.)  Configuration Assistants Run by Oracle Fusion Applications 11g Release 7 (11.1.7) RUP Installer Part 2 of 2*

| Name | Mandatory | Description | Retry Behavior and Troubleshooting |
|---|---|---|---|
| Grant Privileges to Application Schemas | Yes | Grants system privileges to database users and creates base object privileges. | Runs the failed script. |
| Load Database Components | Yes | Uploads the database content packaged in 11*g* Release 7 (11.1.7) to the database, such as database objects, seed data, and package headers and bodies. | Runs failed database commands. See Section 6.13, "Troubleshooting Loading Database Components". |
| Deploy Applications Policies (jazn-data.xml) | Yes | Deploys updated applications policies, based on your selections during the Policy Store Analysis configuration assistant. | Deploys the failed stripes. See Section 6.14, "Troubleshooting Deployment of Applications Policies". |
| Deploy BI Publisher Artifacts | Yes | Using Catalog Manager, performs the following steps:<br><br>■ Backs up BI Presentation Catalog under *APPLICATIONS_ CONFIG*/lcm/admin/*version*/fapatch /BIP/*language_code* for example, *APPLICATIONS_ CONFIG*/lcm/admin/11.1.7.0.0/fapa tch/BIP/en_US/webcat.zip.<br><br>■ Backs up captions under *APPLICATIONS_ CONFIG*/lcm/admin/*version*/fapatch /BIP/*language_code*/captions.zip.<br><br>■ Copies captions to the Oracle Business Intelligence repository.<br><br>■ Deploys BI Presentation Catalog to the Oracle Business Intelligence repository. | Starts from the beginning of the task. See Section 6.19.8, "Troubleshooting Deployment of BI Publisher Artifacts". |
| Import Oracle Data Integrator Repositories | Yes | ■ Imports ODI topology.<br>■ Imports ODI model folders.<br>■ Imports ODI models.<br>■ Imports ODI projects.<br>■ Drops ODI error tables. | Imports failed data. |
| Create Grants/Synonym s on Application Database Objects | Yes | Creates synonyms between database objects and grants object privileges to database users. | Runs the failed script. |
| Offline Preverification Post Database Content Upload | Yes | Validate Host and Port for New Managed Servers. | Starts from the beginning of the task. |
| Deploy Data Security Grants | Yes | Performs GUID reconciliation in LDAP. | Starts from the beginning of the task. |
| Generate SOA Configuration Plan | Yes | Generates the configuration plan to be used for deploying SOA composites. | Starts from the beginning of the task. |

*Table A–5   (Cont.)  Configuration Assistants Run by Oracle Fusion Applications 11g Release 7 (11.1.7) RUP Installer Part 2 of 2*

| Name | Mandatory | Description | Retry Behavior and Troubleshooting |
|---|---|---|---|
| Update Flexfield Configuration | Yes | Updates the `FndSetup` application for supporting new flexfields, new flexfield usages, and flexfield view links added by Oracle Fusion Application products. | Starts from the beginning of the task. |
| Configure New Managed Servers | Yes | Configures managed servers for new applications to be associated with the first non-admin host by default. | Reapplies failed managed server templates. |
| Deploy New Applications | Yes | Deploys new applications using domain extension templates. | Reapplies failed domain extension templates. |
| Generate ADF Domain Configuration Plan | Yes | Generates Oracle ADF domain configuration in Metadata Service (MDS) to be used by Expression Language (EL) expressions in `connections.xml`. | Starts from the beginning of the task. |
| Apply Offline Setting Changes | Yes | Applies Oracle Fusion Applications environment configuration setting changes while all servers are shut down. | Retries failed domains. |
| Verify Node Manager and OPMN Status | Yes | Verifies the following processes:<br>■ Node Managers<br>■ BI OPMN Processes<br>■ GOP OPMN Processes<br>■ Web Tier OPMN Processes<br>You must not exit out of RUP Installer during this configuration assistant. | Runs failed steps. See Section 6.9.3, "Troubleshooting Failure During Verifying Node Manager and OPMN Status". |
| Start All Admin Servers | No | Starts all Administration Servers. | Restarts failed Administration Servers. See Section 6.15, "Troubleshooting Server Start and Stop Failures". |
| Configure DB Persistence Store for JMS/TLogs | Yes | Configures SOA and UMS to store JMS and TLogs content in the database instead of the file system. | Retries failed plug-ins. |
| Configure OPSS Keystore Service | Yes | Configures OPSS to be used for remote task flow Keystore Service. | Starts from the beginning of the task. |
| Deploying LDAP Data (LDIF) | No | Loads new enterprise roles. | Retries to load the failed LDIF files. |
| Create Fusion APPIDs | Yes | Creates Fusion APPID users and groups in the LDAP server and credentials for those users in the credential store. | Starts from the beginning of the task. |
| Apply Admin Server Online Setting Changes | Yes | Applies Oracle Fusion Applications environment configuration setting changes that are applicable to the Administration Servers. | Starts from the beginning of the task. |
| Start Minimal Servers for Configuration Updates | Yes | Starts minimal managed servers required to run the necessary configuration assistants successfully. | Starts from the beginning of the task. |

*Table A–5   (Cont.)  Configuration Assistants Run by Oracle Fusion Applications 11g Release 7 (11.1.7) RUP Installer Part 2 of 2*

| Name | Mandatory | Description | Retry Behavior and Troubleshooting |
|---|---|---|---|
| Apply UCM Configuration | Yes | Configures UCM to store content in the database instead of the file system. | Starts from the beginning of the task. |
| Apply WebCenter Connection Changes | Yes | ■  Replaces `WebCenter-UCM` Connection with `FusionAppsContentRepository` Connection<br>■  Updates Connection References | Retries failed plug-ins. |
| Configure Trust Asserter | Yes | Configures trust asserter to be used for remote task flow Keystore Service. | Starts from the beginning of the task. |
| Start All Servers | No | Starts all servers in all domains, including the BI servers. Also performs the `opmnctl` start for Oracle HTTP Server (OHS) and `BIInstance`. | Restarts failed servers. See Section 6.15, "Troubleshooting Server Start and Stop Failures". |
| Online Preverification | Yes | Performs steps described in see Section A.2.1.1.3, "Steps Performed During Online Preverification". | Runs failed steps. See Section 6.15.4, "EditTimedOutException Error During Online Preverification". |
| Upgrade ADF Metadata | No | Upgrades ADF related metadata. | Retries failed domains. |
| Generate OHS Reference Configuration File | No | Generates OHS configuration files for installed product families in the directory, `APPLICATIONS_CONFIG`/lcm/admin/`version`/fapatch/OHS/patched_moduleconf. | Starts from the beginning of the task. |
| Apply OWSM Configuration | Yes | Upgrades Oracle Web Services Manager (Oracle WSM) policies after backing up the policies. | Restores the backup of the policies and starts from the beginning of the task. |
| Deploy SPE Inline Service Artifacts | No | Deploys SPE Inline Service Artifacts. | Retries the deployment. |
| Deploy Data Role (RGX) Templates | No | Deploys RGX Template artifacts to the Common Domain. | Deploys failed templates. |
| Apply OAM Configuration | No | Applies changes to the Oracle Access Manager (OAM) configuration. | Starts from the beginning of the task. See Section 6.11.4, "Location of GRC Policies in the OAM Applications Domain". |
| Deploy Flexfields | No | Deploys flexfields to the domain that hosts the `FndSetup` application. | Starts from the beginning of the task. |

*Table A–5   (Cont.)  Configuration Assistants Run by Oracle Fusion Applications 11g Release 7 (11.1.7) RUP Installer Part 2 of 2*

| Name | Mandatory | Description | Retry Behavior and Troubleshooting |
|---|---|---|---|
| Apply Online BI Metadata and Configuration Updates | Yes | Applies Oracle Business Intelligence Metadata updates. | Starts from the beginning of the task. If you made any customizations to the Oracle BI Repository, the Oracle BI Presentation Catalog, or JAZN settings related to Oracle Business Intelligence, you must merge your changes. See Section 5.11, "Resolve Conflicts That Occurred During Oracle BI Metadata Updates". |
| Import Group Space Templates | No | Imports Group Space Templates. | Deploys failed templates. |
| SOA Preverification | Yes | Performs the steps described in Section A.2.1.1.4, "Steps Performed During SOA Preverification". If you have customizations, you must merge them during this configuration assistant. | Retries failed steps. See Section 6.16.6, "Merging SOA Composite JDeveloper Customizations During SOA Preverification". |
| Apply SES Configuration Changes | No | Updates additional configuration updates to Oracle Secure Enterprise Search (SES) running on the Common Domain. | Starts from the beginning of the task. |
| Remove UCM SES Objects | No | | |
| Deploy BPM Templates | No | Deploys BPM Templates to the MDS repository. | Deploys failed templates. |
| Deploy B2B Metadata | No | Deploys B2B Metadata. | Deploys failed B2B artifacts. |
| Deploy SOA Shared Repository | Yes | Deploys SOA shared repository artifacts to the SOA servers available in the environment. | Deploys failed SOA shared repository artifacts. |
| Deploy UpdateSOAMDS Composite | No | Deploys the `UpdateSOAMDS` composite to every domain. | Deploys composite on domains that failed. |
| Deploy SOA Composites | No | Deploys SOA composites to the corresponding SOA servers and performs server management steps. | Deploys failed SOA composites. See Section 6.16, "Troubleshooting SOA Composite Deployment Failures". |
| Deploy SOA Resource Bundles | Yes | Deploys SOA Resource Bundles to the corresponding SOA servers. | Deploys failed SOA resource bundles. |

*Table A–5 (Cont.) Configuration Assistants Run by Oracle Fusion Applications 11g Release 7 (11.1.7) RUP Installer Part 2 of 2*

| Name | Mandatory | Description | Retry Behavior and Troubleshooting |
|------|-----------|-------------|-------------------------------------|
| Import Image Routing (IPM) Artifacts | No | Deploys IPM artifacts to the IPM server. | Retries failed IPM artifacts. See Section 6.19.10, "Failure During IPM Import". |
| Restart All SOA Servers | Yes | Restarts all SOA servers in the environment. | Starts at the beginning of the task. |
| Apply Online Setting Changes | No | Applies Oracle Fusion Applications environment configuration setting changes during the online phase. | Starts from the failed task. |
| Generate RUP Lite for OHS | No | Generates the zip file that contains all files needed by RUP Lite for OHS to upgrade OHS. | Starts at the beginning of the task. |
| Apply Downloaded Oracle Fusion Applications Patches | Yes | Applies the Oracle Fusion Applications patches that you downloaded in Section 2.3.6.3, "Download and Unzip Mandatory Post-Release 7 Patches". | Applies failed patches. |
| Post Configuration | No | ■ Reactivates SES Index Optimization<br>■ Reactivates ESS Server from inactive or quiescent mode<br>■ Deletes wallets | Retries failed domains. |

**A.2.1.1.1 Middleware Installers Invoked by the Apply Middleware Patch Sets Configuration Assistant** The following installers are invoked by the **Apply Middleware Patch Sets** configuration assistant:

- Oracle Business Intelligence
- Oracle Common
- Oracle Data Integrator (ODI)
- Oracle Database Client
- Oracle Enterprise Content Management
- Oracle HTTP Server (OHS) - OHS may be installed either beside the rest of the Oracle Fusion Middleware in the Oracle Fusion Applications middle tier or on a separate DMZ machine. For either case, patching OHS requires running RUP Lite for OHS.
- Oracle Fusion Middleware Extensions for Applications
- Oracle Global Order Promising
- Oracle Identity Management (IDMUTIL)
- Oracle Secure Enterprise Search (SES)
- Oracle SOA Suite
- Oracle Social Networking (OSN)
- Oracle WebCenter Suite
- Oracle WebLogic Server

■ Oracle Web Tier

**A.2.1.1.2   Patches Not Supported by the Apply Pre-PSA and Post-PSA Middleware Patches Configuration Assistants** The following patches are not supported by these configuration assistants:

■ Integrated Development Environment (IDE)

■ OHS installed in the DMZ: Installed by RUP Lite for OHS.

■ Database Server: You patch your Database Server using RUP Lite for RDBMS. For more information, see Chapter 3, "Updating the Oracle Fusion Applications and Oracle Identity Management Databases".

■ Oracle Identity Management Server: You patch your IDM server by following the steps in Section 4.4.4, "Upgrade Oracle Identity Management Domain to 11g Release 6 (11.1.6)" and Section 4.4.5, "Upgrade Oracle Identity Management Domain to 11g Release 7 (11.1.7)".

**A.2.1.1.3   Steps Performed During Online Preverification** The following validation steps are performed during the **Online Preverification** configuration assistant, if Release 7 (11.1.7) contains artifacts related to the validation:

■ Taxonomy URL

■ Database validation

■ Flexfield: Checks for the `HelpPortal` Managed Server in the Common Domain and for the successful deployment of the `FndSetup` application.

■ OAM Configuration

■ SES Admin Server URL

■ SPE Inline Service: Checks if the Oracle CRM Performance application is deployed. If it is, the OracleRTD application must be deployed and at least one BI server must be running where the OracleRTD application is deployed.

