Oracle® Fusion Applications

Upgrade Guide

Release 12 (11.12.x.0.0)
E70415-09
March 2018

Oracle Fusion Applications Upgrade Guide, Release 12 (11.12.x.0.0)

E70415-09

Primary Author: Claudia Gomez, Keila Chavez. Special authoring thanks to: Bor-Ruey Fu, Praveena Vajja, Karen Orozco Sanchez, David Lam, Ranjit Mulye.

Contents

7 Upgrade Oracle Identity Management to Release 12

8 Run Post-Upgrade Tasks

9 Monitor and Troubleshoot the Upgrade

10 Additional Information About Upgrade Orchestrator

Preface

This guide describes how to upgrade an Oracle Fusion Applications environment.

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

Related Documents

For more information, see the following documents in the Oracle Fusion Applications technology library:

- *Oracle Fusion Applications Administrator's Guide*
- *Oracle Fusion Applications Installation Guide*
- *Oracle Fusion Applications Patching Guide*

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.

New and Changed Features for Release 12 (11.12.x.0.0)

In this user guide, the nomenclature "11.12.x.0.0", where "x" is a number, is used to indicate the release and patch releases for which the guide is applicable. When using this document be sure to replace "x" with the number of the release that is being used.

Oracle Fusion Applications Release 12 (11.12.x.0.0) includes the following new and changed upgrade features:

- Direct Upgrade allows the upgrade from Releases 8 (and up) to Release 12. Direct upgrade is available for the supported platforms.
- A post upgrade step was added for upgrading the database to 12c.

  The following table shows other changes and new features introduced in Release 11.12.x.0.0:

Table 1 New Features in Release 11.12.x.0.0

Feature/Topic	Location in this Document / Brief Description	Feature Summary
IDM Decoupling	NA	IDM decoupling includes the following changes: – Upgrade of IDM from R1PS2 to R2PS3 – Removal of OIM, SOA, and OIF server with fed migration at OAM

Table 1 (Cont.) New Features in Release 11.12.x.0.0

Feature/Topic	Location in this Document / Brief Description	Feature Summary
PSR server consolidation	NA	Reduces FA footprint by co-deploying application to eliminate 17 managed servers from CRM, HCM, FIN, SCM and IC domains.Consolidation is done automatically for existing and scaled out managed servers during upgrade. There is no impact to upgrade tasks. For OVM environments only, if SCM Financial Orchestration server or SCM Pricing Application (now in the Configurator server in Release 12) is already scaled out before upgrade, then Internal Scale Out utility can be used to redo scale out accordingly.
New Memory Requirements	Verify Memory Requirements	Includes changes in memory requirements for the hosts upgrading to Release 11.12.x.0.0.
Installation of Fusion Middleware (FMW) PS7 / JDK 7	Uptake of FMW PS7 and JDK 7	After upgrade, the Fusion Middleware in the Fusion Applications environment is upgraded to 11g Patch Set 7 (PS7). Additionally, the version of JDK is upgraded from JDK6 to JDK7. These upgrades are done automatically in the upgrade flow. No manual task is required.
RDBMS 12c	Upgrade Oracle Fusion Applications and Oracle Identity Management Databases to 12c RDBMS	Newer tech stack. After upgrading to Release 12, the databases for FA environments can be upgraded to RDBMS 12c. Release 12 upgrade is only supported with the databases still at 11gR2 (11.2.0.4). Newly provisioned Release 12 FA environments will be on RDBMS 12c.

Table 1 (Cont.) New Features in Release 11.12.x.0.0

Feature/Topic	Location in this Document / Brief Description	Feature Summary
Apply Fusion Application Patch Bundles (FA PB) during upgrade	Stage Fusion Applications High-Water Mark Patch Bundles Download and Unzip Mandatory Post-Release 12 Patches	Reduces downtime by eliminating the need for applying FA PB patching after upgrade. The patch content for FA PBs will be applied in parallel during upgrade. In addition, if there are post-release patches (post repo) associated with FA PBs, the post repo will be applied during upgrade. FA PBs and post repo (if needed) must be staged before upgrade begins.
Apply Language Packs (LP) during upgrade	Download and Unzip Release 12 Language Packs	Reduces downtime by eliminating the extra time needed for applying each LP after upgrade. LPs will be applied in parallel during upgrade.LPs must be staged before upgrade begins.
Removal of the Patch Conflict Manager Utility (PCM)	Downloading and unzipping PCM is no longer required. The instruction has been removed from this guide.	Invoking PCM during upgrade flow is no longer needed.
Stage Patch Rollback Automation Script	Download and Unzip the Patch Rollback Automation Script	This script is downloaded and unzipped to roll back conflicting FMW components that cause PS6 to PS7 upgrade issues.
Policy Store Customization Lockdown	Direct Upgrade JAZN	No longer allows modifications to any Oracle shipped policies that will be reset to factory default and lock down starting Release 12 (some exceptions may exist). The policy store will be moved into FA DB.Enterprise roles will be deprecated. There is an associated pre-upgrade tasks to review policy, fixing before upgrade if an environment is upgraded from Release 9. No pre-upgrade task is required for this feature if the upgrade is from Release 11.

Table 1 (Cont.) New Features in Release 11.12.x.0.0

Feature/Topic	Location in this Document / Brief Description	Feature Summary
Health Check Override	Override Health Checks	The Health Checker (HC) Override includes the following changes: – Changes to location of HC override files – Staging of Health Check override ARUs
Check repository integrity after staging repository	Validate Repository	Run repository integrity check after the repository is staged. This check needs to be run only once per data center when the repository is staged. This is different from previous releases when the check had to be run in each invocation of upgrade.
Patching Performance and Resiliency Improvements	NA	Reduces patching time by pre-installing binaries in pre-downtime, performing patch validation in pre-downtime, deferring ODI and BI RPD imports to post downtime, etc. Improves resiliency with auto retry and auto correct for FA Patch Manager and Auto Patch. There is no impact to upgrade tasks.
Increase Tablespace for OTBI Schema	Ensure Free Tablespace for OTBI Schema	Recommended tuning before upgrade to avoid upgrade issues.
Update the Database and Middle Tier Credential Stores	Update the Database and Middle Tier Credential Stores	This task is required for retrofitting and securing the common user credential between the mid tier and database hosts.
Clean Up the Middle Tier Credential Store	Clean Up the Middle Tier Credential Store	This task is required for retrofitting and securing the common user credential between the mid tier and database hosts.
Enable / Disable Oracle Java Virtual Machine (OJVM) in the Database	Enable Oracle Java Virtual Machine in the Database Disable Oracle Java Virtual Machine Support	With database OJVM mitigation patch installed, you must enable OJVM before the upgrade. Then, disable OJVM after upgrade to allow the upgrade process to perform tasks that uses Java in the database hosts.

Other Significant Changes in this Document for Release 12 (11.12.x.0.0)

For Release 12 (11.12.x.0.0), this guide has been updated in several ways. The following are the sections that have been added or changed:

- Stage Fusion Applications High-Water Mark Patch Bundles
- Direct Upgrade JAZN
- Run OPSS Dup Tool
- Validate Repository
- Apply Database Patches for Release 12 (Solaris Only)
- Ensure FUSION_OTBI Schema Version Registry
- Enable Oracle Java Virtual Machine in the Database
- Ensure Free Tablespace for OTBI Schema
- Update the Database and Middle Tier Credential Stores
- Run Database Credential Store Retrofit Utility in Pods Where EM is Not Present
- Run the CSF Cache Utility Manually in Pods Where EM is Not Present
- Clean Up the Middle Tier Credential Store
- Run the CSF Cleanup Utility Manually
- Re-create IDM Schemas Manually (Solaris Only)
- Upgrade Oracle Fusion Applications and Oracle Identity Management Databases to 12c RDBMS
- Disable Oracle Java Virtual Machine Support
- Health Checker FileOwnerAndPermissionsCheck Error
- Troubleshoot Tagging of JAZN Policies
- Health Checker Overrides Across the Fleet
- Health Checker Overrides Customization
- Exclude a Plug-in in FA_pods_overrides.xml
- Exclude a Plug-in in FA_pods_overrides.xml for a Single Pod
- Exclude a Plug-in in FA_pods_overrides.xml for Multiple Pods
- Customization: Re-enable a Plug-in that is Disabled in all_overrides.xml
- Exclude a Plug-in with More Granularity
- Upgrade Oracle Identity Management to Release 12

1

Introduction to the Oracle Fusion Applications Upgrade

This section provides an introduction to the process of upgrading Oracle Fusion Applications to Release 12 (11.12.x.0.0). The following topics are discussed:

1.1 Upgrade Paths to Release 12

The following upgrade paths are supported for Release 12:

- Release 8 (11.1.8.0.0) to Release 12 (11.12.x.0.0)

  Note that this is a direct upgrade path, with no requirement to upgrade to Release 9, Release 10, or Release 11 during the upgrade process.

  Solaris platform supports direct upgrade from Release 8 (11.1.8.0.0) to Release 12 (11.12.x.0.0)

- Release 9 (11.1.9.x.0) to Release 12 (11.12.x.0.0)

  Note that this is a direct upgrade path, with no requirement to upgrade to Release 10 or Release 11 during the upgrade process.

- Release 10 (11.1.10.x.0) to Release 12 (11.12.x.0.0)

  Note that this is a direct upgrade path, with no requirement to upgrade to Release 11 during the upgrade process.

- Release 11 (11.1.11.x.0) to Release 12 (11.12.x.0.0)

1.2 High Level Checklist to Perform the Upgrade

The following checklist provides the list of tasks necessary to perform the upgrade to Release 12 (11.12.x.0.0):

Table 1-1 Checklist of Upgrade Tasks

Task Name	Task Description	Reference Link
Preliminary steps for the Upgrade	Information about the resources you must have access to before starting the upgrade	Preliminary Steps
System Requirements	System requirements that must be met for the system to be upgraded	System Requirements
Create Directories and Stage the Software	Details about the directories that must be created and the software and patches that must be downloaded and staged before starting the upgrade	Set Up Upgrade Directories and Obtain Software
Set Up Upgrade Orchestrator	Steps to set up the orchestration software, followed by additional preparation steps for the upgrade	Set Up Upgrade Orchestrator
Verify Environment Before Proceeding With Downtime	Steps to verify your environment before starting the upgrade	Verify Environment Before Proceeding to Downtime
Update Oracle Fusion Applications and Oracle Identity Management Databases	Steps to update the databases	Update the Oracle Fusion Applications and Oracle Identity Management Databases
Run steps to ensure system reliability	Steps to run checks to ensure system reliability	Run Pre-Downtime Checks
Run Pre-upgrade Steps During Downtime	Steps that must be run if upgrading from Release 8 or Release 9	Perform Pre-Upgrade Steps During Downtime
Update the Database and Middle Tier Credential Stores	Pre-upgrade steps that must be performed Before running RUP Installer	Update the Database and Middle Tier Credential Stores