■ Data Role (RGX) Template: Checks if the Administration Server for the Common Domain is up.

■ Group Space Template: Checks if the following Managed Servers are up: `WC_Spaces`, `WC_Collaboration`, `ucm_server1`.

■ Oracle WSM validation

**A.2.1.1.4   Steps Performed During SOA Preverification** The following validation steps are performed during the **SOA Preverification** configuration assistant:

■ Business Process Management (BPM) Template

■ B2B Metadata: Checks if the Common Domain, SOA Managed Server, and the LDAP Server are up.

■ SOA Shared Repository: Verifies the taxonomy, checks if the Administration Server is up, and checks for SOA_SERVER and SOA_PLATFORM readiness.

■ `UpdateSOAMDS` SOA Composite: Verifies the taxonomy, checks if the Administration Server is up, and if the SOA platform is ready.

■ SOA Resource Bundle: Verifies the taxonomy, checks if the Administration Server is up, and if the SOA platform is ready.

■ SOA Composites: Performs the following validation steps:

- Verifies the taxonomy.

- Checks if the Administration Server is up.

- Checks if the SOA platform is ready.

- Checks if the base composite is deployed.

- Checks if the default revision is deployed.

- Checks if the new revision is not deployed.

- Checks whether the SOA composites that will be affected by the upgrade contain JDeveloper customizations. For more information, see Section 6.16.6, "Merging SOA Composite JDeveloper Customizations During SOA Preverification".

- Image Routing (IPM): Checks if the IPM server is up.

### A.2.1.2  Installer User Interface

RUP Installer and Language Pack Installer provide a graphical user interface which allows you to control the behavior of the installer by the use of buttons, in cases where it encounters a failure. Note that the behavior of these buttons may vary, depending on whether it is a configuration assistant, or a step within a configuration assistant, that fails. The behavior also depends on whether a configuration assistant is mandatory. All mandatory configuration assistants must complete successfully before proceeding to the next configuration assistant. For information about which configuration assistants are mandatory, see Section A.2.1.1, "RUP Installer Configuration Assistants".

You can exit out of the installer in the event of a failure and restart from the point of failure. If a non-mandatory configuration assistant fails, and you continue to the next configuration assistant, you must restart the installer after it finishes the last configuration assistant. When you restart, the installer retries all failed configuration assistants and steps.

An explanation of the usage of each button follows. Note that the buttons are available only in GUI mode, not in silent mode. For information about how to use the buttons during parallel processing of certain configuration assistants, see Section A.2.1.2.7, "Parallel Configuration Assistants".

**A.2.1.2.1   Abort Button**  The **Abort** button allows you to skip a failed configuration assistant or step within a configuration assistant, and records the failure so it can be rerun when you restart the installation. For mandatory configuration assistants, after you abort the configuration assistant, the installer does not proceed and only the **Cancel** button is enabled. You must then resolve the cause of the failure and start the installer from this failure point. For non-mandatory configuration assistants, the installer proceeds to the next configuration assistant after you abort the configuration assistant. This button is enabled only after a failure.

**A.2.1.2.2   Cancel Button**  The **Cancel** button allows you to stop an installer session after the failure of a mandatory action. This button is enabled only after a failure.

**A.2.1.2.3   Close Button**  The Windows **Close** button allows you to stop an installer session after a failure. This is enabled only after a failure.

**A.2.1.2.4   Continue Button**  The **Continue** button allows you to skip a failed non-mandatory step within any configuration assistant The installer records the failure and then proceeds with the next step within the configuration assistant. When you

rerun this installer session, the failed steps within the configuration assistant are attempted again.

Note that this button is enabled only for non-mandatory steps within a configuration assistant.

**A.2.1.2.5  Next Button**  The **Next** button allows you to proceed to the next screen. This button is enabled only when all configuration assistants complete successfully in the current screen.

**A.2.1.2.6  Retry Button**  The **Retry** button allows you to attempt to rerun a failed configuration assistant, or a step within a configuration assistant. Use **Retry** when you know the cause of the failure and can resolve the issue during the current RUP Installer session.

**A.2.1.2.7  Parallel Configuration Assistants**  RUP Installer and Language Pack Installer support parallel processing of certain configuration assistants to improve performance. Parallel configuration assistants are organized by groups and all configuration assistants in a group start running at the same time. The installer proceeds to the next configuration assistant outside of the group, only after all parallel tasks in a group complete successfully. The following example depicts a group of configuration tasks that are running in parallel. As depicted in the following graphic, a group of configuration tasks, **Deploying Security Grants**, **Generating SOA Configuration Plan**, and **Updating Flexfield Configuration**, are running in parallel and have all reached 10% completion.
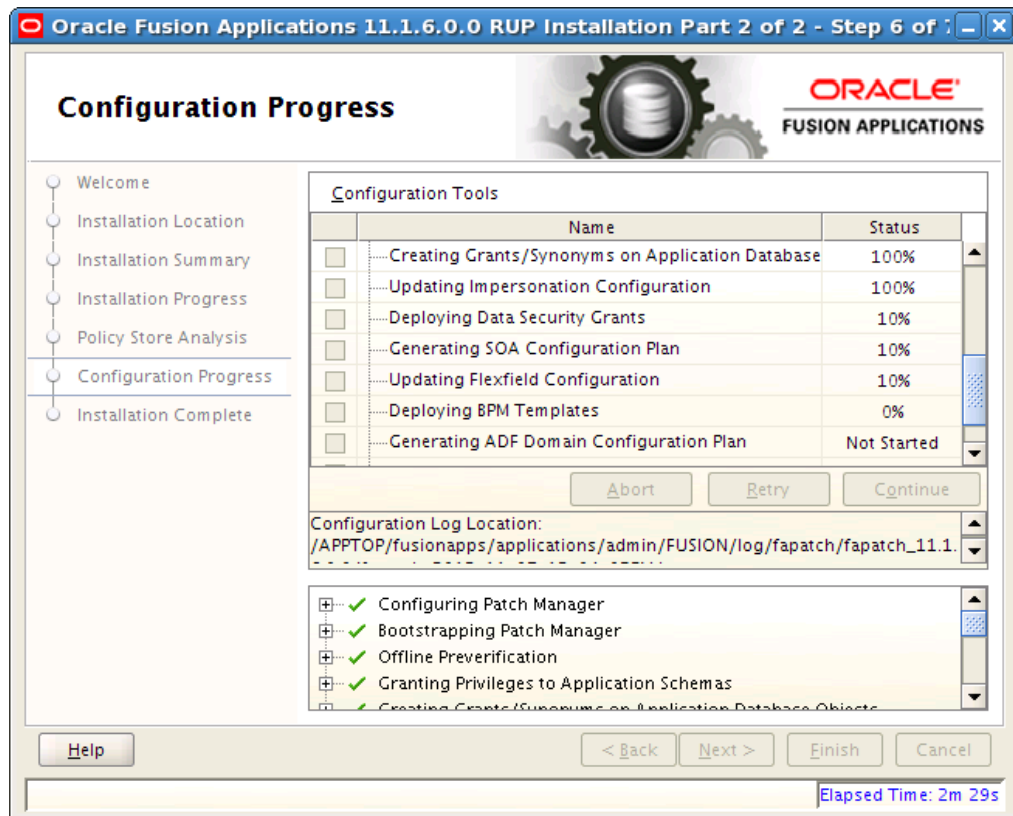
## A.2.2 Health Checker Utility

Health Checker is a command line utility that performs a set of validation checks against an Oracle Fusion Applications environment. The validation checks are organized into groups, based on the purpose of the checks and when the checks are performed. When Health Checker runs, it uses a specific manifest file which performs the appropriate checks. Several health checks are called by Upgrade Orchestrator and all health checks can also be run manually. Health Checker provides a list of corrective actions for the checks that fail validation. The suggested corrective actions must be run manually to fix the issue before proceeding with the related activity, such as upgrading or patching activities.

Note that you should not run the Health Checker manifests that are located in the *FA_ORACLE_HOME*/lcm/hc/config/SaaS directory. If manifests in this directory are run, unexpected failures in the environment may occur.

The following topics describe the usage of Health Checker:

- Health Checker Manifests

- Set Up Health Checker on the DB and OHS Hosts

- How to Run Health Checker

- Troubleshoot Health Checker Failures

- Health Checker Plug-ins

- Health Checks: Overrides

### A.2.2.1 Health Checker Manifests

When you run Health Checker manually, you specify a manifest file which corresponds to the group, as described in Table A–6. The manifest files are located in the following directories:

- Before upgrading your environment, the manifest files in the following location are from the previous release. Do not use these manifest files until after you upgrade:

  *FA_ORACLE_HOME*/lcm/hc/config:

- The manifest files in the following location are from the current release and must be used when running Health Checker before the upgrade:

  *REPOSITORY_LOCATION*/installers/farup/Disk1/upgrade/config

*Table A–6    Health Checker Manifest Files*

| Manifest File | Host Requirements | Typical Usage of the Manifest |
|---|---|---|
| GeneralSystemHealthChecks.xml | Primordial, OHS, Midtier, DB | Run this manifest any time. See Section A.2.2.5.1, "General System Health Checks." |
| PreDowntimeUpgradeReadinessHealthChecks.xml | Primordial, OHS, Midtier, DB | Upgrade Orchestrator runs this manifest before the upgrade downtime. You can run this at any time. See Section A.2.2.5.2, "Pre-Down Time Upgrade Tasks." |

*Table A–6   (Cont.)  Health Checker Manifest Files*

| Manifest File | Host Requirements | Typical Usage of the Manifest |
|---|---|---|
| Release5to7PreUpgradeReadinessChecks.xml | Primordial, OHS, Midtier, DB | Upgrade Orchestrator runs this manifest during down time and before the upgrade starts, when performing the chained upgrade from Release 5 to Release 6 to Release 7. See Section A.2.2.5.3, "Pre-Upgrade Tasks Performed by Health Checker During Down Time." This manifest must be run only on the Release 5 environment and the *REPOSITORY_LOCATION* environment variable must point to the Release 7 Repository. |
| DuringDowntimeUpgradeReadinessHealthChecks.xml | Primordial, OHS, Midtier | Upgrade Orchestrator runs this manifest during down time and before the upgrade starts. See Section A.2.2.5.3, "Pre-Upgrade Tasks Performed by Health Checker During Down Time." |
| VitalSignsChecks.xml | | Upgrade Orchestrator runs this manifest during the upgrade. See Section A.2.2.5.10, "Vital Signs Check." |
| PostUpgradeHealthChecks.xml | Primordial, OHS, Midtier | Upgrade Orchestrator runs this manifest after the upgrade. See Section A.2.2.5.4, "Post-Upgrade Tasks Performed by Health Checker." |
| LanguagePackReadinessHealthChecks.xml | | Run this manifest before installing a language pack. See Section A.2.2.5.5, "Language Pack Readiness Health Checks." |
| PostLanguagePackHealthChecks.xml | | Run this manifest after installing a language pack. See Section A.2.2.5.6, "Post Language Pack Health Checks." |
| PatchingReadinessHealthChecks.xml | | Run this manifest before applying a patch. See Section A.2.2.5.7, "Patching Readiness Health Checks." |
| PostPatchingHealthChecks.xml | | Run this manifest after applying a patch. See Section A.2.2.5.8, "Post Patching Health Checks." |
| DataQualityChecks.xml | | Run this manifest to check the quality of data such as JAZN and seed data. Note that these checks may require significant processing time. See Section A.2.2.5.9, "Data Quality Check." |

### A.2.2.2  Set Up Health Checker on the DB and OHS Hosts

Perform the following one-time setup steps on the database host and the OHS host for Health Checker.

1. Create a ZIP archive of the Health Checker framework that exists on the primordial host in *REPOSITORY_LOCATION*.

   ```
   setenv APPLICATIONS_BASE APPLICATIONS_BASE
   cd REPOSITORY_LOCATION/installers/farup/Disk1/upgrade
   bin/hczip.py /any_scratch_directory/hc.zip --repoLoc $REPOSITORY_LOCATION
   ```

2. Use FTP or another method to transfer the `hc.zip` file to the DB or OHS host.

3. Create a directory where you want the Health Checker framework contents to reside. You must choose a separate directory that does not overlap with any provisioned components. This directory is referred to as *HC_TOP* in this section.

   ```
   mkdir /u01/hcframework
   ```

```
cd /u01/hcframework
cp hc.zip /u01/hcframework
unzip hc.zip
```

### A.2.2.3  How to Run Health Checker

Refer to the appropriate section for the steps to run Health Checker, which is delivered in the *REPOSITORY_LOCATION*/installers/farup/Disk1/upgrade/bin directory as hcplug.sh (UNIX) and hcplug.cmd (Windows).

- Run Health Checker on the Primordial Host

- Run Health Checker on the MidTier Host

- Run Health Checker on the OHS or DB Host

> **Note:** If you are running the
> PreDowntimeUpgradeReadinessHealthChecks.xml or
> PostUpgradeHealthChecks.xml manifests, you must also run the
> GeneralSystemHealthChecks.xml manifest.

**A.2.2.3.1  Run Health Checker on the Primordial Host**  Perform the following steps to run Health Checker on the primordial host.

1. Set the following environment variables:

   - *APPLICATIONS_BASE*: The directory that contains Oracle Fusion Applications. For example, if Oracle Fusion Applications is installed in /server01/APPTOP/fusionapps, then set the APPLICATIONS_BASE environment variable to /server01/APPTOP.

   - *REPOSITORY_LOCATION*: The directory where the repository is staged, *SHARED_LOCATION*/11.1.7.0.0/Repository.

   - *FA_SCRIPTS_DOWNLOAD_DIR*: The location of the PatchConflictManager.py utility, which you downloaded in Section 2.3.4, "Download and Unzip the Patch Conflict Manager Utility".

   - *DOWNLOAD_PATCH_DIR*: The location where you downloaded post-release patches in Section 2.3.6.3, "Download and Unzip Mandatory Post-Release 7 Patches".

   - Note that the following environment variables are set in the primordial host but the values come from the OHS host. For example, /u1/mw_home/Oracle_WT1/instances/CommonDomain_webtier does not exist on the primordial host and this path is a path on the OHS host. However, Health Checker requires this environment variable on the primordial host.

     - *OHS_INSTANCE_ID*: The OHS instance id being upgraded, such as ohs1.

     - *WT_CONFIG_HOME*: The Webtier instance configuration home, such as /u1/mw_home/Oracle_WT1/instances/CommonDomain_webtier.

     - *OHS_HOST_NAME*: The OHS host name, such as ohs_host.my.company.com.

2. Run Health Checker.

```
(UNIX)
$REPOSITORY_LOCATION/installers/farup/Disk1/upgrade/bin/hcplug.sh -manifest
REPOSITORY_LOCATION/installers/farup/Disk1/upgrade/config/manifest_name.xml
-DlogLevel=FINEST
```

```
(Windows)
%REPOSITORY_LOCATION%\installers\farup\Disk1\upgrade\bin\hcplug.cmd -manifest
 REPOSITORY_LOCATION\installers\farup\Disk1\upgrade\config\manifest_name.xml
-DlogLevel=FINEST
```

**3.** If Health Checker fails, follow the steps in Section A.2.2.4, "Troubleshoot Health Checker Failures."

**A.2.2.3.2  Run Health Checker on the MidTier Host**  Perform the following steps to run Health Checker on the MidTier host.

**1.** Set the following environment variables:

- *APPLICATIONS_BASE*: The directory that contains Oracle Fusion Applications. For example, if Oracle Fusion Applications is installed in /server01/APPTOP/fusionapps, then set the APPLICATIONS_BASE environment variable to /server01/APPTOP.

- *REPOSITORY_LOCATION*: The directory where the repository is staged.

- *IS_SECONDARY_NODE:* A value of yes or no, to indicate whether the midtier node is secondary.

**2.** Run Health Checker.

```
(UNIX)
$REPOSITORY_LOCATION/installers/farup/Disk1/upgrade/bin/hcplug.sh  -hostType
MIDTIER -manifest
REPOSITORY_LOCATION/installers/farup/Disk1/upgrade/config/manifest_name.xml
-DlogLevel=FINEST

(Windows)
%REPOSITORY_LOCATION%\installers\farup\Disk1\upgrade\bin\hcplug.cmd  -hostType
MIDTIER -manifest
REPOSITORY_LOCATION\installers\farup\Disk1\upgrade\config\manifest_name.xml
-DlogLevel=FINEST
```

**3.** If Health Checker fails, follow the steps in Section A.2.2.4, "Troubleshoot Health Checker Failures."

**A.2.2.3.3  Run Health Checker on the OHS or DB Host**  Perform the following steps to run Health Checker on the OHS or DB host.

**1.** For pre-down time checks, note the location where the PatchConflictManager.py utility was downloaded in Section 2.3.4, "Download and Unzip the Patch Conflict Manager Utility", because you must set the *FA_SCRIPTS_DOWNLOAD_DIR* environment variable as a pointer to this location in Step 2.

**2.** Set the following environment variables:

- Required environment variables for the OHS host:
    - *APPLICATIONS_BASE: HC_TOP*, which was created in Step 3
    - *REPOSITORY_LOCATION*: The directory where the repository is staged
    - *JAVA_HOME*: The Java home.
    - *WT_MW_HOME*: The Webtier Middleware home directory that contains the oracle_common, webtier, and webgate homes.
    - *WT_ORACLE_HOME*: The Webtier Oracle home which is usually under the Webtier Middleware Home directory.

- *WT_CONFIG_HOME*: The Webtier Config Home that contains the webtier instance, for example, /u01/oracle/mw_home/Oracle_WT1/instances/CommonDomain_webtier.

- *OHS_INSTANCE_ID*: The OHS instance id being upgraded, such as ohs1.

- *UPGRADEOHS_PROP_FILE*: Location for upgradeOHS.properties file. For example: /tmp/upgradeohs.properties.

- *RUPLITE_FOR_OHS_DIR*: Directory for RUPLite for OHS webgate installer. For example: /u01/webgate/webgate_installer_REL7.

- *CURRENT_FA_RELEASE_VERSION*: The current release, 11.1.7.0.0.

- *FA_SCRIPTS_DOWNLOAD_DIR*: The location of the PatchConflictManager.py utility, which you downloaded in Section 2.3.4, "Download and Unzip the Patch Conflict Manager Utility".

- *DOWNLOAD_PATCH_DIR*: The location where you downloaded post-release patches in Section 2.3.6.3, "Download and Unzip Mandatory Post-Release 7 Patches".

- Required environment variables for the database host:

  - *APPLICATIONS_BASE: HC_TOP*, which was created in Step 3

  - *REPOSITORY_LOCATION*: The directory where the repository is staged

  - *JAVA_HOME:* The Java home.

  - *ORACLE_HOME*: The Oracle Database home directory.

  - *PATH*: The path to *Oracle_home/bin*.

  - *LISTENER_NAME:* The Oracle database listener name

  - *ORACLE_SID*: The Oracle database SID

  - *TNS_ADMIN:* The Oracle home admin directory, such as ORACLE_HOME/network/admin

  - *LD_LIBRARY_PATH*: $ORACLE_HOME/lib

  - *GRID_HOME*: On RAC configurations, set this to *GRID_HOME*. Otherwise set to *ORACLE_HOME*.

  - *FA_SCRIPTS_DOWNLOAD_DIR*: The location of the PatchConflictManager.py utility, which you downloaded in Section 2.3.4, "Download and Unzip the Patch Conflict Manager Utility".

  - *DOWNLOAD_PATCH_DIR*: The location where you downloaded post-release patches in Section 2.3.6.3, "Download and Unzip Mandatory Post-Release 7 Patches".

3. Run Health Checker and specify -hostType and the -jreLoc on this host. Note that -jreLoc is the same as the *JAVA_HOME* location for this host.

```
(UNIX)
$REPOSITORY_LOCATION/installers/farup/Disk1/upgrade/bin/hcplug.sh -hostType
[DB|OHS] -jreLoc location_of_Java -manifest
REPOSITORY_LOCATION/installers/farup/Disk1/upgrade/config/manifest_name.xml
-DlogLevel=FINEST [-logDir logfile_directory]

(Windows)
%REPOSITORY_LOCATION%\installers\farup\Disk1\upgrade\bin\hcplug.cmd -hostType
[DB|OHS] -jreLoc location_of_Java -manifest
REPOSITORY_LOCATION\installers\farup\Disk1\upgrade\config\manifest_name.xml
```

```
-DlogLevel=FINEST [-logDir logfile_directory]
```

4. If Health Checker fails, follow the steps in Section A.2.2.4, "Troubleshoot Health Checker Failures."

### A.2.2.4 Troubleshoot Health Checker Failures

If Health Checker finds an issue that must be corrected, the description of the required corrective action displays on the console, in the Health Checker log file, and in an HTML summary report. The log file and the HTML summary are located in *APPLICATIONS_CONFIG*/fapatch/logs/11.1.7.0.0/healthchecker

Health Checker generates a report named *healthcheckplugin*_actionsummary_ *timestamp*.html, that displays the validation checks performed and their statuses. Review this report to determine whether any checks failed to validate and then manually perform the corrective actions for the failed checks.

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.

### A.2.2.5 Health Checker Plug-ins

There may be situations in which you want to run health checks manually, outside of orchestration. For example, you may want to run the pre-down time checks several weeks before you upgrade, so that you have time to fix any issues found by PreDowntimeUpgradeReadinessHealthChecks.xml.

Health Checker calls plug-ins to perform its tasks. This section describes which plug-ins run during the following phases of the installer process:

- General System Health Checks

- Pre-Down Time Upgrade Tasks

- Pre-Upgrade Tasks Performed by Health Checker During Down Time

- Post-Upgrade Tasks Performed by Health Checker

- Language Pack Readiness Health Checks

- Post Language Pack Health Checks

- Patching Readiness Health Checks

- Post Patching Health Checks

**A.2.2.5.1 General System Health Checks** The following checks occur when you run Health Checker using the GeneralSystemHealthChecks.xml manifest.

- Administration Servers and Managed Servers are Up

  Confirms that all relevant Administration Servers and Managed Servers have a RUNNING status.

- Certificate Expiry in Trust Keystore

  Checks the expiration date for the certificates in the Trust key store and reports an error if the expiration date has passed or is within the next 90 days.

- Credential Store Connectivity

  Checks if a connection can be established to the credential store.

- Credentials in Oracle Directory Services Manager (ODSM)

Verifies that a specific user, usually the `PolicyRWUser` user, is part of the `cn=DirectoryAdminGroup`.

- Database Instance Connectivity

  Checks if the database instance is up. For RAC databases, checks if all nodes are up.

- DBMS_STATS Collection for MDS Schema in Oracle Fusion Applications Database

  Confirms that `DBMS_STATS` has recently been run on the MDS schema in the Oracle Fusion Applications database. You must run `DBMS_STATS` on any schemas that are reported by Health Checker.

- Deployed Applications are Up

  Verifies that all deployed applications are up and running.

- FAPatchManager Configuration

  Checks if Oracle Fusion Applications Patch Manager is correctly configured, including the following validations:

  – Checks to see if `FUSION_env.properties` and `ATGPF_env.properties` are correct.

  – Checks for existence of the fapmgr.ini file in the environment.

  – Verifies registered products against the database.

- Flexfields Metadata in the Flex Repository

  Checks if there is a Flexfields metadata violation that indicates that the Extensible Flexfields has a UI Page defined that references a Flexfield Context which has not been associated with the corresponding Category or any of its parent Categories.

- Fusion Applications Certification Matrix

  Confirms the correct versions of installed components, according to the certification matrix.

- Fusion Schema Connectivity

  Validates the database connectivity to all Fusion schemas.

- Hosts Name

  Confirms that host names are correctly formatted in the `/etc/hosts` file. The `/etc/hosts` file is a network configuration file that associates IP addresses with host names and host alias names, if used. The following checks are performed by this plug-in:

  - The /etc/hosts file contains an entry for the IP address 127.0.0.1, followed by the name `localhost`.

  - The format of each host entry in `/etc/hosts` is `IP_address canonical_ hostname [aliases]`. If the machine name is a logical host name and is different from the physical host name that is specified in `/etc/sysconfig/network`, the logical host name must be listed before the physical host. Ensure that the first entry in `/etc/hosts`, machine name (host name), and the value used in `pod.properties`, are identical.

  - If the machine name is the same as the physical host name, there is no need to check the order of the host names.

- Identity and Policy Store LDAP

Verifies the connectivity to the identity store and policy store LDAP using identity store credentials.

■ Identity Store Connectivity using jps-config-jse.xml

Verifies that the `idstore.ldap.provider` in `jps-config-jse.xml` can be used to connect to the identity store.

■ IIR Configuration

Verifies that Fusion Informatica IR is set up properly.

■ INBOUND_CONNECT_TIMEOUT parameter in sqlnet.ora and listener.ora

Checks for recommended values in the `INBOUND_CONNECT_TIMEOUT` parameter in `sqlnet.ora` and `listener.ora` files on the database host.

■ Index Validity in Fusion Schema of Oracle Fusion Applications Database

Checks for unusable indexes in the Fusion Schema of the Oracle Fusion Applications database.

■ `init.ora` parameters

Verifies that the `init.ora` parameters are correct.

■ Invalid Objects

Checks for and reports any invalid objects.

■ JAZN Version in Oracle_Home Matches LDAP

Verifies that the JAZN version in `system-jazn-data.xml` is the same as the version in the policy store.

■ JVM Architecture, JDK platform Type, JAVA Version, and JDK Vendor

Verifies that the JDK version is valid. It also validates the JVM architecture, JDK platform type, and JDK vendor.

■ Listener Configuration

Verifies that the database listener configuration runs from the grid home on the DB host and also that no duplicate processes for the listener are running.

■ Local Port Range Value

Checks the local port range value in `/proc/sys/net/ipv4/ip_local_port_range`. The recommended value is `32768 61000`. If the range is set to any value below `32768`, a system process could potentially use a port that was assigned to one of the Managed Servers. Since RUP Installer requires all domains to be down, those ports are available for the system to use.

■ Mandatory Patches Have Been Applied

Verifies that mandatory patches have been applied.