Table 1-1 (Cont.) Checklist of Upgrade Tasks

Task Name	Task Description	Reference Link
Run Upgrade Orchestrator During Downtime	Steps to run Upgrade Orchestrator to perform the upgrade	Run Upgrade Orchestrator During Downtime
Pause Point 1 - Run RUP Lite for OVM in Pre-Root Mode (Oracle VM Only)	Steps to run RUP Lite for OVM in pre-root mode. This pause point applies only to Oracle VM environments	Pause Point 1 - Run RUP Lite for OVM in Pre-Root Mode (Oracle VM Only)
Pause Point 2 - Upgrade Oracle Identity Management to Release 12	Steps to upgrade Oracle Identity Management, followed by steps to update the status of the pause point task to proceed with the upgrade.	Pause Point 2- Upgrade Oracle Identity Management to Release 12
Pause Point 3 - Reload Orchestration	Steps to reload orchestration, followed by steps to update the status of the pause point task to proceed with the upgrade	Pause Point 3 - Reload Orchestration
Pause Point 4 - Run RUP Lite for OVM in Post-Root Mode (Oracle VM Only)	Steps to run RUP Lite for OVM in post-root mode. This pause point applies only to Oracle VM environments	Pause Point 4- Run RUP Lite for OVM in Post-Root Mode (Oracle VM Only)
Pause Point 5 - Create the Incremental Provisioning Response File	Steps to create the response file if incremental provisioning is run	Pause Point 5 - Create the Incremental Provisioning Response File
Pause Point 6 - Perform Incremental Provisioning	Steps to run incremental provisioning	Pause Point 6 - Perform Incremental Provisioning

Table 1-1 (Cont.) Checklist of Upgrade Tasks

Task Name	Task Description	Reference Link
Run Upgrade Orchestrator in the Downtime During Language Pack (LP) phase	Steps to run orchestration to perform LP upgrade tasks	Resume Upgrade Orchestrator
Run Post Upgrade Tasks	Required post upgrade tasks that must be performed after Upgrade Orchestrator runs to successful completion	Run Post-Upgrade Tasks
Troubleshoot the Upgrade	Possible failure and error scenarios that may occur during the upgrade, including solutions or workarounds	Monitor and Troubleshoot the Upgrade

1.3 Hosts, Directories, and Files Required by Upgrade Orchestrator

Before proceeding with the upgrade, get familiar with the following concepts and information:

- Host Types
- Directories and Files Required by Upgrade Orchestrator

1.3.1 Host Types

The Release 12 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. OIF is optional.
- **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**: Includes the following 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 of the managed servers for any application when they are not on the same host as the administration server of the same domain. Typically used when a domain spans two physical servers.
  - **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. See Scale Oracle Fusion Applications in the *Oracle Fusion Applications Installation Guide*.

1.3.2 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: This directory is created in a shared location, which is accessible to all hosts in the environment, including scaled out hosts. See Create Directories in a Shared Location.
- ORCHESTRATION_CHECKPOINT_LOCATION and ORCHESTRATION_CHECKPOINT_ARCHIVE_LOCATION: These directories are created under SHARED_LOCATION, where orchestration checkpoint related files are saved. See Create Orchestration Checkpoint Locations. These directory locations are stored as properties in the `pod.properties` file. See Table 11-1.
- SHARED_UPGRADE_LOCATION: This temporary directory is created to copy files and perform write operations. See Create the Shared Upgrade Location Directory.
- ORCH_LOCATION: This directory is created when unzipping `orchestration.zip` and is referred to as the orchestration directory. See Unzip Orchestration.zip.
- POD_NAME: This is the name used throughout this guide to refer to the directory created. It is possible to create the `POD_NAME` directory under ORCH_LOCATION.
- Manifest files: Manifest files are .xml type distribution files that are required by both Upgrade Orchestrator and Health Checker. These files are used throughout this guide to define specific tasks performed during the upgrade process.

1.4 Back Up Strategy

Before starting the upgrade process, knowledge of the backup requirements is needed, 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. Backups are manual steps and can be automated outside of Upgrade Orchestrator based on the IT requirements and processes.

The following components must be backed up:

- Oracle Fusion Applications, including the following:
  - Oracle Fusion Applications database
  - *`APPLICATIONS_BASE`* directory

  - *APPLICATIONS_CONFIG* directory
  - Oracle Identity Management database
  - Upgrade Orchestration directories
  - OHS and /etc/hosts files
  - Central Inventory
- OPSS Security Store: This component is backed up by Upgrade Orchestrator.

> **Note:**
>
> Back up the Oracle Fusion Applications upgrade at multiple stages during the upgrade process. It is recommended to back up the entire Fusion Applications environment, including the databases before and after the upgrade.

1.5 Plan the Downtime

Consider the following suggestions when planning the downtime for the upgrade:

- Perform pre-downtime steps ahead of time. See Prepare for the Release 12 Upgrade Before Downtime.
- Perform the database patching in a separate maintenance window. See Update the Oracle Fusion Applications and Oracle Identity Management Databases.
- Perform steps to check system reliability in pre-downtime mode after all prerequisites are met. See Run Pre-Downtime Checks .

1.6 Directories Structure Overview

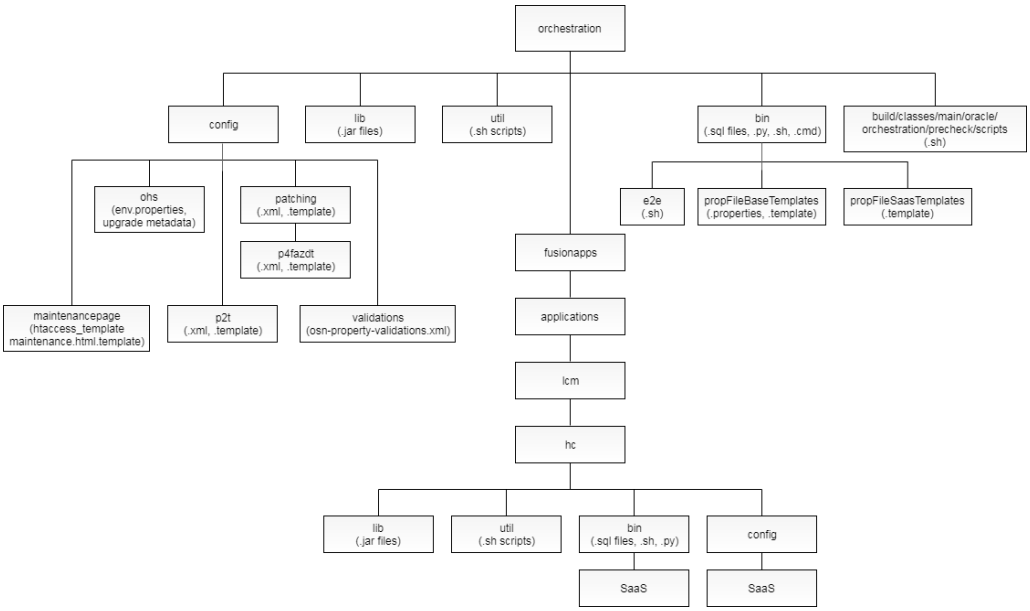
Upgrade Orchestrator references and uses the following directories:

- The ORCH_LOCATION Directory
- Download Directories
- Oracle Fusion Applications Shared Directories

1.6.1 The ORCH_LOCATION Directory

The following figure shows the directory structure that is created when the `Orchestration.zip` file is unzipped, and is referred to as *ORCH_LOCATION*. See Unzip Orchestration.zip.

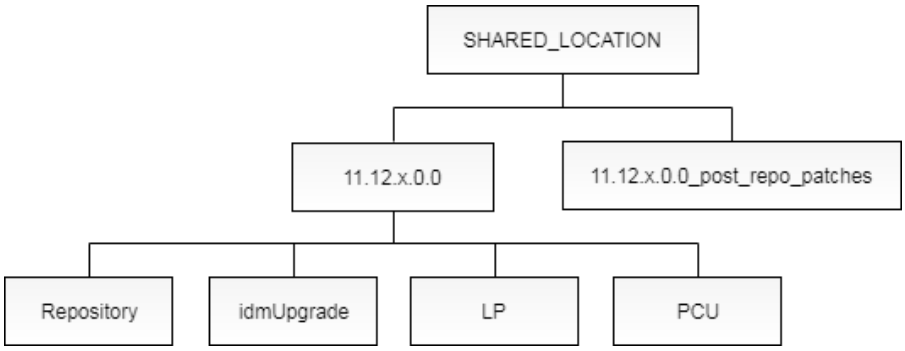
Figure 1-1 Directory Structure of Upgrade Orchestrator



1.6.2 Download Directories

The following figure shows the directory structure that is created during the preparation of the environment for the upgrade. There are specific files that must be downloaded into each of these directories. See Create Directories in a Shared Location.

Figure 1-2 Directory Structure of Downloaded Patches and Repositories



1.6.3 Oracle Fusion Applications Shared Directories

The following home directories are referenced during the upgrade steps:

- ***APPLICATIONS_CONFIG***

  The root directory for the Oracle Fusion Applications configuration and instance files.

- ***APPLICATIONS_BASE***

  The root directory for the Oracle Fusion Applications product binary files.

- ***FA_ORACLE_HOME***

  The Oracle Fusion Applications Oracle home directory. This directory is located under the *APPLICATIONS_BASE*/fusionapps directory (net/mount1/appbase/fusionapps). The /fusionapps directory is an Oracle Fusion Applications Middleware home (*APPLICATIONS_BASE*/fusionapps).

See Oracle Fusion Applications Shared Directory Structure in the *Oracle Fusion Applications Installation Guide*.

1.7 Incremental Provisioning

Incremental provisioning provides the ability to extend the Oracle Fusion Applications environments during the upgrade. This extension is done by adding product offerings that are introduced in a release that is higher than the release of the existing Oracle Fusion Applications environments. A product offering is a logical grouping of features and functionality of Oracle Fusion Applications.

To use incremental provisioning, the Provisioning Wizard from a prior release must have been used to create the environment. See Extend an Oracle Fusion Applications Environment Using Incremental Provisioning During Upgrade in the *Oracle Fusion Applications Installation Guide*. Alternatively, use incremental provisioning if the Oracle Fusion Applications environment is created from Oracle Fusion Applications Oracle Virtual Machine (VM) templates. See Deployment of Oracle VM Templates in the *Oracle Fusion Applications Installing and Managing in an Oracle VM Environment*.

Adding optional VM hosts for product offerings such as, Value Chain Planning (VCP) and Governance, Risk and Control (GRC) during upgrade for environments previously created from a prior release of Oracle Fusion Applications Oracle Virtual Machine (VM) templates is *not* supported.