■ MDS Schema Connectivity

Checks database connectivity for schemas that contain FUSION_MDS in their name.

■ Middleware Schema Connectivity

Checks database connectivity for all schemas except for FUSION_MDS schemas.

■ Multi-Tenant set-up in Fusion Schema of Oracle Fusion Applications Database

Ensures that only one enterprise is enabled in the database.

- Node Manager Crash Recovery Is Set To True

  Verifies the `CrashRecoveryEnabled` entry in `nodemanager.properties` is set for each host.

- Node Managers are up and accessible

  Checks if node managers for all hosts are running and are accessible.

- OAM Configuration

  Verifies the following information in `Fusion_env.properties`:

  - OAM_ADMIN_SERVER_HOST

  - OAM_ADMIN_SERVER_PORT

  - OAM_WEB_DOMAIN

  - OAM admin user credential from the credential store

- ODI Repository URLs

  Finds all jdbc connection URLs in the ODI repository and validates that they point to the same database as the database that is referenced in the `DB_CONNECT_STRING` parameter in `Fusion_env.properties`.

- ODI supervisor credentials

  Confirms the correct connection URLs exist in the ODI Repository.

- OHS Instance Registration

  Verifies that the OHS instance is registered in `topology.xml`.

- OHS Process Status on OHS Using OPMN

  Check if the OHS process is up on the OHS host.

- OPatch Version in FA_ORACLE_HOME

  Verifies that the version of OPatch is compatible with Oracle Fusion Applications. If an incompatible version of OPatch exists in *FA_ORACLE_HOME*, errors can occur while applying patches and running RUP Installer.

- Open File Limit

  Verifies the open file limit. RUP Installer uses multiple workers for uploading database content. The number of workers used dictates the open file limit setting for the machine where you run the RUP Installer. To understand how the number of workers are calculated and the requirement for the open file limit setting for the workers, see "Patching Database Artifacts" in the *Oracle Fusion Applications Patching Guide*. For more information, see "Increase the Open Files Limit" in the *Oracle Fusion Applications Installation Guide*.

- Oracle Homes are Registered in the Central Inventory

  Verifies that the Oracle Business Intelligence, Global Order Processing, Web Tier, and Web Tier Common Oracle home directories are registered for use by Oracle Fusion Applications.

- ORACLE_COMMON Inventory Location on OHS

  Verifies that the OH home and the Oracle Common home are pointing to the correct inventory location on OHS in *WT_MIDDLEWARE_HOME*/oracle_common/oraInst.loc.

- OS Attributes

Validates the operating system name, architecture and versions.

- Password Expiry For Critical Bind Users in LDAP

  Verifies that the passwords for critical bind users are not locked and will not expire within the next three days.

- Read Write Access to *APPLICATIONS_BASE*

  Verifies that directory the APPLICATIONS_BASE directory has read-write access.

- Remote OPMN Access

  Verifies that the remote OPMN process is accessible.

- Size and Contents of `default-keystore.jks` File in All Domains

  Verifies that the size of the `default-keystore.jks` file for all domains is same as that of CommonDomain.

- Taxonomy URL

  Verifies the `TAXONOMY_URL` value, which is obtained from `FUSION_env.properties`.

- User Administrator or Super User Role

  Verifies that the owner of APPLICATIONS_BASE is the same as the user who is running Health Checker.

- Virtual Hosts Wiring

  Verifies that the host and port wirings in the *APPLICATIONS_CONFIG*`/CommonDomain_webtier/config/OHS/ohs1/moduleconf/FusionVirtualHost_app.conf` files are correct.

- WSM-PM Application is Active

  Verifies that the WSM-PM application is running on all SOA domains.

**A.2.2.5.2  Pre-Down Time Upgrade Tasks**  The following checks occur when Health Checker runs using the `PreDowntimeUpgradeReadinessHealthChecks.xml` manifest.

- Base SOA Composites Exist

  Verifies that all base SOA composites exist for the versions that are going to be upgraded by a patch.

- Data Guard State

  Checks if Data Recovery is enabled in the environment and that it is stopped before the upgrade.

- Environment Properties on OHS

  This plug-in verifies the properties used by the RUP Lite for OHS utility.

- Free and Total Memory

  Verifies that the primordial host has enough free memory for the upgrade. The required memory is calculated based on which domains and servers are configured to run on the host where the Health Checker is run.

- Free Disk Space

  Checks for free and usable disk space on the primordial and non-primordial Oracle Fusion Applications hosts.

- HCM Workforce Reputation Offerings Shared Mount

If the environment is provisioned with HCM Workforce offerings, verifies if the environments have the mandatory shared directory and mount point configured.

- Middleware Installer exists in Release Repository

  Verifies that all Middleware installers exist in the repository.

- No Locked ODI Objects or SES Objects Exist

  Verifies that there are no locked objects in the `FUSION_ODI` and `SES` schemas.

- No Patch Conflicts Exist

  Runs the PatchConflictManager utility to remove conflicting patches.

- WLS Edit Sessions and Unactivated Changes Exist

  Verifies that no WLS edit sessions or unactivated changes exist.

- OHS Process Status on OHS Using OPMN

  Verifies that the OHS process is up and running on the OHS host.

- Oracle Fusion Applications Release Version:

  To install Release 7, the installed Oracle Fusion Applications version must be Release 6. This plug-in ensures that the installed version of Oracle Fusion Applications is 11*g* Release 6, (11.1.6.0.0).

- Permissions For Temp Directory

  Verifies that files in the temporary directory that match the pattern, `/tmp/*pki*`, are owned by the same user that starts servers.

- Availability of ports for new Managed Servers

  Verifies the availability of ports for managed servers that were added. This plug-in is available only in Release 7.

- Properties for DB Host Upgrade

  Verifies that the environment properties to be used for DB Host upgrade are valid.

- Repository Integrity

  Checks whether all required files are present in the repository and reports any missing files.

- Seed Data For Potential Conflicts

  Performs a set of validations to prevent potential seed data failures.

- SES Schedules and Index Optimizer are Stopped/Disabled

  Verifies that SES schedules and the index optimizer are stopped.

- SOA Platform is Ready

  Verifies whether the SOA platform is ready for each domain that is impacted by the contents of the upgrade.

- Sessions holding 'library cache load lock' in Fusion Schema of Oracle Fusion Applications Database

  Checks whether there are any database sessions that are holding a "library cache load lock" in the Fusion schema of the Oracle Fusion Applications database.

- Total Memory and Swap

Verifies there is sufficient memory for upgrading. The memory requirement calculation is based on the domains and servers that are configured to run where Health Checker runs.

**A.2.2.5.3   Pre-Upgrade Tasks Performed by Health Checker During Down Time**   The following checks occur when Health Checker runs the `DuringDowntimeUpgradeReadinessHealthChecks.xml` manifest.

- AD Admin Sessions, AutoPatch and Patch Manager Processes are Complete

    Checks whether any AD Administration, AutoPatch or Patch Manager processes are running.

- Credential Store Connectivity

    Checks if a connection can be established to the credential store.

- Data Guard State

    Checks if Data Recovery is enabled in the environment and that it is stopped before the upgrade.

- Database Instance Connectivity

    Checks if the database instance is up. For RAC databases, checks if all nodes are up.

- Database version

    Checks if Oracle Database version is above the minimum required for Oracle Fusion Applications 11*g* Release 7 (11.1.7).

- Database is Running and in Idle State

    Verifies that no SQL sessions, jobs, or processes are running or are scheduled to be running against the database.

- Free Memory and Swap

- Identity and Policy Store LDAP

    Verifies the connectivity to the identity store and policy store LDAP using identity store credentials.

- Identity Store Connectivity using jps-config-jse.xml

    Verifies that the `idstore.ldap.provider` in `jps-config-jse.xml` can be used to connect to the identity store.

- Invalid Objects

    Checks for and reports any invalid objects.

- JAZN Version in Oracle_Home Matches LDAP

    Verifies that the JAZN version in `system-jazn-data.xml` is the same as the version in the policy store.

- Mandatory Patches Have Been Applied

    Verifies that mandatory patches have been applied.

- MDS Schema Connectivity in RUP1 Env

    Checks database connectivity for schemas that contain FUSION_MDS in their name.

- Middleware Schema Connectivity in RUP1 Env

Checks database connectivity for all schemas except for FUSION_MDS schemas.

- Node Managers are down

  Verifies Node Managers are down.

- Administration Servers and Managed Servers are Down

  Confirms that all relevant Administration Servers and Managed Servers are down.

**A.2.2.5.4  Post-Upgrade Tasks Performed by Health Checker**  The following checks occur when Health Checker runs the `PostUpgradeHealthChecks.xml` manifest.

- AD Admin Sessions, AutoPatch and Patch Manager Processes are Complete

  Checks whether any AD Administration, AutoPatch or Patch Manager processes are running.

- Data Guard State

  Checks if Data Recovery is enabled in the environment and that it is stopped before the upgrade.

- Database version

  Checks if Oracle Database version is above the minimum required for Oracle Fusion Applications 11*g* Release 7 (11.1.7).

- Installed Languages are Upgraded to Release

  Checks if a language pack has been upgraded to the current release or needs to be upgraded to the current release.

- JAZN Conflicts

  Validates the results of the JAZN analysis reports for each stripe to find any potential conflicts or deletions that were not patched automatically by the installer.

- Locked ODI Objects or SES Objects

  Verifies that there are no locked objects in the `FUSION_ODI` and `SES` schema.

- Permissions For Temp Directory

  Verifies that files in the temporary directory that match the pattern, `/tmp/*pki*`, are owned by the same user that starts servers.

- SOA Composites in the Repository are Deployed

  Verifies that the SOA composites in the repository were deployed by the upgrade.

- SOA Platform is Ready

  Verifies whether the SOA platform is ready for each domain that is impacted by the contents of the upgrade.

- WLS Edit Sessions and Unactivated Changes

  Verifies that no WLS edit sessions or unactivated changes exist.

**A.2.2.5.5  Language Pack Readiness Health Checks**  The following checks occur when Health Checker runs the `LanguagePackReadinessHealthChecks.xml` manifest. You typically run this manifest before you install a language pack. For more information, see "Installing and Maintaining Oracle Fusion Applications Languages" in *Oracle Fusion Applications Administrator's Guide*.

- AD Admin Sessions, AutoPatch and Patch Manager Processes are complete

Checks whether any AD Administration, AutoPatch or Patch Manager processes are running.

- All Installed Languages are Upgraded to Release

  Checks if a language pack has been upgraded to the current release or needs to be upgraded to the current release.

- Database is Running and in Idle State

  Verifies that no SQL sessions, jobs, or processes are running or are scheduled to be running against the database.

- Repository Integrity

  Checks whether all required files are present in the repository and reports any missing files.

- SOA Platform is Ready

  Verifies whether the SOA platform is ready for each domain that is impacted by the contents of the upgrade.

**A.2.2.5.6  Post Language Pack Health Checks**  The following checks occur when Health Checker runs the `PostLanguagePackHealthChecks.xml` manifest. You typically run this manifest after you install a language pack. For more information, see "Installing and Maintaining Oracle Fusion Applications Languages" in the *Oracle Fusion Applications Administrator's Guide*.

- JAZN Conflicts

  Validates the results of the JAZN analysis reports for each stripe to find any potential conflicts or deletions that were not patched automatically by the installer.

**A.2.2.5.7  Patching Readiness Health Checks**  The following checks occur when Health Checker runs the `PatchingReadinessHealthChecks.xml` manifest. You typically run this manifest before applying a patch. For more information, see "Step 7 Prepare the System" in the *Oracle Fusion Applications Patching Guide*.

- AD Admin Sessions, AutoPatch and Patch Manager Processes are complete

  Checks whether any AD Administration, AutoPatch or Patch Manager processes are running.

- Base SOA Composites Exist

  Verifies that all base SOA composites exist for the versions that are going to be upgraded by a patch.

- Database version

  Checks if Oracle Database version is above the minimum required for Oracle Fusion Applications 11*g* Release 7 (11.1.7).

- Database is Running and in Idle State

  Verifies that no SQL sessions, jobs, or processes are running or are scheduled to be running against the database.

- IPM server status

- No Locked ODI Objects or SES Objects Exist

  Verifies that there are no locked objects in the `FUSION_ODI` or SES schema.

- WLS Edit Sessions and Unactivated Changes Exist

Verifies that no WLS edit sessions or unactivated changes exist.

- SOA Platform is Ready

  Verifies whether the SOA platform is ready for each domain that is impacted by the contents of the upgrade.

**A.2.2.5.8  Post Patching Health Checks**  The following checks occur when Health Checker runs the `PostPatchingHealthChecks.xml` manifest. You typically run this manifest after applying a patch. For more information, see "Step 11 Run Health Checker for Post Patching Health Checks" in the *Oracle Fusion Applications Patching Guide*

- AD Admin Sessions, AutoPatch and Patch Manager Processes are complete

  Checks whether any AD Administration, AutoPatch or Patch Manager processes are running.

- JAZN Conflicts

  Validates the results of the JAZN analysis reports for each stripe to find any potential conflicts or deletions that were not patched automatically by the installer.

- No Locked ODI Objects or SES Objects Exist

  Verifies that there are no locked objects in the `FUSION_ODI` schema.

- WLS Edit Sessions and Unactivated Changes Exist

  Verifies that no WLS edit sessions or unactivated changes exist.

**A.2.2.5.9  Data Quality Check**  The Validating JAZN Policy Data check occurs when Health Checker runs the `DataQualityChecks.xml` manifest.

**A.2.2.5.10  Vital Signs Check**  The following checks occur when Health Checker runs the `VitalSignsChecks.xml` manifest.

- Database Instance Connectivity

  Checks if the database instance is up. For RAC databases, checks if all nodes are up.

- Fusion Schema Connectivity

  Validates the database connectivity to all Fusion schemas.

- Identity and Policy Store LDAP

  Verifies the connectivity to the identity store and policy store LDAP using identity store credentials.

- Identity Store Connectivity using jps-config-jse.xml

  Verifies that the `idstore.ldap.provider` in `jps-config-jse.xml` can be used to connect to the identity store.

- MDS Schema Connectivity

  Checks database connectivity for schemas that contain `FUSION_MDS` in their name.

- Middleware Schema Connectivity

  Checks database connectivity for all schemas except for `FUSION_MDS` schemas.

- Verify All Admin Servers and Managed Servers are Up

  Verifies that all Administration and Managed Servers are up.

### A.2.2.6 Health Checks: Overrides

The Health Checker utility offers a method for you to manage which health checks run on your environment. For example, you may want to exclude a health check that is related to a known issue in an environment. You can also add a new check to an existing Health Checker plug-in, if needed. The configuration parameters for Health Checker are stored in the `REPOSITORY_LOCATION/installers/farup/Disk1/upgrade/config/healthchecks.xml` file. You are not allowed to edit this file. If you want to override any configuration parameters or exclude certain plug-ins from running, you can create configuration override files.

Health Checker first loads the configuration parameters that are stored in `healthchecks.xml` and then it considers the configuration override files.

This section describes the following topics related to managing Health Checker sessions:

- Create Override Files

- Override Health Checker Configuration Parameters

- Example For Overriding Health Checks

- Disable a Plug-in

- Customize Plug-in Timeouts

**A.2.2.6.1 Create Override Files** The first step in overriding the standard checks run by Health Checker is to create one or more override files. To create an override file, copy the appropriate override template to the override directory, which defaults to location *SHARED_UPGRADE_LOCATION/*healthchecker/*POD_NAME*, and rename this file to eliminate the `.template` extension. The following templates are located in the *ORCH_LOCATION*/fusionapps/applications/lcm/hc/config directory. *ORCH_LOCATION* is where `orchestration.zip` is unzipped, as described in Section 2.3.7, "Unzip Orchestration.zip".

- `ALL_overrides.xml.template`

- `DB_overrides.xml.template`

- `MIDTIER_overrides.xml.template`

- `OHS_overrides.xml.template`

- `PRIMORDIAL_overrides.xml.template`

Select the template that corresponds to the host type for which you want to create the overrides. For example, if you want to create overrides for the primordial host, use `PRIMORDIAL_overrides.xml`. If the override applies to all hosts, use `ALL_overrides.xml`.

The default location for override files is *SHARED_UPGRADE_LOCATION/*healthchecker/*POD_NAME*.

**A.2.2.6.2 Override Health Checker Configuration Parameters** To override configuration parameters within an override file, uncomment the XML portion of the override file, and customize the override file to meet your requirements. Remove all values from the override file except for the values that you want to exclude. To disable a check, add `disabled=true` to the check. To add a check, add the value to the override file.

**A.2.2.6.3 Example For Overriding Health Checks** This example shows how to customize the list of URIs that are verified by Health Checker. The following steps describe this customization:

1. Copy the template for the override file.

```
cp REPOSITORY_LOCATION/installers/farup/Disk1/upgrade/config/ALL_
overrides.xml.template SHARED_UPGRADE_LOCATION/healthchecker/POD_NAME/ALL_
overrides.xml
```

2. Uncomment the XML portion of the override file.

   The original override file looks as follows:

```
<!--
<checks category="context_root_locations">
<check value="/console"/>
<check value="/soa-infra"/>
<check value="/wsm-pm"/>
<check value="/apm"/>
<check value="/setup"/>
<check value="/helpPortal"/>
<check value="/fndSetup"/>
<check value="/homePage"/>
</checks>
-->
```
   After removing the XML comment lines, <!--, the -->, the override file now looks as follows:

```
<checks category="context_root_locations">
<check value="/console"/>
<check value="/soa-infra"/>
<check value="/wsm-pm"/>
<check value="/apm"/>
<check value="/setup"/>
<check value="/helpPortal"/>
<check value="/fndSetup"/>
<check value="/homePage"/>
</checks>
```

3. Remove all rows except those that you want to exclude. In this example, you do not want Health Checker to validate the URI for soa-infra and you want to add a validation for myuri. To disable a check, add disabled="true" to the check. To add a URI to be checked, add the URI to the override file. The override file now looks as follows:

```
<checks category="context_root_locations">
<check value="/soa-infra" disabled="true"/>
<check value="/myuri"/>
</checks>
```

**A.2.2.6.4  Disable a Plug-in** To disable a plug-in, you must first find its display name (from the HTML report), its class name (from the log file), or its ID (from the manifest). The following example displays how a plug-in is defined in a Health Checker manifest file:

```
<plugin id="TotalMemoryCheck"
description="Verifying Total Memory and Swap"
invoke=""
plugin.class="oracle.check.sys.TotalMemCheckPlugin"
```

The following example depicts how you can override the plug-in the override file. This example shows the display name, class name, and ID for the plug-in, but only one of these is required. Note that excluded plug-ins must be listed under the "exclude" category.

```
<checks category="exclude">
<check name="TotalMemoryCheck"/>
<check name="Verifying Total Memory and Swap"/>
<check name="oracle.check.sys.TotalMemCheckPlugin"/>
<check name="TotalMemCheckPlugin"/>
```

**A.2.2.6.5  Customize Plug-in Timeouts**  To prevent a plug-in timeout while Health Checker runs, you can create an override file to specify a longer timeout. You must know the plug-in class name, and the timeout value in seconds to modify the value. You can find the plug-in class name in the Health Checker manifest. In the following example, the plug-in class name for the `Verify DataSource connectivity` check is `oracle.check.apps.VerifyDSConnectivity`.

```
GeneralSystemHealthChecks.xml-  plugin id="DSStatusPlugin"
GeneralSystemHealthChecks.xml-    description="Verify DataSource connectivity"
GeneralSystemHealthChecks.xml-    invoke=""
GeneralSystemHealthChecks.xml:
plugin.class="oracle.check.apps.VerifyDSConnectivity"
GeneralSystemHealthChecks.xml-    class.path="$HC_LOCATION/lib/precheckplugin.jar;
GeneralSystemHealthChecks.xml-    $HC_LOCATION/lib/hccommon.jar"
GeneralSystemHealthChecks.xml-    stoponerror="false"/>
```

To find the current timeout value, open the healthchecker log file and find the portion of the log that was produced by the plug-in. The log includes the current timeout value, as shown in the following examples:

```
[2013-08-08T22:35:42.791+00:00] [healthcheckplug] [NOTIFICATION] []
[oracle.healthcheckplug] [tid: 10] [ecid: 0000K1W4R2R3v1G5IzXBif1I11oQ000000,0]
Using default timeout of 120 seconds

[2013-08-08T22:35:17.877+00:00] [healthcheckplug] [NOTIFICATION] []
[oracle.healthcheckplug] [tid: 10] [ecid: 0000K1W4R2R3v1G5IzXBif1I11oQ000000,0]
[SRC_CLASS: oracle.check.common.util.Utils] [SRC_METHOD: getTimeout] Timeout for
VerifyDSConnectivity is 901 seconds
```

Perform the following steps to modify the timeout value.

1. Create the override file as described in .

2. Go to the `timeout_seconds` section as shown in the following example.

   ```
   <!-- Timeout, used by plugins for running external commands or wlst scripts or
   ... -->
   <checks category="timeout_seconds">
       <check name="VerifyDSConnectivity" value="600"/>
       <check name="LdapDataQualityCheckPlugin" value="1800"/>
       <check name="ContextRootCheckPlugin" value="1800"/>
   </checks>
   ```

3. If the plug-in is already listed in this section, set the new timeout value in seconds. If the plug-in is not listed, add it.

   In the following example, the time out for `Verify DataSource connectivity` (`oracle.check.apps.VerifyDSConnectivity`) is set to 45 minutes (2700 seconds).

   ```
   <checks category="timeout_seconds">
       <check name="VerifyDSConnectivity" value="600"/>
       <check name="LdapDataQualityCheckPlugin" value="1800"/>
       <check name="ContextRootCheckPlugin" value="1800"/>
       <!-- Either of the two lines below changes the timeout to 2700 -->
       <check name="VerifyDSConnectivity" value="2700"/>
       <check name="oracle.check.apps.VerifyDSConnectivity" value="2700"/>
   ```

```
        </checks>
```

## A.2.3  RUP Lite for OVM Utility

The **RUP Lite for OVM** utility addresses the differences between a newly provisioned Oracle VM environment on the latest release and an Oracle VM environment provisioned in a previous release. You run RUP Lite for OVM only if you are running Oracle Fusion Applications in an Oracle VM environment that was created from the official releases of Oracle VM templates for Oracle Fusion Applications Release 2 (11.1.2) and higher. This utility is not applicable for any Oracle VM environments that are created using other methods.

The following steps provide an overview of how Upgrade Orchestrator supports RUP Lite for OVM when upgrading from Release 5 to Release 6 to Release 7. Plug-ins for both Release 6 and Release 7 are included and shared plug-ins run only once.

Note that log files for RUP Lite for OVM are located under the location from where you are running RUP Lite for OVM. An example location for running RUP Lite for OVM in offline mode follows:

```
/u01/lcm/rupliteovm/output/logs/11.1.7.0.0/mycompany.com/rupliteoffline.lo
g
```

*Table A–7    Orchestration of RUP Lite for OVM - Release 5 to Release 7 Upgrade*

| Description | Step Support | For More Information |
|---|---|---|
| Copy the Release 6 `rupliteovm` pre-upgrade directory to *SHARED_LOCATION* | Pre-Upgrade Step | Step 1, Section 2.4.2.2.1, "Prepare RUP Lite for OVM for Release 6" |
| Copy the Release 7 `rupliteovm` pre-upgrade directory to *SHARED_LOCATION* | Pre-Upgrade Step | Step 1, Section 2.4.2.2.2, "Prepare RUP Lite for OVM for Release 7" |
| Configure the properties for each release | Pre-Upgrade Step | Section 2.4.2.2.1, "Prepare RUP Lite for OVM for Release 6" |
| Run RUP Lite for OVM in wallet mode for each release | | Section 2.4.2.2.2, "Prepare RUP Lite for OVM for Release 7" |
| Run RUP Lite for OVM Release 6 in validate mode | Upgrade Orchestrator | |
| Install Release 6 `fasaaslcmtools` Oracle home | | |
| Run RUP Lite for OVM in offline mode | | |
| Run RUP Installer for Release 6 | | |
| Run RUP Lite for OVM in online mode | | |
| Run RUP Lite for OVM in post-root mode for Release 6 | Pause Point | Section 4.4.7, "Run RUP Lite for OVM in Post-Root Mode for Release 6" |
| Run RUP Lite for OVM Release 7 in validate mode | Upgrade Orchestrator | |
| Install and upgrade Release 7 `fasaaslcmtools` Oracle home | | |

*Table A–7   (Cont.)  Orchestration of RUP Lite for OVM - Release 5 to Release 7 Upgrade*

| Description | Step Support | For More Information |
| --- | --- | --- |
| Run RUP Lite for OVM in pre-root mode | Pause Point | Section 4.4.6, "Run RUP Lite for OVM in Pre-Root Mode for Release 7" |
| Run RUP Lite for OVM in offline mode | Upgrade Orchestrator | |
| Run RUP Installer for Release 7 | | |
| Run RUP Lite for OVM in online mode | | |
| Run RUP Lite for OVM in post-root mode | Pause Point | Section 4.4.8, "Run RUP Lite for OVM in Post-Root Mode for Release 7" |

RUP Lite for OVM implements several plug-ins that are designed specifically for Oracle VM environments. Each plug-in determines which nodes it needs to run on and in which mode it must run. Table A–8 describes the plug-ins that are included in RUP Lite for OVM in offline mode.