2

Prepare for the Release 12 Upgrade Before Downtime

This section describes the preparation steps for upgrading to Oracle Fusion Applications Release 12 (11.12.x.0.0), all of which can be performed before the scheduled downtime. The following topics are discussed:

2.1 Preliminary Steps

Before starting the upgrade, perform the following preliminary steps:

1. Perform all steps listed in the Pre-Upgrade Known Issues in the latest *Oracle Fusion Applications Technical Known Issues - Release 12 (Doc ID 2224140.1)* found on My Oracle Support.
2. If there are any installed languages in addition to US English, perform all steps list in the Pre-Upgrade Known Issues, if any, from the latest *Oracle Fusion Applications NLS Known issues* found on My Oracle Support.
3. Ensure that the following update bundles have been applied on the environment prior to upgrading to the next release:
    - Oracle Fusion Middleware Update Bundles (P4FA) for Oracle Fusion Applications

      To find the latest technical patch bundle for the release being upgraded from, perform the following steps:

        a. Go to My Oracle Support, log in, and then navigate to **Patches and Updates**
        b. In the Patch Search panel, select **Product or Family (Advanced)** and enter "Oracle Fusion Applications Technology Patches" in the drop down labeled **Product**.
        c. Select the correct release and platform, and then click **Search**.
        d. In the search results, find the patches with the **P4FA** naming convention and select the most recent one.
    - Oracle Fusion Applications Update Bundles

Refer to *Oracle Fusion Applications Known Issues and Update Documents (Doc ID 1603154.1)* on My Oracle Support. Then, click **Oracle Fusion Applications Update Documents**.

For information about how to install update bundles, review the update bundle `README` file. To obtain additional information about update bundles, contact Oracle Support.

4. Ensure `sendmail` is configured and working on all hosts where Upgrade Orchestrator runs by sending a test mail from the hosts. `Sendmail` must be working properly before running the upgrade to effectively monitor the upgrade status.
5. If you are upgrading from Release 8 (11.1.8.0.0), you must upgrade the Fusion Applications and IDM databases from Oracle Database version 11.2.0.3 to 11.2.0.4. This is a prerequisite for upgrade to Fusion Applications Release 12 (11.12.x.0.0). You should upgrade the database before performing the tasks listed in Update the Oracle Fusion Applications and Oracle Identity Management Databases.
6. The task Prepare to Register Database Schema Information requires a password which is referred to as the "Master Orchestration Password" in this documentation. Decide upon the master orchestration password at this time. 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.

2.2 Pre-Upgrade Tasks for Release 8 to Release 12 Direct Upgrades

Before performing Release 8 to Release 12 direct upgrades, you must download the HCM bundle patch (26486308 FA HCM AOO 170719 11.1.8.0.0) from My Oracle Support and apply it to the environment as follows:

1. Download the patch 26486308 from My Oracle Support and stage it into the environment where the patch needs to be applied.
2. Unzip the patch content as shown in the following example:

```
unzip /u01/p26486308_111800_Fusion_GENERIC.zip
```

3. Validate the patch as follows:
   a. Copy the patch to the `patch_stage` location. For example:

      ```
      cd /u01
      ```

   b. Run the `validate` command as follows:

      ```
      <APPLTOP_LOC> /lcm/ad/bin/fapmgr.sh validate -patchtop <patch_num> -online
      ```

      For example:

      ```
      /u01/APPLTOP/fusionapps/applications/lcm/ad/bin/fapmgr.sh validate -patchtop
      26486308 -online
      ```

4. Apply the patch as follows:
   a. Copy the patch to the `patch_stage` location. For example:

      ```
      cd  /u01
      ```

b. Run the `apply` command as follows:

```
<APPLTOP_LOC>/lcm/ad/bin/fapmgr.sh apply -patchtop $patchnum -
start_adpatch_opt force_branch_order=Patch_Is_Higher -end_adpatch_opt -
workers=4 -stoponerror -online
```

For example:

```
/u01/APPLTOP/fusionapps/applications/lcm/ad/bin/fapmgr.sh apply -patchtop
26486308 -start_adpatch_opt force_branch_order=Patch_Is_Higher -
end_adpatch_opt -workers=4 -stoponerror -online
```

5. Verify the patch application by running the following command:

```
<APPLTOP_LOC> /lcm/ad/bin/fapmgr.sh report -isapplied -patch <patch_num>
```

For example:

```
/u01/APPLTOP/fusionapps/applications/lcm/ad/bin/fapmgr.sh report -isapplied -
patch 26486308
```

This task will resolve upgrade issues during loading of DB components.

2.3 Pre-Upgrade Tasks for IDM for FA Upgrade to Release 12

Before you begin the upgrade of your IDM environment for Oracle Fusion Applications (FA) to Release 12, you must verify that your system meets the upgrade requirements and perform pre-upgrade tasks:

- Ensure your Oracle Fusion Applications IDM is on a Release 8 (11.1.8) or Release 9 (11.1.9) environment.
- Back up the IDM middle tier and the IDM database (DB). To perform these backups, see Performing Backups and Recoveries in

  Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management.
- Ensure you have at least 30GB of free space for `/u01`, 10GB for `/u02`, and 4GB for the `/tmp` folder on the IDM host. Note that these values could vary in distributed topology.
- Ensure that all the directories are owned by the installing user. For more information, see Plan Directory Structure and Naming Conventions and Complete the Storage Tab of the Oracle Fusion Applications Installation Workbook in the *Oracle Fusion Applications Installation Guide*.

2.4 System Requirements

Ensure that the environment meets the following system requirements:

- Verify Memory Requirements
- Verify Free Disk Space Requirements
- Verify Reserved Ports Are Available
- Verify OS Patch Requirements

2.4.1 Verify Memory Requirements

If the environment does not meet the memory requirements, Health Checker reports an error during the pre-downtime phase. Verify that the memory configuration meets the requirement mentioned in the following table:

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

Memory Specifics	Upgrade From Release 8, 9, 10 or 11 to Release 12
Memory per Managed Servers	2.75GB (2816MB) multiplied by the number of managed servers in the environment, plus 4GB
Memory Per Administration Servers	• 1GB multiplied by the number of administration servers in the environment, if the WebLogic domain is not a product family of the product offerings that was selected • 2GB multiplied by the number of administration servers in the environment, if the WebLogic domain is a product family of the product offerings that was selected
Business Intelligence Cluster (bi_cluster / BIDomain)	7GB multiplied by the number of instances of managed servers of bi_clusters in the environment
Oracle Enterprise Data Quality Cluster (EDQCluster / CommonDomain)	16GB for two instances of the EDQ WebLogic managed server created out of the box if any of the following product offerings has been selected: • CRM: Sales, Marketing, Customer Data Management, Enterprise Contracts • Financials: Financials, Procurement • SCM: Product Management, Material Management and Logistics, Supply Chain Financial Orchestration
Workforce Reputation Cluster (WorkforceReputationCluster / HCMDomain)	8GB multiplied by the number of managed servers in the environment if any of the following product offerings is selected: • Workforce Development • Workforce Deployment

For Oracle Virtual Machine (VM) memory requirements, see Suggested Memory (in GB) and Number of vCPUs in *Oracle Fusion Applications Installing and Managing in an Oracle VM Environment*.

2.4.2 Verify Free Disk Space Requirements

The disk space requirements mentioned in the following table are recommendations on the disk space required on specific hosts. If the environment does not meet these requirements, Health Checker reports an error during the pre-downtime phase. The disk space check does not check for total space, as it checks 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 there are 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 2-2 Free Disk Space Requirements

Host Name	Upgrade From Release 8, 9, 10 or 11 to Release 12
Primordial	100GB for /u01 + 4GB for /tmp
DB	36GB for tablespaces and redo logs + 4GB for flash recovery area (if configured). Use a higher value for estimated tablespaces as required. For example, calculate the consolidated total free space required for upgrade from multiple schemas for FUSION_TS_TOOLS tablespace (for example, 10GB free space in FUSION_TS_TOOLS)
APPOHS	10GB for /u01 + 4GB for /tmp
Midtier (Primary, Secondary, and BI Hosts)	5GB for /u01 + 4GB for /tmp
OID/OIM	30GB for /u01/IDMTOP + 10GB for /u02/local/IDMTOP + 4GB for /tmp
OHSAUTH	10GB for /u01/IDMTOP + 10GB for /u02/local/IDMTOP + 4GB for /tmp
OID/OIM/ OHSAUTH	400MB for log directory. This is shared between the hosts. Log directory is the value configured for the `LOG_LOCATION` property in IDM.properties and the `LOG_DIR` property in upgradeOnPremise.properties. However, `LOG_DIR` is the location where IDM on-premise upgrade logs are placed.

2.4.3 Verify Reserved Ports Are Available

Ensure that the following reserved ports are not used for any customization or manual scale up activities to prevent port conflicts:

- Ports 7000 through 13000 are reserved for creating WLS components across all domains
- Ports starting from 17000 are used by internal scale out and external scale out

2.4.4 Verify OS Patch Requirements

For Solaris 10 Only

- For Oracle Solaris on SPARC (64-bit) platforms, ensure that the Solaris Operating System patch 150400-xx is installed on the servers.
- For Oracle Solaris on x86-64 (64-bit) platform, ensure that the Solaris x64 Operating System patch 150401-xx is installed on the servers.

These patches can be obtained from My Oracle Support.

For Solaris 11 Only

- Ensure that the Solaris Package `SUNWttf-bh-luxi` is installed on the FA servers for both Oracle Solaris on SPARC (64-bit) and Oracle Solaris on x86-64 (64-bit) platforms.
- The SRU 11.3.3.6.0 or later (mandatory patch) is required for the Solaris 11 Update 3 on SPARC or x86-64.

2.5 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 Orchestration Checkpoint Locations
- Create the Shared Upgrade Location Directory
- Download and Unzip the Patch Rollback Automation Script
- Download and Unzip the Release 12 Repository
- Stage Fusion Applications High-Water Mark Patch Bundles
- Download and Unzip Mandatory Post-Release 12 Patches
- Download and Unzip Release 12 Language Packs
- Download Patches for the Health Checker Exclusion List
- Unzip Orchestration.zip
- Copy and Unzip idmUpgrade.zip

2.5.1 Create a Common User Group and Permissions for Shared Directories

The steps in this section 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 different operating system (OS) users and groups are used to own Oracle Fusion Applications components (such as FA, FMW, and IDM) on the hosts in the Oracle Fusion Applications environment (such as 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.

MANDATORY: 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 Create Directories in a Shared Location.

To set up permissions on directories that are shared across multiple hosts and are used by Oracle Fusion Applications Upgrade Orchestrator, perform the following steps:

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

2. Perform the following steps as a privileged OS user, such as `root`, on all hosts that participate in orchestration:

   a. Create the common group as shown in the following example (if needed):

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

      (Solaris) /usr/sbin/groupadd -g 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 as shown in the following example:

      ```
      (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
      ```

      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. 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 Create Directories in a Shared Location.

   e. Before any additional content is created in the shared directories, change the group ownership of the top-level directory to the common group, such as `orch` as shown in the following example:

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

   f. Set permissions on the directory so that the group has read, write, and access privileges as shown in the following example:

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

   g. 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. For example:

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

3. Perform the following steps on all hosts that participate in orchestration. Make sure to be logged in as the OS user that owns the Oracle Fusion Applications content on the host when running these steps:

   a. Set the default mask for files so that the group has sufficient privileges on the files as follows:

      ```
      umask 0007
      ```

   b. Confirm that the group changes are effective. The `groups` command displays all groups that the current OS user belongs to. Confirm that the common group, `orch`, is one of them as follows:

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

   c. Confirm that the permissions are set up correctly on each host. To do this, 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 privileges.
- For files, the group should have at least read and write privileges.