*Table A–8    Offline Plug-ins for RUP Lite for OVM*

| Plug-in Name | Mandatory | Description |
| --- | --- | --- |
| ValidateEnvironment | Yes | Checks if the node is a valid Oracle VM node. This plug-in always runs and has no properties. |
| SetupCredentials | Yes | Prompts for credentials and stores the results in a secure manner for other plug-ins to use. This plug-in always runs and only prompts for secure properties that are needed by other plug-ins that will run. If a plug-in does not run on the current node or is disabled, then its properties are not requested. |
| UpdateResolvConf | No | Adds DNS name servers, search domains, and other options by updating `/etc/resolv.conf`. This plug-in runs on all nodes. |
| ApplyMemorySettings | No | This plug-in runs only on the `admin-apps` node. It increases existing memory settings for WebLogic servers based on the latest Oracle recommendations. It updates settings to the higher of the current setting or the recommended setting. If memory settings increase to a level where the Oracle VM's memory settings need to be increased, then the update to the Oracle VM must be done before running RUP Lite for OVM. <br><br> Note that values that are higher in the environment compared to the reference values are not changed. Only lower values are increased. |
| GenerateOptimizedQueryPlans | Yes | Generates optimized query plans for Oracle MDS queries. |
| DisableSearchUI | Yes | Disables the global search UI for Oracle Fusion Applications. |
| UpdateFusionIIRDiag | Yes | Updates the `fusioniirdiag.sh` script in the `APPLICATIONS_BASE`/InformaticaIR/bin directory. |
| DisableWebchat | Yes | Performs the steps to disable Webchat. |

Table A–9 describes the plug-ins that are included in RUP Lite for OVM in online mode.

*Table A–9    Online Plug-ins for RUP Lite for OVM*

| Plug-in Name | Mandatory | Description |
| --- | --- | --- |
| ValidateEnvironment | Yes | Checks if the node is a valid Oracle VM node. This plug-in always runs and does not have any properties. |
| SetupOnlineCredentials | Yes | Prompts for credentials for online plug-ins and stores the results in a secure manner for other plug-ins to use. This plug-in always runs and only prompts for secure properties that are needed by other plug-ins that will run. If a plug-in does not run on the current node or is disabled, then its properties are not requested. You are prompted for the password twice. |
| DeployECSF | Yes | Deploys ECSF artifacts that are not yet deployed, such as search objects, search categories, and index schedules. |
| DisableWebchatConnecti ons | Yes | Disables Webchat WebCenter connections. |
| ConfigureBIEmailDelive ry | Yes | Enables outbound email communication of BI Delivery reports |

## A.2.4  RUP Lite for OHS Utility

The *RUP Lite for OHS* utility manages the steps required to update WebGate, OHS, and *ORACLE_COMMON*. The following steps are performed by RUP Lite for OHS to accomplish this upgrade:

- Stop Oracle Process Manager and Notification Server (OPMN) processes and start the OPMN server.

- Apply OPatches from the repository to WebGate, OHS, and *ORACLE_COMMON*.

- Apply manually downloaded OPatches to WebGate, OHS, and *ORACLE_ COMMON*.

- Update the OHS configuration files.

- Apply OHS settings changes.

- Start the OPMN server process.

- Reassociate OHS to the Common Domain.

- Start the OHS instance.

## A.2.5  RUP Lite for BI Utility

The *RUP Lite for BI* utility automates changes to `BIInstance` configurations files required for Oracle Business Intelligence after upgrading.

# B

# Upgrade Orchestrator Properties Files

This appendix describes the properties files used by Upgrade Orchestrator.

To configure any property, follow the instructions for each property's description in the respective property file. The following properties files are required by Upgrade Orchestrator:

- pod.properties
- PRIMORDIAL.properties
- MIDTIER.properties
- IDM.properties
- OHS.properties

*Table B–1    pod.properties*

| Property Name | Mandatory | Description |
| --- | --- | --- |
| ORCHESTRATION_ CHECKPOINT_LOCATION | Yes | The shared location, available to all hosts in the environment, where files related to the orchestration checkpoint are saved. Select a shared mount point that has high disk I/O performance, especially for writing. Upgrade Orchestrator automatically creates *POD_NAME* under the directory you specify. It is a best practice to not use *ORCH_LOCATION*/config as a value for this property. |
| ORCHESTRATION_ CHECKPOINT_ARCHIVE_ LOCATION | Yes | The shared location, available to all hosts in the environment, where files related to the orchestration checkpoint are saved. Select a shared mount point that has high disk I/O performance, especially for writing. Upgrade Orchestrator automatically archives the checkpoint file stored under the *POD_NAME* directory under the directory specified by the ORCHESTRATION_ CHECKPOINT_LOCATION. property. It is a best practice to not use *ORCH_LOCATION*/config as a value for this property. |
| HOSTNAME_PRIMORDIAL | Yes | The host name of your Oracle Fusion Applications primordial host. This must be one and only one host name. |
| HOSTNAME_MIDTIER | Yes | A comma separated list of all host names of your Oracle Fusion Applications MidTier hosts. In Oracle VM environments, this must be a comma separated list of host names for primary, secondary, BI and OSN hosts. |

**Table B–1  (Cont.) pod.properties**

| Property Name | Mandatory | Description |
|---|---|---|
| HOSTNAME_PRIMARY | Yes | A comma separated list of all host names of your Oracle Fusion Applications primary hosts. This is applicable only for Oracle VM environments. |
| HOSTNAME_SECONDARY | Yes | A comma separated list of all host names of your Oracle Fusion Applications secondary hosts. This is applicable only for Oracle VM environments. |
| HOSTNAME_BIINSTANCE | Yes | A comma separated list of all host names of your Oracle Fusion Applications BI hosts. This is applicable only for Oracle VM environments. |
| HOSTNAME_OSN | Yes | This property is not applicable. |
| HOSTNAME_OHS | Yes | A comma separated list of all host names for the Oracle Fusion Applications Webtier (APPOHS). |
| HOSTNAME_IDMOID | Yes | Host name, virtual or actual, of the OID server, for example, `server_name.oracleoutsourcing.com`. |
| HOSTNAME_IDMOIM | Yes | Host name, virtual or actual, of the OIM server, for example, `server_name.oracleoutsourcing.com`. |
| HOSTNAME_IDMOHS | Yes | Host name, virtual or actual, of the AuthOHS server, for example, `server_name.oracleoutsourcing.com`. |
| EMAIL_TO_RECIPIENT | Yes | A comma separated list of email addresses to whom the upgrade notifications are sent. Test that recipients can receive emails by sending a test mail using sendmail or using the SMTP configuration specified in the SMTP_* properties if sendmail is not configured on this host. |
| EMAIL_CC_RECIPIENT | No | A comma separated list of email addresses to whom the upgrade notifications are sent as copies. Test that recipients can receive emails by sending a test mail using sendmail or using the SMTP configuration specified in the SMTP_* properties if sendmail is not configured on this host. |
| EMAIL_SENDER | No | The email address of the sender from which you want notifications to be sent. This must be a single value, such as `no-reply@domain.com`. |
| EMAIL_DEFAULT_ENGINE | Yes | Valid email engine that can be used on all hosts for this pod. The default value is `/usr/sbin/sendmail`. |
| EMAIL_PROTOCOL | No | Value must always be `smtp` as that is only supported protocol. |
| SMTP_HOSTNAME | No | The valid smtp host name. The default value is localhost. |
| SMTP_PORT_NUMBER | No | The SMTP protocol port number. |
| SMTP_AUTHORIZATION | No | A true or false value to indicate whether authorization key is used to connect to the SMTP server. The default value is false. |
| SMTP_AUTH_USER | No | The SMTP authorized user id. |
| SMTP_AUTH_PASSWORD | No | The SMTP authorized password. |
| SMTP_AUTH_ENCRYPTED_PASSWORD | No | The encrypted SMTP authorized password. If this property is empty, the SMTP_AUTH_PASSWORD value is used. |

**Table B–1  (Cont.)  pod.properties**

| Property Name | Mandatory | Description |
|---|---|---|
| SMTP_SOCKETFACTORY_CLASS | No | The factory class name to connect to the SMTP server. |
| REL6_REPOSITORY_LOCATION | No | The location where the Release 6 repository is downloaded to a shared mount, for example *SHARED_ LOCATION*/11.1.6.0.0/Repository. As a best practice, it should be on the shared mount that is shared across all pods or environments. This is mandatory only for chained upgrade from Release 5 to Release 6 to Release 7. |
| REL7_REPOSITORY_LOCATION | Yes | The location where the Release 7 repository is downloaded to a shared mount, for example *SHARED_ LOCATION*/11.1.7.0.0/Repository. As a best practice, it should be on the shared mount that is shared across all pods or environments. |
| SHARED_UPGRADE_LOCATION | Yes | The temporary directory where Upgrade Orchestrator copies files and perform write operations. Select a shared mount point that is shared across all hosts for a given pod/environment that has high disk I/O performance, especially for writing. You can clean up this area after your upgrade is complete. The default value is /u01/*SHARED_UPGRADE_LOCATION*. |
| THREAD_POOL_SIZE | Yes | This property is used for parallel execution of tasks within orchestration. You can choose to change the default value of 10 to a different numeric value if you want to control how many tasks run in parallel. For example, a value of 1 means everything runs sequentially, a value of 2 means only two tasks can run in parallel. |
| PATCH_CONFLICT_MANAGER_ LOCATION | Yes | The location of the patch conflict manager utility that you create in Section 2.3.2.1, "Patch Conflict Manager Directory." The default value is/u01/PatchConflictManager. |
| SAAS_ENV | Yes | This property should be set to true only if your Oracle VM environments are created in the Oracle Cloud Customer Environment. |
| SAAS_FACONTROL_SCRIPTS_ LOCATION | No | This property is not applicable. |
| PRE_REL6_SAAS_FACONTROL_ SCRIPTS_LOCATION | No | This property is not applicable. |
| SHARED_RDBMS_HOME | No | This property is not applicable. |
| REL6_SAAS_LCM_INSTALLER_ DIR | No | This property is applicable to Oracle Fusion Applications VMs only. This is the directory where FASAASLCMTOOLS.zip is downloaded and unzipped. As a best practice it should be on the shared mount that is shared across all pods/environments. This is mandatory only for the chained upgrade from Release 5 to Release 6 to Release 7. *SHARED_ LOCATION*/11.1.6.0.0/fasaaslcmtools is an example. |
| REL7_SAAS_LCM_INSTALLER_ DIR | Yes for Oracle VM | This property is applicable to Oracle Fusion Applications VMs only. This is the directory where FASAASLCMTOOLS.zip is downloaded and unzipped. As a best practice it should be on the shared mount that is shared across all pods/environments. *SHARED_ LOCATION*/11.1.7.0.0/fasaaslcmtools is an example. |

*Table B–1   (Cont.) pod.properties*

| Property Name | Mandatory | Description |
|---|---|---|
| ORCH_REPORT_LOCATION | No | A shared location accessible to all hosts that is used to save the upgrade report, as described in Section 1.3.4, "Oracle Fusion Applications Orchestrator Upgrade Report." |
| REL6_DOWNLOADED_PATCHES_LOCATION | No | The location of the post-release 6 patches that are identified as critical for upgrade, as described in Section 2.3.5.2, "Download and Unzip Mandatory Post-Release 6 Patches." This directory should be on a shared mount point shared across all hosts and ideally all pods, for example, *SHARED_LOCATION/*11.1.6.0.0_post_repo_patches. |
| REL7_DOWNLOADED_PATCHES_LOCATION | No | The location of the post-release 7 patches that are identified as critical for upgrade, as described in Section 2.3.6.3, "Download and Unzip Mandatory Post-Release 7 Patches." This directory should be on a shared mount point shared across all hosts and ideally all pods, for example, *SHARED_LOCATION/*11.1.7.0.0_post_repo_patches. |
| HC_OVERRIDE_FILES | No | The location of the directory that contains Health Checker configuration override files. The default value is *APPLICATIONS_CONFIG*/fapatch/healthchecker. |
| FORCE_OSN_ENABLED | No | This property is set to false by default and should be ignored. |

*Table B–2   PRIMORDIAL.properties*

| Property Name | Mandatory | Description |
|---|---|---|
| REL7_LP_REPOSITORY_LOCATION | Yes, if upgrading languages | The location of all Release 7 Language Pack repositories, as described in Section 2.3.6.2, "Download and Unzip Release 7 Language Packs." This directory should be on a shared mount point shared across all pods/environments, for example *SHARED_LOCATION/*11.1.7.0.0/LPRepository /u01/rel7LPRepositoryLocation. |
| REL6_RUPINSTALLER_UPGRADE_PARAM | No | You can leave this property blank because its value is automatically set by Upgrade Orchestrator during the upgrade. Alternatively, you can provide a space separated list of command line options passed to the RUP and Language Pack installers. For a list of options, refer to "Table 3-6" in the *Oracle Fusion Applications Administrator's Guide*. If you set this parameter manually, use only -D options. Do not use -J-D options. |
| REL7_RUPINSTALLER_UPGRADE_PARAM | No | You can leave this property blank because its value is automatically set by Upgrade Orchestrator during the upgrade. Alternatively, you can provide a space separated list of command line options passed to the RUP and Language Pack installers. For a list of options, refer to "Table 3-6" in the *Oracle Fusion Applications Administrator's Guide*. If you set this parameter manually, use only -D options. Do not use -J-D options. |

*Table B–2    (Cont.) PRIMORDIAL.properties*

| Property Name | Mandatory | Description |
|---|---|---|
| MANIFEST_FILE | Yes | The file name and location for the .xml manifest file for the host type and the upgrade level.<br><br>For a release 7 upgrade, the value should be `ORCH_LOCATION/config/rel7_primordial.xml`.<br><br>For multi-hop upgrade, the value should be `ORCH_LOCATION/config/rel5-7_primordial.xml`. |
| APPLICATIONS_BASE | Yes | The top-level directory for the Oracle Fusion Applications binaries. The default value is `/u01/APPLTOP`. |
| JRE_LOC | Yes | The absolute path where the Java Runtime Environment is installed. This option does not support relative paths. The default value is `/u01/APPLTOP/fusionapps/jdk6`. |
| CSF_SYSTEM_USERS_ENCRYPTED_INI | Yes | The absolute path and filename for the encrypted .ini file for adding new system users, for example, `/APPTOP/instance/lcm/admin/pcu/system_user_encrypted.ini`. For more information, see Section 2.4.2.4, "Prepare to Register System User Information." |
| CSF_ENCRYPTED_FILE | Yes | The absolute path and filename for the CSF encrypted file generated by the iniGen.sh script. This property is used by orchestration to pass the value to schemaPasswordChangeTool.sh. For more information, see Section 2.4.2.3, "Prepare to Register Database Schema Information." |
| SKIP_UPGRADE_FOR_LANGUAGE | No | A comma separated list of languages that you do not want orchestration to upgrade. The list items must:<br><br>■ Meet ISO language code convention<br><br>■ Be a previously installed language<br><br>■ Not be the JAZN policy store language |

*Table B–3    MIDTIER.properties*

| Property Name | Mandatory | Default Value |
|---|---|---|
| APPLICATIONS_BASE | Yes | The top-level directory for the Oracle Fusion Applications binaries. The default value is `/u01/APPLTOP`. |
| MANIFEST_FILE | Yes | The file name and location for the .xml manifest file for the host type and the upgrade level.<br><br>For a release 7 upgrade, the value should be `ORCH_LOCATION/config/rel7_midtier.xml`.<br><br>For multi-hop upgrade, the value should be `ORCH_LOCATION/config/rel5-7_midtier.xml`. |
| JRE_LOC | Yes | The absolute path where the Java Runtime Environment is installed. This option does not support relative paths. The default value is `/u01/APPLTOP/fusionapps/jdk6`. |

*Table B–3 (Cont.) MIDTIER.properties*

| Property Name | Mand atory | Default Value |
|---|---|---|
| RUPLITE_DOMAIN_CONFIG_ COPY_LOCATION | No | The read/write location to copy the `ruplite` domain config folder and files from the primordial host after RUP Installer Part 1 completes. If you do not have local domains, you can leave this property blank. This location must be local where local domains exists on the Midtier host and not the shared mount point. |
| | | If you do not have local domains, you can leave this properly blank. The default value is `/u01/ruplitedomain`. |

*Table B–4 IDM.properties*

| Property Name | Mandatory | Default Value |
|---|---|---|
| MANIFEST_FILE | Yes | The file name and location for the .xml manifest file for the host type and the upgrade level. |
| | | For a release 7 upgrade, the value should be *ORCH_LOCATION*/config/rel7_ idm.xml. |
| | | For multi-hop upgrade, the value should be *ORCH_LOCATION*/config/rel5-7_ idm.xml. |
| JRE_LOC | Yes | The absolute path where the Java Runtime Environment is installed. This option does not support relative paths. The default value is /u01/APPLTOP/fusionapps/jdk6. |
| IDM_SETUP_TYPE | Yes | Set this property to IDM node types. Valid values are SINGLE, 3-NODE, AND 4-NODE. The default value is 4-NODE. |
| LOG_LOCATION | Yes | The location for all logs to be written. This directory can be host specific or it can be on a shared mount. Select a directory that has high disk I/O performance especially for writing. |

*Table B–5 OHS.properties*

| Property Name | Mandatory | Default Value |
|---|---|---|
| APPLICATIONS_BASE | Yes | The top-level directory for the Oracle Fusion Applications binaries. The default value is /u01/APPLTOP. |
| MANIFEST_FILE | Yes | The file name and location for the .xml manifest file for the host type and the upgrade level. |
| | | For a release 7 upgrade, the value should be *ORCH_LOCATION*/config/rel7_ ohs.xml. |
| | | For multi-hop upgrade, the value should be *ORCH_LOCATION*/config/rel5-7_ ohs.xml. |

**Table B–5   (Cont.) OHS.properties**

| Property Name | Mandatory | Default Value |
| --- | --- | --- |
| RUPLITEOHS_UNZIP_LOCATION | Yes | Specify a location, local to the OHS host, where the webgate install zip file should be unzipped, to be used by the RUP Lite for OHS upgrade, for example, `/u01/webgate`. |
| JRE_LOC | Yes | The absolute path where the Java Runtime Environment is installed. This option does not support relative paths. An example is `ORCH_LOCATION/`jdk. |
| LOG_LOCATION | Yes | Location for logs to be written. |
| WT_MW_HOME | Yes | Location of the web tier `MW_HOME`, for example, `/oracle/work/MW_HOME`. If you have scaled out OHS hosts, copy this property for each OHS host, prefixed with the host name of the host to indicate the web tier `MW_HOME` location on the specific host. |
| WT_ORACLE_HOME | Yes | Location of the web tier Oracle WT1 directory, which is a sub-directory under `WT_MW_HOME`, for example: `/oracle/work/MW_HOME/Oracle_WT1`. If you have scaled out OHS hosts, copy this property for each OHS host, prefixed with the host name of the host to indicate the web tier Oracle WT1 location on the specific host. |
| WT_CONFIG_HOME | Yes | Location of the web tier instance directory, for example, `/oracle/work/MW_HOME/Oracle_WT1/instances/instance1`. If you have scaled out OHS hosts, copy this property for each OHS host, prefixed with the host name of the host to indicate the web tier `WT_CONFIG_HOME` location on the specific host. |
| OHS_INSTANCE_ID | Yes | The OHS instance ID on the host. Normally this is ohs1 and is the value for ias_component id in the opmn.xml file. If you have scaled out OHS hosts, copy this property for each OHS host, prefixed with the host name of the host to indicate the `OHS_INSTANCE_ID` on the specific host. |
| OHS_UPGRADE_BINARIES_ HOSTNAME | Yes | Comma separated list of your OHS host names which do not share the binaries. |

# C

# Platform Specific Pre-Upgrade Steps

This appendix describes the pre-upgrade steps for non-Linux and non-Windows platforms.

This appendix includes the following topics:

- Loading New Schemas in Release 7 From Respective RCUs
- Set Environment Variables for AIX

## C.1 Loading New Schemas in Release 7 From Respective RCUs

The following schemas were added in Release 7 of Oracle Fusion Applications: IAU, TOPOLOGY_MANAGER, FUNCTIONAL_SETUP_MANAGER, and OSN.

The Oracle Fusion Applications RCU is available only on Windows and Linux platforms. For other platforms, such as Solaris Sparc, Solaris X64 and AIX, you must install and run the RCU from a Windows or Linux machine to load the new schemas.

Perform the steps in this section to prepare the RCU on Windows or Linux:

1.  Copy or mount the Oracle Fusion Applications Release 7 Repository on Linux or Windows machine.

2.  Locate the appropriate RCU software for your platform.

    a.  For IAU Schema loading:

        –   For Linux, go to *REPOSITORY_LOCATION*/installers/apps_rcu/linux and locate the rcuHome_fusionapps_linux.zip file. Extract the contents of rcuHome_fusionapps_linux.zip to a folder on the Linux system.

        –   For Windows, go to *REPOSITORY_LOCATION*/installers/apps_rcu/windows and locate the rcuHome_fusionapps_win.zip file. Extract the contents of rcuHome_fusionapps_win.zip to a folder on the Windows system.

        –   Refer to these locations as *IAU_RCU_HOME*.

    b.  Topology Manager RCU software:

        –   For Linux, the RCU is located at *REPOSITORY_LOCATION*/installers/tmrcu.

        –   For Windows, the RCU is located at *REPOSITORY_LOCATION*\installers\tmrcu\windows\tmrcu.

        –   Refer to these locations as *TM_RCU_HOME*.

    c.  The Functional Setup Manager RCU software:

> > – For Linux, the RCU is located at *REPOSITORY_ LOCATION*/installers/fsrcu.
> >
> > – For Windows, the RCU is located at *REPOSITORY_ LOCATION*\installers\fsrcu\windows\fsrcu.
> >
> > – Refer to these locations as *FS_RCU_HOME*.
>
> **d.** The OSN RCU software:
>
> > – For Linux, go to *REPOSITORY_LOCATION/*installers/apps_rcu/linux to find the rcuHome_fusionapps_linux.zip file and extract its contents.
> >
> > – For Windows, go to *REPOSITORY_LOCATION*\installers\apps_rcu\windows to find the rcuHome_fusionapps_windows.zip file and extract its contents.
> >
> > – Refer to these locations as *OSN_RCU_HOME*.

**3.** Load the respective RCUs by running the following commands:

> **a.** Run the following command from *IAU_RCU_HOME* to create the IAU schema:
>
> ```
> IAU_RCU_HOME/bin/rcu -silent -createRepository -databaseType ORACLE
> -connectString db_server:db_port/db_sid -dbUser sys -dbRole sysdba
> -schemaPrefix FUSION -component FUSION_IAU
> ```
>
> You are prompted for the following values:
>
> > – Sys password
> >
> > – FUSION_IAU password
> >
> > – FUSION_IAU_APPEND password
> >
> > – FUSION_IAU_VIEWER password
>
> **b.** Run the following command from *TM_RCU_HOME* to create the Topology Manager component for the new schema:
>
> ```
> TM_RCU_HOME/bin/rcu -silent -createRepository -databaseType ORACLE
> -connectString db_server:db_port/db_sid -dbUser sys -dbRole sysdba
> -component TOPOLOGY_MANAGER
> ```
>
> You are prompted for the following values:
>
> > – Sys password
> >
> > – FUSION_SETUP password
> >
> > – Schema Name for FUSION as FUSION (not changeable)
> >
> > – Schema Name for FUSION_RUNTIME as FUSION_RUNTIME (not changeable)
> >
> > – RCU_MODE as UPGRADE (not changeable)
>
> **c.** Run the following command from *FS_RCU_HOME* to create the Functional Setup Manager component for the new schema:
>
> ```
> FS_RCU_HOME/bin/rcu -silent -createRepository -databaseType ORACLE
> -connectString db_server:db_port/db_sid -dbUser sys -dbRole  sysdba
> -component FUNCTIONAL_SETUP_MANAGER
> ```
>
> You are prompted for the following values:
>
> > – Sys password
> >
> > – FUSION_SETUP password

- Schema Name for FUSION as FUSION (not changeable)

- Schema Name for FUSION_RUNTIME as FUSION_RUNTIME (not changeable)

- RCU_MODE as UPGRADE (not changeable)

- APPLTOP directory name (Note that this parameter is not used in the RCU. You can choose to provide a dummy value, such as `/tmp/dummy`.)

- ADPATCH database defaults file directory name (Note that this parameter is not used in the RCU. You can choose to provide dummy value, such as `/tmp/dummy`.)

**d.** Run the following command from `OSN_RCU_HOME` to load the OSN RCU:

```
OSN_RCU_HOME/bin/rcu  -silent -createRepository -databaseType ORACLE
-connectString db_server:db_port/db_sid -dbUser sys -dbRole  sysdba
-schemaPrefix FUSION -component FUSION_SOCIAL -component FUSION_SOCIAL_
VIEWS -component FUSION_SOCIAL_CEF
```

You are prompted for the following values:

- Sys password

- FUSION_SOCIAL password

- FUSION_SOCIAL_VIEWS password

- FUSION_SOCIAL_CEF password

## C.2 Set Environment Variables for AIX

Set the `SKIP_ROOTPRE` environment variable before starting Upgrade Orchestrator on an AIX platform, as follows:

**1.** Set the `SKIP_ROOTPRE` environment variable:

```
export SKIP_ROOTPRE=TRUE
```

**2.** Set the `CONFIG_JVM_ARGS` environment variable:

```
export CONFIG_JVM_ARGS=-Xmx512m
```

To proceed with the upgrade, perform the steps in Chapter 4, "Upgrading to Oracle Fusion Applications Release 7".

# D

# Oracle Identity Manager Upgrade Properties

This appendix lists the example values to use when upgrading Oracle Identity Manager for Oracle Fusion Applications Release 7.