Run the following commands after creating 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}'" "`"
```

Then, remove the temporary file.

When unzipping 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 extracting 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 upgrade, `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 reports 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`.

2.5.2 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 the Oracle Fusion Applications environment. This location is referred to as *SHARED_LOCATION* in this guide.

If more than one environment are being upgraded, 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. It is possible to choose to use other naming conventions. See Download Directories.

Create the following directories for Release 12 repositories:

- *SHARED_LOCATION*/11.12.x.0.0/Repository

- *SHARED_LOCATION*/11.12.x.0.0_post_repo_patches
- *SHARED_LOCATION*/11.12.x.0.0/idmUpgrade
- *SHARED_LOCATION*/11.12.x.0.0/LP (required only if languages other than US English have been installed)
- *SHARED_LOCATION*/11.12.x.0.0/PCU. Stage post repo patch for the pcu_bundle.zip in this location. Leave this location empty if there is no post repo for pcu_bundle.zip.

2.5.3 Create Orchestration Checkpoint Locations

Create the following directories in a shared storage that is available to all users and all host types within the environment that is getting upgraded:

These directories can also optionally be configured to be shared across other environments.

- ORCHESTRATION_CHECKPOINT_LOCATION

  This is a shared location available to all hosts in the environment where orchestration checkpoint related files are saved. Ensure a shared mount point that has high disk I/O performance is selected, especially for writing. Orchestration framework automatically creates *POD_NAME* under the specified directory. 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 archived. Ensure that a shared mount point that has high disk I/O performance is selected, 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.

2.5.4 Create the Shared Upgrade Location Directory

Create a directory referred to as *SHARED_UPGRADE_LOCATION* in shared storage that is available to all users and all host types within the environment that is getting upgraded. This directory can also optionally be configured to be shared across other environments.

This is a temporary directory required by the upgrade to copy files and perform write operations. Ensure that a shared mount point that is shared across all hosts for a given environment that has high disk I/O performance is selected, especially for writing. This area can be cleaned up after all of the environments have been successfully upgraded to Release 12.

Additionally, create the following directory:

SHARED_UPGRADE_LOCATION/healthchecker/common

Grant write access to the group that was created in Create a Common User Group and Permissions for Shared Directories as well as the checkpoint location and shared upgrade directories that were created in this section.

2.5.5 Download and Unzip the Patch Rollback Automation Script

To download and unzip the Patch Rollback Automation script, perform the following steps:

1. Download and unzip patch 22005049 from My Oracle Support into `SHARED_LOCATION/11.12.x.0.0`. Unzip this patch as the same user that runs the upgrade. Unzipping the file creates the `PatchRollbackUtil` directory with the relevant scripts under `SHARED_LOCATION/11.12.x.0.0` that gets used during upgrade.
2. Validate and correct the Oracle Homes and the JDK location properties found within the following properties files:

   These files can be found under their `config` folders respectively, where the `PatchRollbackUtil` patch is staged.

   - `config/ADMIN-APPS/ADMIN-APPS.properties`
   - `config/APPOHS/APPOHS.properties`
   - `config/AUTHOHS/AUTHOHS.properties`
   - `config/OIDFA/OIDFA.properties`
   - `config/OIMFA/OIMFA.properties`

2.5.6 Download and Unzip the Release 12 Repository

The Release 12 repository contains all patches that are required to upgrade to Release 12 in an existing Oracle Fusion Applications environment. To download the repository from the Oracle Fusion Applications Product Media Package, perform the following steps:

1. Go to Oracle Software Delivery Cloud.
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 the platform to identify the media pack to be downloaded.
4. Choose the appropriate media pack from the search results, such as Release 12 (11.12.x.0.0) for your platform, and download the Release repository (in zipped format) to *`SHARED_LOCATION`*`/11.12.x.0.0/Repository`.
5. Extract the contents of all zipped files to the same target directory, *`SHARED_LOCATION`*`/11.12.x.0.0/Repository`. This directory is referred to as *`REPOSITORY_LOCATION`* in this guide.

   To download the Oracle Fusion Applications 11*g* Media Pack, use the UnZip / 7-Zip utility to extract the Oracle software to *`REPOSITORY_LOCATION`*. UnZip is a freeware tool that is available at the Info-Zip website.

To see the options available to obtain the Oracle Fusion Applications software, see Obtain the Software in the *Oracle Fusion Applications Installation Guide*.

2.5.6.1 Download and Unzip the BI Patch 25499241 into the FA Repository (Solaris Only)

The BI patch 25499241 application fails in Fusion Applications (FA) upgrade in Release 11.12.x.0.0. To resolve this issue, perform the following steps:

1. Download the patch 25499241 from My Oracle Support to any temporary directory (outside the FA repository) on the machine where the FA repository is present.
2. Remove the patch 25499241 from the FA repository as follows:

   ```
   rm -rf <REPOSITORY_LOCATION>/installers/biappsshiphome/patch/25499241
   ```

3. Extract the patch downloaded in Step 2 to the FA repository as shown in the following example:

   ```
   cd <REPOSITORY_LOCATION>/installers/biappsshiphome/patch
   unzip <PATCH_LOCATION>/p25499241_111190_SOLARIS64.zip  (for Solaris Sparc)
   unzip <PATCH_LOCATION>/p25499241_111190_Solaris86-64.zip (for Soalrisx86-64)
   ```

2.5.7 Stage Fusion Applications High-Water Mark Patch Bundles

It is mandatory to apply Fusion Applications High-Water Mark Patch Bundles after upgrade is completed. The patch bundles includes P4FA, BIPB, and FAPB patch bundles.

To get more information about high-water mark patch bundles, contact My Oracle Support.

2.5.7.1 Inject ASINST Patch into Repository

The ASINST Patch 25588435 requires injecting the fix into the repository directly. If you intend to install additional Languages, then you must complete the step Download and Unzip Release 12 Language Packs to stage the language packs into the repository, and then perform the instructions in this section.

To inject the fix, you must stage the new repository injection patch 25588435 to a temporary location, and then perform the following steps:

1. Go to the temporary location.
2. Invoke the following command:

   ```
   ./applyPatch.sh -repoDir SHARED_LOCATION/11.12.x.0.0/Repository
   ```

   This command will inject the patch in `farup` and `fusionapps` and it will also try to inject the patch assuming the `langpack` directory is one of following:

   - `/fsnadmin/upgrade/fusionChangeOps/11.12.1.0.0/LP`
   - `/fsnadmin/fusionChangeOps/patches/lang/rel12.1`

   If the `langpack` directory is different, then pass `-langpackBaseDir <location>` as shown in the following example:

   ```
   ./applyPatch.sh -repoDir SHARED_LOCATION/11.12.x.0.0/Repository [-
   langpackBaseDir <location>]
   ```

   If the patch apply is not successful, the exit code will be non-zero.

2.5.7.2 Inject OUI Patch 26243092 into Repository

If you are uptaking July 17 Post Repo or later and have not injected the OUI patch 26243092 into the repository, then you must perform the following steps:

The bug 26243092 requires injecting the fix into the repository directly. To inject the fix, you must stage the new repo injection patch to a temporary location, and then perform the following steps:

1. Go to the temporary location.
2. Invoke the following command:

   ```
   ./inject.sh [-repo_dir <Absolute path of repository directory>]
   ```

   For example:

   ```
   ./inject.sh -repo_dir /scratch/fa_repos
   ```

   Command for Solaris:

   ```
   bash inject.sh [-repo_dir <Absolute path of repository directory>]
   ```

   For example:

   ```
   bash inject.sh -repo_dir /scratch/fa_repos
   ```

   This command will inject the patch in the following `shiphomes` under the specified repository: `faprov`, `farup`, `fusionapps`, `gop`, `bhd/fusionbhd` and `oui_upgrade/cd`.

   If the patch apply is not successful, the exit code will be non-zero.

2.5.8 Download and Unzip Mandatory Post-Release 12 Patches

After the repository is shipped for every release of Oracle Fusion Applications, additional required patches are staged in a "post repository" directory. The Upgrade Orchestrator can apply these mandatory post-release if the patches are downloaded from My Oracle Support before starting upgrade. The latest post-release patches are cumulative. You must always start by staging the latest post-release patches in a clean location that does not have any files or directories.

To download patches for Release 11.12.x.0.0, first unzip the `/SHARED_LOCATION/11.12.x.0.0/Repository/installers/pre_install/PostRepoPatchDirs.zip` file into the `/SHARED_LOCATION/11.12.x.0.0_post_repo_patches` directory to create the directory structure for the downloaded patches. Then, stage the patch bundles and post repo patches accordingly. The orchestration process automatically picks the patches from the `SHARED_LOCATION/11.12.x.0.0_post_repo_patches` directory when launching the Upgrade Orchestrator, and the upgrade process continues.

The following table shows the patches that must be installed when upgrading to Oracle Fusion Applications Release 12.

> **Note:**
>
> For information about the September 18 Post Repo onward, see the *Oracle Fusion Applications Technical Known Issues - Release 12 (Doc ID 2224140.1)*.

Table 2-3 Mandatory Release 11.12.x.0.0 Patches

Patch Type	Release	Patch Number	Action to be Taken
Installer	11.12.x.0.0	Patch 23012897	Perform the following steps: 1. Download and unzip the contents of patch 23012897 based on the target release you are upgrading to. For example, if you are upgrading to 11.12.1.0.0 (from any release), you must download and stage the patch associated with the high watermark release you are upgrading to. 2. Stage the downloaded content under `SHARED_LOCATION/11.12.x.0.0_post_repo_patches/installer`. 3. After unzipping the patch, verify that the following folders and files are available directly under the `SHARED_LOCATION/11.12.x.0.0_post_repo_patches/installer` directory: • LatestUpdates (folder) • metadata (folder) • readme.txt (file) The readme.txt file contains the details of the patch. **Note**: The patch delivers solutions to issues that were

Table 2-3 (Cont.) Mandatory Release 11.12.x.0.0 Patches

Patch Type	Release	Patch Number	Action to be Taken
			identified post release. If you do not find content under patch 23012897 associated with the high watermark release you are upgrading to, no new version of the installer patch is released for that release.

Table 2-3 (Cont.) Mandatory Release 11.12.x.0.0 Patches

Patch Type	Release	Patch Number	Action to be Taken
FMW/LCM	11.12.x.0.0	September 11 Post Repo: Patch 26773421	Perform the following steps: 1. Download patch 26773421 and unzip it into a temporary location. You should get a directory containing the patch and the `readme` files. 2. From the temporary location, locate the `post_repo_linux64.tar.gz` under `<patch number>/dist` directory. 3. Inspect `post_repo_linux64.tar.gz` to make sure there are top directories such as `atgpf`, `biaapsshiphome`, `ecm_bucket2`, `fusionapps`, `fusionapps_opatch`, `oracle_common`, etc., for example: `tar tzf post_repo_linux64.tar.gz --exclude '*/*/*'` 4. Once confirmed, unzip `post_repo_linux64.tar.gz` into the `SHARED_LOCATION/11.12.x.0.0_post_repo_patches` directory. For Solaris platforms only: unzip the post repo patch tar file (`post_repo_solar`

Table 2-3 (Cont.) Mandatory Release 11.12.x.0.0 Patches

Patch Type	Release	Patch Number	Action to be Taken
			issparc64.tar.gz for Solaris Sparc and post_repo_solarisx64.tar.gz for Solaris x86-64) on a Linux host, then copy the extracted patches to SHARED_LOCATION/11.12.x.0.0_post_repo_patches. 5. After the post repo patch is staged, you should have all the patch contents including directories such as atgpf, biaapsshiphome, ecm_bucket2, fusionapps, fusionapps_opatch, oracle_common, etc. under SHARED_LOCATION/11.12.x.0.0_post_repo_patches.
FA	11.12.x.0.0	Patch 26580880	Download and unzip the content of patch 26580880 into the SHARED_LOCATION/11.12.x.0.0_post_repo_patches directory. This will place the patch contents under the SHARED_LOCATION/11.12.x.0.0_post_repo_patches/fusionapps/upgrade directory.

Table 2-3 (Cont.) Mandatory Release 11.12.x.0.0 Patches

Patch Type	Release	Patch Number	Action to be Taken
LCM	11.12.x.0.0	Patch 26879742	Download and unzip the content of patch 26879742 into the `SHARED_LOCATION/11.12.x.0.0_post_repo_patches/fusionapps/patch` directory.

To verify if the Installer (Auto Update Patch) post release patch is picked up correctly, check the following after the upgrade:

Installer Log

- Ensure that the installer log has messages indicating that the updates from post-repo patch location are merged.
- File: `/u01/inventory/admin-apps.oracleoutsourcing.com/oraInventory/logs` (look for the file that matches the timestamp of the operation).
- Look for the following message:

```
"Applying Updates and Restarting Installer"
```

OracleHomeProperties

- File: `fusionapps/applications/inventory/ContentXML/oraclehomeproperties.xml`.
- Ensure that the `ARU_ID` set to 226 and `PATCHINGMODEL` set to `SNOWBALL` as shown in the following example:

```
<ARU_ID>226</ARU_ID>
<PROPERTY NAME="PATCHING_MODEL" VAL="snowball"/>
```

- Ensure that `OracleHomeProperties` has hard-links defined (must be > 1) as shown in the following example:

```
ls -ls oraclehomeproperties.xml
4 -rw-r----- 2 aime svrtech 483 Feb 13 12:20 oraclehomeproperties.xml
```

Language Installed Artifacts

This step is only applicable if language packs are installed.

- Ensure that it has hard-links defined (must be > 1) as shown in the following example:

```
ls -ls fin/deploy/jar_*.jar
4 -rw-r----- 2 aime svrtech 1207 Feb 13 12:05 jar_FinPmtFDCoreSoaResource.jar
```

To create the directory structure for the downloaded patches, unzip the `/SHARED_LOCATION/11.12.x.0.0/Repository/installers/pre_install/PostRepoPatchDirs.zip` into the `11.12.x.0.0_post_repo_patches` directory. Then, proceed with staging all the available Post Release Patch content. The post-repo structure looks like the following:

Default Post Repo: (Will only get used when FA PB is not applied within the upgrade window)

- SHARED_LOCATION/11.12.1.0.0/11.12.1.0.0_post_repo_patches/<fa post repo content corresponding to GA level>
- SHARED_LOCATION/11.12.1.0.0/11.12.1.0.0_post_repo_patches/<latest fmw post repo content>
- SHARED_LOCATION/11.12.1.0.0/11.12.1.0.0_post_repo_patches/<Installer content>

2.5.9 Download and Unzip Release 12 Language Packs

For each language installed in your environment, download the Release 12 language pack from http://edelivery.oracle.com to the *SHARED_LOCATION*/11.12.x.0.0/LP directory. The location of the downloaded language packs is recorded in the REL12_LP_REPOSITORY_LOCATION property in the Primordial host properties file, as described in Table 11-2.

To find all installed languages in the environment, run the following query:

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

2.5.10 Download Patches for the Health Checker Exclusion List

Health Checker performs sets of validations at various stages of the upgrade. Download the following patches for Release 11.12.x.0.0 from My Oracle Support to have all the required information available for Health Checker:

Create the *SHARED_UPGRADE_LOCATION*/healthchecker/common directory if it does not yet exist.

- Download patch 24623814 and extract its contents to the *SHARED_UPGRADE_LOCATION*/healthchecker/common directory. This patch defines Health Checker plug-ins that are to be disabled out-of-the-box. This patch will be updated with additional plug-in(s) to be excluded as short term solutions(s) when required.

  MANDATORY: This patch is mandatory and its latest version must be downloaded and staged before running Orchestration.
- Verify whether the following patches are available from My Oracle Support. If one of the patches for the target release is not available, ignore the patch as no action is required:
  - Patch 17051994: If available, download and extract its contents, such as FA_invalid_overrides.xml, from the patch to the *SHARED_UPGRADE_LOCATION*/healthchecker/common directory. This patch ensures that a set of objects that get into an invalid state during intermediate stages of the upgrade are safely ignored.
  - Patch 21196045: If available, download and extract its content, such as FA_file_permissions_template_overrides.xml, from the patch to the *SHARED_UPGRADE_LOCATION*/healthchecker/common directory. This patch defines the metadata that is used to check Fusion Applications file permissions. When filenames and folder names are added to the contents of this file, those files and folders are verified by the Health Checker File Permission check. This plug-in is disabled out-of-box. To re-enable this check, see Customization: Re-enable a Plug-in that is Disabled in all_overrides.xml.
  - Patch 21204921: If available, download and extract its content, such as FA_fmw_file_permissions_template_overrides.xml, from the patch to the

SHARED_UPGRADE_LOCATION/healthchecker/common directory. This patch defines the metadata that is used to check Fusion Middleware file permissions. When filenames and folder names are added to the contents of this file, those files and folders are verified by the Health Checker File Permission check. This plug-in is disabled out-of-box. To re-enable this check, see Customization: Re-enable a Plug-in that is Disabled in all_overrides.xml.

2.5.11 Unzip Orchestration.zip

To download and unzip the latest versions of Orchestration.zip and the Health Checker framework, perform the following steps:

1. The latest version of the Orchestration.zip file is uploaded to patch 23012894 on My Oracle Support after Release 12 is released. To ensure you have the latest version of Orchestration.zip, download patch 23012894 from My Oracle Support. The patch contains Orchestration.zip, readme.txt, and validateOrchVersion.py scripts. Extract the patch contents to a temporary location.

   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.
   The patch delivers solutions to issues that were identified post release. If content associated with the high watermark release being upgraded to is not found under patch 23012894, no new version of Orchestration.zip was released yet. Use the Orchestration.zip file that is delivered in the Release 11.12.x.0.0 repository, located at *SHARED_LOCATION*/11.12.x.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/11.12.x.0.0. Unzip the Orchestration.zip file as the same operating system user that was used to set up the Oracle Fusion Applications environment. If the file is unzipped under a different user, see Create a Common User Group and Permissions for Shared Directories.

   When unzipping Orchestration.zip, a directory named orchestration is created. This directory is referred to as *ORCH_LOCATION*. See The ORCH_LOCATION Directory.

3. If the patch was not downloaded in Step 1, proceed to Step 4. If the latest Orchestration.zip file was downloaded from the patch in Step 1, run the validate script given below to validate the version of Orchestration.zip. This confirms that the correct Orchestration.zip file was unzipped to the shared storage location.

   ```
   validateOrchVersion.py 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. After unzipping the Orchestration.zip file, which contains the Health Checker framework, ensure that the latest version of Health Checker is installed by checking the existence of patch 20845106 on My Oracle Support.

   - If there is no patch available, use the Health Checker packaged with Orchestration.zip downloaded in Step 1.

- If the patch is available, view the creation date in the `readme.txt` file available with the Health Checker patch file and compare the file's creation date with the creation date of `Orchestration.zip`. To check which `Orchestration.zip` file is being used, see Step 1 of this procedure.
  - If the Health Checker patch is older than `Orchestration.zip`, no action is required. Use the same Health Checker embedded with the `Orchestration.zip` file.
  - If the Health Checker patch is newer than `Orchestration.zip`, unzip patch 20845106 from My Oracle Support. 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.

2.5.12 Copy and Unzip idmUpgrade.zip

There are two different types of IDM upgrades for this release. In the following chapters you will choose your upgrade type and perform the steps and use the patches applicable to that type only. For more information see, IDM for FA Upgrade Roadmap.

To upgrade IDM for FA to Release 12, you must download the following patches:

- Patch 25734394: This patch contains the `idmUpgrade.zip` file. It is a common patch used for both type 1 and type 2 IDM upgrade scenarios.
- Patch 26504255: This patch contains true-up tars and is needed only for the type 2 IDM upgrade scenario.

After you download all the patches listed above, stage the latest `idmUpgrade.zip` file only if the environment meets all of the following requirements:

- Runs on a Linux or Solaris platform
- Supports the Type 1 or Type 2 IDM upgrade

To stage the latest `idmUpgrade.zip` file, perform the following steps:

1. Always use the latest version of the `idmUpgrade.zip` file. This file is available in patch 25734394.

   To use a new version of the `idmUpgrade.zip` file downloaded from the patch, after having started the upgrade, terminate any running orchestration instances, perform Cancel and Restore steps, and start the upgrade from the beginning.
2. Unzip `idmUpgrade.zip`, using the `unzip -K` option, into *`SHARED_LOCATION`*`/11.12.x.0.0/`.
3. Create the *`SHARED_LOCATION`*`/11.12.x.0.0/idmUpgrade/lib` directory.
4. Include *`SHARED_LOCATION`*`/11.12.x.0.0/idmUpgrade/lib` in the `LD_LIBRARY_PATH` by running the following command on all IDM terminals of IDM hosts before starting orchestration:

   ```
   export LD_LIBRARY_PATH= SHARED_LOCATION/11.12.x.0.0/idmUpgrade/
   lib:$LD_LIBRARY_PATH
   ```

2.6 Set Up Upgrade Orchestrator

To set up Upgrade Orchestrator, perform the following steps:

- Set Up Upgrade Orchestrator on a Shared Location
- Prepare RUP Lite for OVM
- Prepare User Authentication Wallet File
- Update Orchestrator Properties Files
- Create an Override File for RUP Installer
- Prepare Incremental Provisioning
- Validate Repository

2.6.1 Set Up Upgrade Orchestrator on a Shared Location

To set up Upgrade Orchestrator on a shared location, perform the following steps:

1. Unzip the jython zip file, located in *REPOSITORY_LOCATION*/installers/fusionapps/Disk1/stage/ext/jlib/ext_jlib_jars/oam, to a temporary location and use the jython jar to execute orchsetup.py in the next step.
2. Run the orchsetup script on the primordial host. Note that the location for *JYTHON_LOC* is the temporary location from the previous step and the location of *APPLICATIONS_BASE* is described in Oracle Fusion Applications Shared Directories.

   ```
   (UNIX)
   cd ORCH_LOCATION/bin
   java -cp JYTHON_LOC/jython.jar org.python.util.jython orchsetup.py -r
   SHARED_LOCATION/11.12.x.0.0/Repository --appbase APPLICATIONS_BASE
   ```

3. Create a subdirectory to contain setup files for the environment that is being upgraded, define a name for it, 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, it is possible to use this location for the test, production, and development environments, if all three environments are being upgraded to Release 12.