Use these values when editing the file /u01/oim/*OIM_ HOME*/server/bin/oimPS1PS2upgrade.properties

```
Section 1: Neccessary env variables[Mandatory]
java_home=<Put Location of Java Home here>


#For domain level configurations  put here your admin server related credentials
[Mandatory]

weblogic_user=<put your Weblogic Admin Username Here>
weblogic_host=<put your weblogic admin server host name here>
weblogic_port=<put your weblogic admin server port here>
weblogic.server.dir=<Enter PATH of your weblogic Installation dir>
#Section 2: Env Dependent Variables.

#Put value as true if your env is LDAPSYNC Enabled, you can set this var false or
ignore this if your env is non LDAPSYNC.
#LDAPSYNCEnabled=<Set true/false here>
#Put value true if your env is FA, you can set this var false or ignore this if
your env is non FA.
#FAEnabled=<Set true/false here>
#Put value true if your env is FA-SOD, you can set this var false or ignore this
if your env is non FA-SOD.
#FASODEnabled=<Set true/false here>
#Put value true if your env is Multi-Tenant, you can set it false or ignore this
if your env is a non Multi-Tenant.
#MTEnabled=<Set true/false here>


#OID Details, Needed only if you have LDAPSYNC Enabled in your env.[if
LDAPSYNCEnabled=true]
#oid_user=<Put your oid username here for eg. oid_user=cn=orcladmin>


#For uptaking the direct based user/role creation callbacks specify: update_
callbacks=DIRECT
#For uptaking the recon based user/role creation callbacks specify: update_
callbacks=RECON
#For uptaking both of these user/role creation callbacks specify: update_
callbacks=ALL
#For ignorning user/role creation callbacks from both DIRECT/RECON specify:
update_callbacks=NONE
```

```
#This is case insensitive. Value can be provided in any case.
#There is no impact on existing functionality. This is a new feature which can be
uptaken by adding this new property.The valse here is set for
default as NONE.
update_callbacks=NONE


#Section-3: For passwords if you dont want to put password </optional> in this
file just comment it out from here, you will be prompted for it in runtime.

#weblogic_password=<put weblogic admin password here>
#OIM.DBPassword=<put your oimOperations DB password here>
#oid_password=<If your env is ldapsync enabled, put your oid password here>
#mdsDB.password=<Put your mds DB password here>


#Section 4: Auto discovered parameters.

#All parameter beyond this section are discovered automatically from OIM
installation and should not be specified here. They can be overridden only on
Oracle Support's recommendation to handle any special requirements.

#ant_home=<put your ant home here, in a typical install it should be at MW_
HOME\modules\org.apache.ant_1.7.1>

#appserver.type=wls

#oimOperations DB configuration variables
#operationsDB.user=<Put your OIM schema user name here>
#operationsDB.host=<Put your oimdb hostname here>
#operationsDB.port=<Put your OIM DB port here>
#Please provide servicename, SID will not work.
#operationsDB.serviceName=<Put your oim-db servicename here>

#mds DB configuration variables      [If Your env is FA or MT Enabled You will need
to put these credentials]
#mdsDB.user=<Put your mds-db schema user name here>
#mdsDB.host=<Put your mds-db schema hostname here>
#mdsDB.port=<Put your mds-db schema port here>
#Please provide servicename, SID will not work.
#mdsDB.serviceName=<Put your mds db servicename here>

#oid related details [Only if you have LDAPSYNC Enabled in your env.]
#oid_host=<put your oid hostname here>
#oid_port=<put your oid port here>

#oim specific domain level parameters [Only if you have FA Enabled in your env.]
#oimserver_host=<put your oimserver hostname here>
#oimserver_port=<put your oimserver port here>
#oim_servernamr=<Put the name of oim managed server, if your env is cluster put
the name of cluster instead>

#SOA specific details
#soa_home=<put your SOA home location here>

## Uncomment the following property to disable the validation of the input params
##skipValidate=true
```

# E

# Stopping and Starting Identity Management Related Servers

This appendix describes how to start, stop and restart the various components of the Oracle Enterprise Deployment for Identity Management.

This appendix contains the following topics.

## E.1  Starting, Stopping, and Restarting Oracle HTTP Server

Prior to starting/stopping the Oracle HTTP server:

- Set `ORACLE_INSTANCE` to *WEB_ORACLE_INSTANCE*.

- Set `ORACLE_HOME` to *WEB_ORACLE_HOME*.

- Ensure that the *ORACLE_HOME*`/opmn/bin` appears in the *PATH*.

### E.1.1  Starting Oracle HTTP Server

Start the Oracle Web Tier by issuing the command:

```
opmnctl startall
```

### E.1.2  Stopping Oracle HTTP Server

Stop the Web Tier by issuing the command

```
opmnctl stopall
```

to stop the entire Web Tier or

```
opmnctl stoproc process-type=OHS
```

to stop Oracle HTTP Server only.

### E.1.3 Restarting Oracle HTTP Server

You can restart the Web Tier by issuing a `Stop` followed by a `Start` as described in the previous sections.

To restart the Oracle HTTP server only, use the following command.

```
opmnctl restartproc process-type=OHS
```

# E.2 Starting, Stopping, and Restarting Oracle Identity Manager

Start and stop Oracle Identity Manager and Oracle SOA Suite servers as follows:

### E.2.1 Starting Oracle Identity Manager

To start the Oracle Identity Manager Managed Server(s), log in to the WebLogic console at: `http://ADMIN.mycompany.com/oamconsole`

Then proceed as follows:

1.  Select **Environment - Servers** from the Domain Structure menu.

2.  Click the **Control** tab.

3.  Select **SOA Servers (WLS_SOA1 and/or WLS_SOA2)**.

> **Note:** You can start the Oracle Identity Manager and Oracle SOA Suite servers independently of each other. There is no dependency in their start order. However, the SOA server must be up and running for all of the Oracle Identity Manager functionality to be available.

4.  Click the **Start** button.

5.  Click **Yes** when asked to confirm that you want to start the server(s).

6.  After WLS_SOA1 and/or WLS_SOA2 have started, select WLS_OIM1 and/or WLS_OIM2

7.  Click **Start**.

8.  Click **Yes** when asked to confirm that you want to start the server(s).

### E.2.2 Stopping Oracle Identity Manager

To stop the Oracle Identity Manager Managed Server(s), log in to the WebLogic console at: `http://ADMIN.mycompany.com/oamconsole`

Then proceed as follows:

1.  Select **Environment - Servers** from the Domain Structure menu.

2.  Click the **Control** tab.

3.  Select **OIM Servers (WLS_OIM1 and/or WLS_OIM2)** and **(WLS_SOA1 and/or WLS_SOA2)**.

4.  Click the **Shutdown** button and select **Force Shutdown now**.

5.  Click **Yes** when asked to confirm that you want to shutdown the server(s).

### E.2.3  Restarting Oracle Identity Manager

Restart the server by following the `Stop` and `Start` procedures in the previous sections.

## E.3  Starting and Stopping Oracle Identity Federation Managed Servers

Start and stop Oracle Identity Federation Managed Servers as follows:

### E.3.1  Starting Oracle Identity Federation

To start the Oracle Identity Federation Managed Server(s), log in to the WebLogic console at: `http://ADMIN.mycompany.com/oamconsole`

Then proceed as follows:

1. Select **Environment - Servers** from the **Domain Structure** menu.

2. Click the **Control** tab.

3. Select **OIF Servers (WLS_OIF1 and/or WLS_OIF2)**.

4. Click **Start**.

5. Click **Yes** when asked to confirm that you want to start the server(s).

### E.3.2  Stopping Oracle Identity Federation

To stop the Oracle Identity Federation Managed Server(s), log in to the WebLogic console at: `http://ADMIN.mycompany.com/oamconsole`

Then proceed as follows:

1. Select **Environment - Servers** from the **Domain Structure** menu.

2. Click the **Control** tab.

3. Select **OIF Servers (WLS_OIF1 and/or WLS_OIF2)**.

4. Click **Shutdown** and select **Force Shutdown now**.

5. Click **Yes** when asked to confirm that you want to shut down the server(s).

### E.3.3  Restarting Oracle Identity Federation

Restart the server by following the previous Stop and Start procedures.

### E.3.4  Starting the EMAgent

Start the EMAgent by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl startall
```

You can verify that the instance started successfully by executing:

```
ORACLE_INSTANCE/bin/opmnctl status -l
```

### E.3.5  Stopping the Oracle Identity Federation Instances and EMAgent

Stop the Oracle Identity Federation Instance and EMAgent by executing the following command:

```
OIF_ORACLE_INSTANCE/bin/opmnctl stopall
```

## E.4 Starting, Stopping, and Restarting Oracle Access Manager Managed Servers

Start and stop Oracle Access Manager Managed Servers as follows:

### E.4.1 Starting an Access Manager Managed Server When None is Running

Normally, you start Access Manager managed servers by using the WebLogic console. After you have enabled Single Sign-On for the administration consoles, however, you must have at least one Access Manager Server running in order to access a console. If no Access Manager server is running, the only way you can start one is from the command line.

To start WLS_OAM1 manually, use the command:

```
MSERVER_HOME/bin/startManagedWeblogic.sh WLS_OAM1 t3://ADMINVHN:7001
```

where `7001` is `WLS_ADMIN_PORT` in Section A.3.

### E.4.2 Starting an Oracle Access Manager Managed Server When Another is Running

To start an Oracle Access Manager Managed Server when you already have another one running, log in to the WebLogic console at: `http://ADMIN.mycompany.com/oamconsole`

Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu.

2. Click the **Control** tab.

3. Select **OAM Servers (WLS_OAM1 and/or WLS_OAM2)**.

4. Click the **Start** button.

5. Click **Yes** when asked to confirm that you want to start the server(s).

> **Note:**   After you have enabled single sign-on for the administration consoles, ensure that at least one Oracle Access Manager Server is running to enable console access.
>
> If you have used the Oracle WebLogic console to shut down all of the Oracle Access Manager Managed Servers, then restart one of those Managed Servers manually before using the console again.
>
> To start WLS_OAM1 manually, use the command:
>
> ```
> MSERVER_HOME/bin/startManagedWeblogic.sh WLS_OAM1
> t3://ADMINVHN:7001
> ```

### E.4.3 Stopping Oracle Access Manager Managed Servers

To stop the Oracle Access Manager Managed Server(s), log in to the WebLogic console at: `http://ADMIN.mycompany.com/oamconsole`

Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu.

2. Click the **Control** tab.

3. Select **OAM Servers (WLS_OAM1 and/or WLS_OAM2)**.

4. Click the **Shutdown** button and select **Force Shutdown now**.

5. Click **Yes** when asked to confirm that you want to shut down the server(s).

## E.4.4 Restarting Oracle Access Manager Managed Servers

Restart the server by following the `Stop` and `Start` procedures in the previous sections.

# E.5 Starting, Stopping, and Restarting WebLogic Administration Server

Start and stop the WebLogic Administration Server as described in the following sections.

> **Note:** `Admin_user` and `Admin_Password` are only used to authenticate connections between Node Manager and clients. They are independent from the server administration ID and password and are stored in the *ASERVER_HOME*`/config/nodemanager/nm_password.properties` file.

## E.5.1 Starting WebLogic Administration Server

The recommended way to start the Administration server is to use WLST and connect to Node Manager:

```
cd ORACLE_COMMON_HOME/common/bin
./wlst.sh
```

Once in WLST shell, execute

```
nmConnect('Admin_User','Admin_Password','ADMINHOST1','5556', 'IDMDomain','ASERVER_
HOME')
nmStart('AdminServer')
```

Alternatively, you can start the Administration server by using the command:

```
DOMAIN_HOME/bin/startWeblogic.sh
```

## E.5.2 Stopping WebLogic Administration Server

To stop the Administration Server, log in to the WebLogic console at:
`http://ADMIN.mycompany.com/oamconsole`

Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu.

2. Click the **Control** tab.

3. Select **AdminServer(admin)**.

4. Click **Shutdown** and select **Force Shutdown now**.

5. Click **Yes** when asked to confirm that you want to shut down the Administration Server.

## E.5.3 Restarting WebLogic Administration Server

Restart the server by following the `Stop` and `Start` procedures in the previous sections.

## E.6  Starting and Stopping Oracle Virtual Directory

Start and stop Oracle Virtual Directory as follows.

### E.6.1  Starting Oracle Virtual Directory

Start system components such as Oracle Virtual Directory by typing:

```
ORACLE_INSTANCE/bin/opmnctl startall
```

You can verify that the system components have started by executing:

```
ORACLE_INSTANCE/bin/opmnctl status -l
```

### E.6.2  Stopping Oracle Virtual Directory

Stop system components such as Oracle Virtual Directory by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl stopall
```

## E.7  Starting and Stopping Oracle Internet Directory

Start and stop Oracle Internet Directory as follows.

### E.7.1  Starting Oracle Internet Directory

Start system components such as Oracle Internet Directory by typing

```
ORACLE_INSTANCE/bin/opmnctl startall
```

You can verify that the system components have started by executing:

```
ORACLE_INSTANCE/bin/opmnctl status -l
```

### E.7.2  Stopping Oracle Internet Directory

Stop system components such as Oracle Internet Directory by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl stopall
```

## E.8  Starting and Stopping Node Manager

Start and stop the Node Manager as follows:

### E.8.1  Starting Node Manager

If the Node Manager being started is the one that controls the Administration Server (IDMHOST1 or IDMHOST2), then prior to starting the Node Manager, set `JAVA_OPTIONS` to `-DDomainRegistrationEnabled=true` and issue the commands:

```
cd IAM_MW_HOME/wlserver_10.3/server/bin
./startNodeManager.sh
```

### E.8.2 Stopping Node Manager

To stop Node Manager, kill the process started in the previous section.

### E.8.3 Starting Node Manager for an Administration Server

Set the environment variable `JAVA_OPTIONS` to `-DDomainRegistrationEnabled=true` and issue the commands:

```
cd IAM_MW_HOME/wlserver_10.3/server/bin
./startNodeManager.sh
```

> **Note:** It is important to set `-DDomainRegistrationEnabled=true` whenever you start a Node Manager that manages the Administration Server.