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

   The term *Pod* is equivalent to *environment*.
4. Copy the following template files to the directory that was created in Step 3, without using the template extension, as shown in the following example:

   ```
   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
   ```

5. Copy the silent.rsp.template file to APPLICATIONS_CONFIG/lcm/temp/orchestration/<version>/config/silent.rsp, where <version> is the value of orchestration property FA_TARGET_VERSION as shown in the following example:

   ```
   cp silent.rsp /APPTOP/instance/lcm/temp/orchestration/11.12.x.0.0/config/
   silent.rsp
   ```

2.6.2 Prepare RUP Lite for OVM

Perform the steps in this section only if Oracle Fusion Applications is being run in an Oracle Virtual Machine (VM) environment that was created from official releases of Oracle VM templates for Oracle Fusion Applications Release 12 (11.12.x.0.0) 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, 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, 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. Also check if there is a `/u01/ovmext` directory to determine if it is an Oracle VM IDM instance.

To install the Oracle Fusion Applications 11.12.x.0.0 Lifecycle Management Tools for Oracle VM Installer repository on the Oracle VM hosts, perform the following steps:

This repository includes RUP Lite for OVM.

1. Two patches deliver solutions to issues that are identified post release. If content is not found under the following patches associated with the high watermark release (11.12.x.0.0) being upgraded to, no new version has been released yet:
   - Patch 23012885 delivers the latest post release version of the `fasaaslcmtools.zip` file on My Oracle Support. If no content exists in this patch, use the `fasaaslcmtools.zip` file that is delivered in the Release 11.12.x.0.0 *`OVAB_HOME`*.
   - Patch 23012889 delivers the latest post release version of the `fasaasstagedtools.zip` file on My Oracle Support. The patch contains `fasaasstagedtools.zip`, `readme.txt`, `validate.py`, and `validate.label`. If no content exists in this patch, use the `fasaasstagedtools.zip` file that is delivered in the Release 11.12.x.0.0 *`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.
2. Unzip `fasaaslcmtools.zip` to a temporary location, which creates the `fasaaslcmtools/Disk1` directory. Then unzip `fasaasstagedtools.zip` to the `fasaaslcmtools/Disk1` directory, which creates the `fasaaslcmtools/Disk1/preupg` directory. Specify the *`temporary_location`*`/fasaaslcmtools` location in the `REL12_SAAS_LCM_INSTALLER_DIR` property in the `pod.properties` file. See Update Orchestrator Properties Files.
3. Copy the entire contents of the *`temporary_location`*`/fasaaslcmtools/Disk1/preupg/rupliteovm` directory to *`SHARED_LOCATION/ORCH_LOCATION/config/POD_NAME`*`/11.12.x.0.0/rupliteovm`.
4. 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 REL12_SAAS_LCM_INSTALLER_DIR property from Step 2. 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.

5. Verify that the env.properties file under the *SHARED_LOCATION/ORCH_LOCATION/config/POD_NAME*/11.12.x.0.0/rupliteovm/metadata directory contains the required property values for the following plug-ins:

   - AddBIUsageTrackerDBHost (runs in pre-root mode)

     ```
     ovm.plugin.AddBIUsageTrackerDBHost.enabled=true
     ```

   - AddOHSScaleoutHAToEtcHosts (runs in pre-root mode)

     ```
     ovm.plugin.AddOHSScaleoutHAToEtcHosts.enabled=true
     ovm.plugin.AddOHSScaleoutHAToEtcHosts.ohs_mapping_directory=
     ovm.plugin.AddOHSScaleoutHAToEtcHosts.standby_ohs_mapping_subdirectory=ohs_ma
     pping_files
     ```

   - GenerateOptimizedQueryPlans (runs in offline mode)

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

   - DeployECSF (runs in online mode)

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

   - FixBaseOHSInEtcHosts (runs in post-root mode)

     ```
     ovm.plugin.FixBaseOHSInEtcHosts.enabled=true
     ovm.plugin.FixBaseOHSInEtcHosts.ohs_mapping_directory=
     ovm.plugin.FixBaseOHSInEtcHosts.standby_ohs_mapping_subdirectory=ohs_mapping_
     files
     ```

6. 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.

For more information about the plug-ins, see RUP Lite for OVM Utility.

2.6.3 Prepare User Authentication Wallet File

If Oracle Beehive is used in a Windows environment to send email alerts from Upgrade Orchestrator, then there must be a secured SMTP connection, which requires user authentication data. Such data must not be stored in any property file, and it cannot be pre-seeded in a credential store. However, it is possible to use the mkstore command utility to save this required user authentication information in a wallet file. By default, this wallet file is located at *ORCH_LOCATION*/config/orchfwk/wallet.

To add user authentication data to the wallet file, perform the following steps:

1. At an operating system prompt on the machine that includes the shared location *ORCH_LOCATION*/config, enter the following command, replacing *sending_email_address@my_company.com* and *sending_email_password* with actual values for the SMTP email account that will send the email notifications:

   ```
   orchestration.cmd mkstore -key sending_email_address@my_company.com -value
   sending_email_password
   ```

   If the key, (email address), already exists, this command overwrites the existing password with new input. If the key does not exist in the wallet, it appends the new key and value to the existing wallet.

If this command is entered in a LINUX environment, use single quotes or spaces to enclose any values that include special characters such as the dollar sign ($).

2. Set the following properties in the *ORCH_LOCATION*/config/*POD_NAME*/pod.properties file, substituting appropriate values. To send emails to multiple users, enter a comma-delimited list of email addresses in the EMAIL_TO_RECIPIENT property.

```
EMAIL_TO_RECIPIENT=notification_receiving_email_address@my_company.com
EMAIL_DEFAULT_ENGINE=java
EMAIL_PROTOCOL=smtp
SMTP_AUTHORIZATION=true
SMTP_HOSTNAME=your_SMTP_host_name
SMTP_PORT_NUMBER=your_SMTP_port_number
SMTP_SOCKETFACTORY_CLASS=javax.net.ssl.SSLSocketFactory
SMTP_AUTH_USER=sending_email_address@my_company.com
SMTP_AUTH_PASSWORD=
```

Make sure that the SMTP_AUTH_PASSWORD line of the pod.properties file does *not* specify a password. Instead, the password value is automatically retrieved from the encrypted wallet file.

2.6.4 Update Orchestrator Properties Files

To update properties files, perform the following step:

If any property file values are updated while orchestration is running, the new values do not take effect until a new orchestration session is restarted.

- Update the properties files which are located in the *ORCH_LOCATION*/config/*POD_NAME* directory. If a property is not relevant for the environment, leave it empty, but do not remove the property. For a detailed list of properties, see Upgrade Orchestrator Properties Files.

2.6.5 Create an Override File for RUP Installer

Perform the following steps to create an override file that will be referenced by the REL12_RUPINSTALLER_UPGRADE_PARAM property during the upgrade. This step is not applicable for Oracle VM environments.

1. Create an override file, which can be located in *SHARED_LOCATION*. In this example, the file name is override.properties. It is possible to use a different name for the override file in the environment.
2. The override file contains the following properties:
   - The VIRTUAL_HOST_MODE property must be set to one of three values: IP, Name, or Port. To determine which property value to use, perform the following steps:
     a. Open *WEBTIER_INSTANCE_HOME*/config/OHS/ohs1/moduleconf/FusionVirtualHost_fs.conf. An example of *WEBTIER_INSTANCE_HOME* is APPTOP/instance/CommonDomain_webtier.
     b. If the FusionVirtualHost_fs.conf file contains the string, NameVirtualHost, use VIRTUAL_HOST_MODE=NAME in the override file.
     c. If more than one host exist in FusionVirtualHost_fs.conf for the VirtualHost directive, use VIRTUAL_HOST_MODE=IP in the override file.
     d. Otherwise, use VIRTUAL_HOST_MODE=Port.

- Set the user base `dn` and group base `dn` to configure Application Security Console (ASE). The default values are set as follows:

  a. `user.create.bases= cn=Users,dc=us,dc=oracle,dc=com`

  b. `group.create.bases= cn=FusionGroups,cn=Groups,dc=us,dc=oracle,dc=com`

  If the default value are used, there is no need to set them in overriding properties file. Otherwise, set these two properties accordingly to be consistent with the actual LDAP Identity Store setup.

- The `REFERENCE_ROLES_FILES` property contains a list of the offerings that were selected to be provisioned in the environment. It is possible to obtain this list from the *`APPLICATIONS_CONFIG`*`/fapatch/FUSION_env.properties` file, using only the offerings that also have an entry set to TRUE in this properties file.

  The following examples are provided for each pillar:

  ```
  overrides-hcm.txt:
  VIRTUAL_HOST_MODE=Name
  REFERENCE_ROLES_FILES=PER_CORE,PER_WKF_DEPL,PER_WKF_DEV

  overrides-fscm.txt:
  VIRTUAL_HOST_MODE=Name
  REFERENCE_ROLES_FILES=XLE_FINANCIALS_JUR,PO_PROCUREMENT,PJF_PROJ_MNG,PIM_PROD
  _MNG,DOO_ORCHESTRATION,INV_LOGISTICS,FOS_SCM_FIN_ORCHESTRATION

  overrides-crm.txt
  VIRTUAL_HOST_MODE=Name
  REFERENCE_ROLES_FILES=MKT_MARKETING,ZBS_SALES,CMP_OIC_BU
  ```

- Perform the following step if Load Balancer (LBR) is enabled:

  To create the wiring for the OHS configuration that is used by the Product Management application in the SCM domain, create the following properties. These properties must contain the values for the host and port of the custom LBR external endpoints:

  – `PROCUREMENTDOMAIN.SUPPLIERPORTALAPP.LBR_HOSTNAME`

  – `PROCUREMENTDOMAIN.SUPPLIERPORTALAPP.LBR_PORT`

  The OHS.properties file contains two related properties that must be populated for both the LBR enabled and LBR disabled scenarios: `SUPPLIER_PORTAL_VIRTUAL_HOSTNAME` and `SUPPLIER_PORTAL_VIRTUAL_PORT`. For a scaled out scenario, multiple properties exist, prefixed with the `OHS_INSTANCE_ID`:

  – `ohs1_SUPPLIER_PORTAL_VIRTUAL_HOSTNAME`

  – `ohs1_SUPPLIER_PORTAL_VIRTUAL_PORT`

  – `ohs2_SUPPLIER_PORTAL_VIRTUAL_HOSTNAME`

  – `ohs2_SUPPLIER_PORTAL_VIRTUAL_PORT`

3. Update the `REL12_RUPINSTALLER_UPGRADE_PARAM` property in the `pod.properties` file to add the following value:

   `-DrupOverride=`*`SHARED_LOCATION`*`/override.properties`

2.6.6 Prepare Incremental Provisioning

To determine if Upgrade Orchestrator needs to run incremental provisioning, review the following list of requirements:

Incremental Provisioning Requirements for Oracle VM Environments

Review the following steps if an Oracle Virtual Machine (VM) Environment is used:

- Review the offerings in the applicable OVM template for your environment in Overview in the *Oracle Fusion Applications Installing and Managing in an Oracle VM Environment.*
- If the environment contains all of the offerings available in the template, there is no need to run Incremental Provisioning.
- If the environment does *not* contain all of the offerings available in the template, run Incremental Provisioning to add offerings so that the environment matches the OVM template.

Incremental Provisioning Requirements for non-Oracle VM Environments

Review the following steps if a non-Oracle Virtual Machine (VM) Environment is used:

- Review all offerings in Oracle Fusion Applications Product Families and Product Offerings in the *Oracle Fusion Applications Installation Guide* and compare them with your current installed offerings.
  - If offerings need to be added from the list of offerings for your business needs, then run Incremental Provisioning to add these offerings. If the environment has at least one SCM offering or the Procurement offering, select all mandatory SCM offerings in Incremental Provisioning.
  - If the environment has all of the offerings needed, then consider the following questions and refer to the table below to determine what to do next:
    * If the environment has no SCM offerings, then there is no need to run Incremental Provisioning.
    * If the environment has at least one SCM offering or the procurement offering, then the environment must have all mandatory SCM offerings from all releases. If the environment does not meet this requirement, then run Incremental Provisioning.

Table 2-4 Mandatory Offerings

Condition	Mandatory Offering(s)	What to do	Comments
The environment contains at least one SCM offering or the Procurement offering	Choose one of the following: • Recommended: Add "Manufacturing and Supply Chain Materials Management" offering to the environment. • Alternative: Ensure the environment has "Material Management and Logistics" and "Supply Chain Financial Orchestration" offerings.	Log in to Fusion Applications. Go to Setup and Maintenance to review the list of provisioned offerings. If the environment does not have the mandatory offering(s), then run Incremental Provisioning to add the offering(s).	The Supply Chain Financial Orchestration offering was first introduced in Release 9. "Manufacturing and Supply Chain Materials Management" was first introduced in Release 12 which supersedes "Material Management and Logistics" and "Supply Chain Financial Orchestration" offerings.
All other conditions	No mandatory offering is required.	There is no need to run Incremental Provisioning to add mandatory provisioning offerings. If provisioning offerings need to be added for your business needs, then run Incremental Provisioning to add these offerings.	No additional comments.

For more information, see the Extend an Oracle Fusion Applications Environment Using Incremental Provisioning During Upgrade section in the *Oracle Fusion Applications Installation Guide*.

To prepare for incremental provisioning, perform the following steps:

1. Set the `PERFORM_INCREMENTAL_PROVISIONING` property to `true` in the `pod.properties` file. If there is a plan to run incremental provisioning but this property was not set to `true`, then Upgrade Orchestrator skips the pause point and there will not be an opportunity to run incremental provisioning. For more information about setting the property, see pod.properties.
2. If the environment does not already have any one of the Oracle Sales, Oracle Marketing, or Oracle Financials offerings, and you plan to add at least one of them through incremental provisioning, then confirm that the true-type fonts are installed at `/usr/share/X11/fonts/TTF`. If the true-type fonts are missing, install them before proceeding to the next step.

2.6.7 Validate Repository

After staging is done, ensure that the repository is valid by executing the following script as an Oracle user:

```
$ cd SHARED_LOCATION/11.12.x.0.0/Repository/installers
$ ./validate_repo.sh repository_manifest.xml
```

If the repository is valid, the check returns the following message:

```
Repository integrity check completed successfully.
```

Solaris Only
The following output messages are expected for Solaris platforms:

```
./installers/biappsshiphome/patch/25499241/files/bifoundation/server/bin/
libmemhook64.so does not exists in the repository
./installers/oracle_common/patch/25217940/etc/config/.nfsA6D7 does not exists in the
repository
Total resource entries in the manifest file: 71711, missing resource entries: 2
This repository is corrupt because of some missing files
```

If you see these messages on the `validate_repo.sh` output, ignore them and proceed.

2.7 Other Steps to Perform Before Downtime

Ensure that the following steps are performed before downtime:

- Clean Up Old Patch Storage Directories
- Update the Node Manager Password in a Cloned Environment

2.7.1 Clean Up Old Patch Storage Directories

Patching, at the prior release level, leaves behind significant amount of content in internal patch storage directories and slows down upgrades. This content should be cleaned up prior to upgrade by performing the following steps:

1. Download the patch 25147788 from My Oracle Support.
2. Unzip the patch zip file (`p25147788_111000_Generic.zip`) to a temporary directory as follows:

   ```
   $ unzip -d /scratch/tmp/ p25147788_111000_Generic.zip
   ```

3. Change your current directory to the unzipped directory as follows:

   ```
   $ cd /scratch/tmp/25147788
   ```

4. Set the `JAVA_HOME` environment variable to the JDK installation location.
5. Execute the `patchStorageCleanup.sh` script as follows:

   ```
   $ ./patchStorageCleanup.sh
   ```

   If the `MW_HOME` or `OracleHome` are not in default locations, then launch the script in one of the following ways:

   - `./patchStorageCleanup.sh -mwHome <Path to MiddleWareHome(s) to be cleaned up in comma separated fashion>`

For example:

```
./patchStorageCleanup.sh -mwHome /opt/mwh1,/opt/mwh2
```

- `./patchStorageCleanup.sh -oh <Path to Oracle Home(s) to be cleaned up in comma separated fashion>`

  For example:

  ```
  ./patchStorageCleanup.sh -oh /opt/oh1,/opt/oh2
  ```

- `./patchStorageCleanup.sh -oh <Path to Oracle Home(s) to be cleaned up in comma separated fashion> -mwHome <Path to MiddleWareHome(s) to be cleaned up in comma separated fashion>`
- `./patchStorageCleanup.sh -mwHome <Path to MiddleWareHome(s) to be cleaned up in comma separated fashion> -oh <Path to Oracle Home(s) to be cleaned up in comma separated fashion>`

  For example:

  ```
  ./patchStorageCleanup.sh -mwHome /slot/ems1234/appmgr/APPTOP/fusionapps
  ```

The script scans can be found at the following default locations:

- `/u01/IDMTOP/products/app`
- `/u01/IDMTOP/products/dir`
- `/u01/IDMTOP/products/ohs`
- `/u01/APPTOP/fusionapps`
- `/u01/APPTOP/webtier_mwhome`
- `/u01/APPLTOP/fusionapps`
- `/u01/APPLTOP/webtier_mwhome`

6. Check the log files created under the '`logs`' directory for details about the cleanup.
7. Repeat steps 1 through 6 as listed on this section on the FA Admin, FA OHS, Auth OHS, and one of the IDM hosts (OIM/OID) to clean up old patch content.

2.7.2 Update the Node Manager Password in a Cloned Environment

The upgrade process does not expect the Node Manager password to be different from the keystore password. This difference in passwords causes a failure during the upgrade, which includes the following error message:

```
ERROR KEYSTORE WAS TAMPERED WITH, OR PASS...
```

To prevent this issue, confirm that the Node Manager password is the same as the keystore password before starting the upgrade. Use the Administration Console to change the values for the Node Manager password and properties.

If a cloned instance is being upgraded, change the Node Manager password back to the original password that is used by the Node Manager in the source environment for the clone. After the upgrade, it is possible to change the password back to what it was in the cloned environment after the clone was complete.

2.8 Verify Environment Before Proceeding to Downtime

Perform the following steps to verify the environment before proceeding to downtime steps:

- Confirm Database Settings
- Confirm JDeveloper Customizations Can Be Merged
- Maintain Versions of Customized BI Publisher Reports
- Remove Distributed Order Orchestration Customizations (DOO)
- Verify the FUSION User Quota on FUSION_TS* Tablespaces
- Validate Domain Directories
- Verify the Node Manager Configuration is Correct
- Verify the SSL Configuration is Correct
- Verify the Default Realm Name is `myrealm`
- Verify Removal of Manual Updates to FusionVirtualHost*.conf on OHS Host
- Verify Version of `/bin/bash` on All Hosts (Unix Platforms)

2.8.1 Confirm Database Settings

Refer to the latest *Technical Known Issues* to verify that the database and Sql*Net tuning parameters are set properly to avoid timeout errors during the upgrade.

2.8.2 Confirm JDeveloper Customizations Can Be Merged

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

Merge the customizations after the **SOA Preverification** configuration assistant fails during the upgrade. See Merge SOA Composite JDeveloper Customizations During SOA Preverification.

2.8.3 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 overwrites any customizations applied to the original report. For more information on customizing business intelligence, see the Creating and Editing Analytics and Reports guides relevant to your products.

2.8.4 Remove Distributed Order Orchestration Customizations (DOO)

If Extended Flexfields is being used and the DOO SOA composites have been customized for mapping between EBO and DOO SDO, it is possible to remove these

customizations before upgrading to Release 12 and use the new automap feature. See Preserve SOA Composite JDeveloper Customizations Before Apply a Patch in the *Oracle Fusion Applications Patching Guide*.

For more information about the automap feature in Release 12 that allows you to avoid using SOA composite customizations by setting up Oracle Fusion Distributed Order Orchestration Extensible Flexfields, see the *Oracle Fusion Applications Order Orchestration Implementation Guide*.

2.8.5 Verify the FUSION User Quota on FUSION_TS* Tablespaces

The FUSION user must have an unlimited quota on all FUSION_TS* tablespaces. To verify that the FUSION user has an unlimited quota on all FUSION_TS* tablespaces, run the following query:

```
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, grant the unlimited quota by running the following command:

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

2.8.6 Validate Domain Directories

Run the `validatedomains` script to confirm that all Administration Server domain locations are detectable. If the steps to scale out hosts were followed, the Administration Server of the scaled out host may have been added 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, the Administration Server is added back to the machine that was created during scaleout.

Whether the hosts have been scaled out or not, 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*`/11.12.x.0.0/Repository/installers/farup/Disk1/upgrade/validate` directory into any directory on the primordial host.
   a. Update the path with the correct location of JDK by placing the JDK apptop in front of the path so that java runs from it as follows:

      ```
      (UNIX)
      PATH=$1/jdk6/bin:$1/fusionapps/jdk6/bin:$PATH
      export PATH
      ```

   b. If *FA_MW_HOME* is *APPLICATIONS_BASE*`/fusionapps`, run the following command:

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

      For example:

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

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

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

For example:

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

2. If `validatedomains.sh` reports any domains that failed the validation, and there are no scaled out hosts, skip to Step 3.

   If `validatedomains.sh` reports any domains that failed the validation, and if there scaled out hosts, perform the following steps on the Administration Server of each of the reported domains:

   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.

   i. Skip Step 3 of this procedure.

3. If `validatedomains.sh` reports any domains that failed the validation, and if there are no scaled out hosts, perform the following steps:

   a. Download the patch 18062458 to a local directory.

   b. Run the extracted command against each domain directory under `APPLICATIONS_CONFIG` as follows:

   ```
   For Unix:
   FA_MW_HOME/oracle_common/common/bin/wlst.sh fixadminconfig.wlst
   APPLICATIONS_CONFIG/domains/<HOST>/<DOMAIN NAME>
   ```

   c. Run the `validatedomains` script again, to ensure that all Administration Server domain locations are detectable.

2.8.7 Verify the Node Manager Configuration is Correct

Perform the following steps on the `admin-apps/PRIMORDIAL` host and all Midtier hosts 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 WebLogic Scripting Tool (WLST) command as described in the following steps:

   a. Run the WLST command to fix the configuration in each domain directory as follows:

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

   b. Open the domain in offline mode as follows:

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

   c. Run the following commands for each impacted machine:

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

   d. Save the domain and exit WLST as shown in the following example:

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

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

2.8.8 Verify the SSL Configuration is Correct

To verify that the node manager configuration is correct, perform the following steps on the `admin-apps/PRIMORDIAL` host and all Midtier hosts:

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

   ```
   <server>
   <name>SERVER_NAME</name>
   <ssl>
   <name>SERVER_NAME</name>
   ...
   </ssl>
   </server>
   ```

2. If any of the `ssl` 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 command 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 impacted machine:

      ```
      cd('/Server/SERVER_NAME/SSL/SERVER_NAME')
      set('Name', 'SERVER_NAME')
      ```

d. Save the domain and exit WLST:

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

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

2.8.9 Verify the Default Realm Name is `myrealm`

Upgrade Orchestrator expects the default realm name to be `myrealm` for the Common Domain. Changing the name to anything other than `myrealm` causes Upgrade Orchestrator to fail. To verify that this value has not been changed to any other name, perform the following steps :

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.

2.8.10 Verify Removal of Manual Updates to FusionVirtualHost*.conf on OHS Host

Any manual updates, such as the addition of headers, to the virtual host configuration files on the OHS hosts must be removed. The file names impacted by this step are in the following format:

`FusionVirtualHost*.conf`

2.8.11 Verify Version of `/bin/bash` on All Hosts (Unix Platforms)

Upgrade Orchestrator uses "Bash" as the default shell on Unix platforms. Ensure that the `/bin/bash` shell version 3.2 or higher is installed on all hosts.

3

Update the Oracle Fusion Applications and Oracle Identity Management Databases

This section describes how to update an Oracle Fusion Applications database and Oracle Identity Management database before an upgrade. The following topics are discussed:

- Check Database Version
- Apply Database Patches for Release 12 (Solaris Only)
- Apply Exadata Patches for Release 12
- Ensure FUSION_OTBI Schema Version Registry
- Install and Run Oracle Fusion Applications Repository Creation Utility (Release 8 Solaris Platforms Only)
- Enable Oracle Java Virtual Machine in the Database
- Enable RDF Option in the Database

The steps in this and the following sections are downtime activities and can be planned and performed in a separate downtime window prior to the upgrade.

3.1 Check Database Version

Before proceeding, ensure that the Oracle Database version is 11.2.0.4. All of the patches discussed in this section require this database version. If you are upgrading from Release 8 (11.1.8.0.0), you must upgrade the Fusion Applications and IDM databases from Oracle Database version 11.2.0.3 to 11.2.0.4. This is a pre-requisite to upgrade to Fusion Applications Release 12 (11.12.x.0.0).

It is a best practice to apply these patches on Identity Management databases to keep both the Oracle Fusion Application database and Identity Management database synchronized. It is also a best practice to back up both of these databases before patching. See Back Up and Recover Oracle Fusion Applications in the *Oracle Fusion Applications Administrator's Guide*.

3.2 Apply Database Patches for Release 12 (Solaris Only)

To apply the certified database (DB) bundle patch and to upgrade the `fusionapps` database on Solaris platforms, perform the following steps:

1. Apply the version of OPatch that is delivered in the repository on the database host as follows:

```
export  ORACLE_HOME=<Fusionapps DB oracle home >
cd $ORACLE_HOME
mv -f  OPatch OPatch_orig
unzip
<REPOSITORY>/installers/database_upgrade/opatch/p6880880_112000_SOLARIS64.zip
```

2. Execute `catsem.sql` as shown in the following example and confirm the `MDSYS` schema creation is successful:

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

SQL> select namespace, attribute, value, description
from mdsys.rdf_parameter
where namespace = 'MDSYS' and attribute = 'SEM_VERSION';

    NAMESPACE                      ATTRIBUTE              VALUE
DESCRIPTION
--------------------------------------------------------------------------------
----------------------
    MDSYS                          SEM_VERSION            11204              VALID
```

3. Shutdown the Fusion Applications (FA) DB.
4. Apply the DB patches as follows:

```
cd <REPOSITORY>/installers/database_upgrade/psu
$ORACLE_HOME/OPatch/opatch napply

 cd  <REPOSITORY>/installers/database_upgrade/patch
$ORACLE_HOME/OPatch/opatch napply
```

5. Restart the FA DB and perform the following post installation steps:
   a. Connect to the FA DB and execute the following sql script with the given arguments:

      ```
      @$ORACLE_HOME/rdbms/admin/catbundle.sql  exa apply
      ```

   b. Run the following sql script to recompile the invalid objects created in the DB:

      ```
      @$ORACLE_HOME/rdbms/admin/utlrp.sql
      ```

6. Execute the following query to check if any invalid objects are present in the database after the upgrade:

   ```
   SELECT owner, object_type, object_name FROM dba_objects WHERE status = 'INVALID'
   ORDER BY owner, object_type, object_name;
   ```

   Proceed to Steps 7 and 8 only if the query returns any rows.
7. Log in to the FA DB as sys user and execute the following grants:

```
GRANT SELECT ON CRM_FUSION_SOAINFRA.WFTASK TO FUSION;
GRANT SELECT ON CRM_FUSION_SOAINFRA.WFMESSAGEATTRIBUTE TO FUSION;
GRANT SELECT ON CRM_FUSION_SOAINFRA.WFASSIGNEE TO FUSION;
GRANT SELECT ON CRM_FUSION_SOAINFRA.WFTASK TO FUSION_RUNTIME;
GRANT SELECT ON CRM_FUSION_SOAINFRA.WFMESSAGEATTRIBUTE TO FUSION_RUNTIME;
GRANT SELECT ON CRM_FUSION_SOAINFRA.WFASSIGNEE TO FUSION_RUNTIME;
```

8. Run the following script to re-compile the invalid objects:

```
@$ORACLE_HOME/rdbms/admin/utlrp.sql
```

3.3 Apply Exadata Patches for Release 12

To upgrade to Oracle Fusion Applications Release 12 (11.12.x.0.0), use the certified RDBMS patch 11.2.0.4.160811FA-DBBP (11gR2).

If you are using the Oracle Exadata Database Machine, download the latest P4FA from My Oracle Support to get the quarterly Exadata database patch as well as the

one-off Exadata patches that are specifically required for your platform. After downloading the latest P4FA, it is possible to find these Exadata quarterly patches under the `rdbms_version` directory, where *`version`* is the database version. An example of the directory path is as follows:

```
rdbms_12.1.0.2.0/exadata
```

After downloading and unzipping the latest P4FA, perform the following steps:

The examples in this procedure use linux64 as the platform.

1. Get opatch patch from the `rdbms_12.1.0.2.0/exadata/linux64/opatch/` directory.
2. Apply the Exadata bundle that is located under the `rdbms_12.1.0.2.0/exadata/linux64/exadata_bundles/` directory.
3. Apply the one-off patches from the generic and linux64 directories as shown in the following example:

   The one-off patches can be applied in any order.

   - `rdbms_12.1.0.2.0/exadata/generic/one_off_patches/*`
   - `rdbms_12.1.0.2.0/exadata/linux64/one_off_patches/*`

See Apply Technical Patch Bundles: P4FA in the *Oracle Fusion Applications Patching Guide*.

3.3.1 Tune Database Parameters Manually

This section provides the parameters that need to be manually tuned in both the Fusion Applications (FA) database and the Oracle Identity Manager (IDM) database.

FA Database

The following table displays the FA database parameters to be tuned manually. Update these parameters to the recommended values:

Table 3-1 Recommended Values for FA Database Parameters for Manual Tuning

Parameter	Type	Location	Recommended Value
`AUDIT_SYS_OPERATIONS`	Initialization	Spfile/pfile	FALSE
`DISK_ASYNCH_IO`	Initialization	Spfile/pfile	TRUE
`RESOURCE_MANAGER_PLAN`	Disk IO	Spfile/pfile	FUSIONAPPS_PLAN
`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

Table 3-1 (Cont.) Recommended Values for FA Database Parameters for Manual Tuning

Parameter	Type	Location	Recommended Value
PARALLEL_MAX_SERVERS	Initialization	Spfile/pfile	12
JOB_QUEUE_PROCESSES	Initialization	Spfile/pfile	12
AUDIT_TRAIL	Initialization	Spfile/pfile	DB, EXTENDED
SQL Tuning Advisor Job	Automated Maintenance Tasks	Database	Disable
Segment Advisor job	Automated Maintenance Tasks	Database	Disable

IDM Database

The following are the recommended redo log files sizes:

- 11*g* Database: The default is 0.05GB but 2GB for each redo log file is recommended for improving the redo log performance.
- 12*c* Database: The default is 0.05GB but 2GB for each redo log file is recommended for improving the redo log performance. The 12*c* database recommended parameters will apply after the upgrade to Release 12 is done and the 11*g* database is upgraded to 12*c*.

The following table displays the IDM database parameters to be tuned manually. Update these parameters to the recommended values:

Table 3-2 Recommended Values for IDM Database Parameters for Manual Tuning

Parameter	Type	Location	Recommended Value
job_queue_processes	Initialization	Spfile	12
shared_servers	Initialization	Spfile	0
_active_session_legacy_behavior	Initialization	Spfile	TRUE

3.4 Ensure FUSION_OTBI Schema Version Registry

Perform this step if you are upgrading from a Release 11.1.8.x.0 environment to Release 11.12.x.0.0.

Run the following command in your Oracle Fusion Database:

```
select * from schema_version_registry where
OWNER='FUSION_OTBI' and COMP_ID='ATGLITE_OTBI';
```

The command should return records. If no records are returned, run the following SQL statement:

```
INSERT INTO SCHEMA_VERSION_REGISTRY
(COMP_ID,COMP_NAME,MRC_NAME,MR_NAME,MR_TYPE,OWNER,VERSION,STATUS,UPGRADED,START_TIME,
MODIFIED) values ('ATGLITE_OTBI','Oracle Transactional Business Intelligence-
ATGLITE','FUSION_OTBI','ATGLITE_OTBI','ATGLITE_OTBI','FUSION_OTBI','11.1.1.7.0','VALI
D','N',null,null)
```

3.5 Install and Run Oracle Fusion Applications Repository Creation Utility (Release 8 Solaris Platforms Only)

If Oracle Fusion Applications Release 8 is being run on a Solaris platform only, perform the following steps to add schemas that are introduced between Release 8 and Release 11 along with new schemas introduced in Release 12:

1. Copy or mount the Oracle Fusion Applications Release 12 Repository on a Linux machine.
2. Locate the `rcuHome_fusionapps_linux.zip` file in *`REPOSITORY_LOCATION`*`/installers/apps_rcu_11g/linux` and unzip its contents. This location is referred to as *`RCU_HOME`*.
3. Run the following command from *`RCU_HOME`* to create the required schemas:

   ```
   RCU_HOME/bin/rcu -silent -createRepository -databaseType ORACLE -connectString
   db_server:db_port/db_sid -dbUser sys -dbRole
   sysdba -schemaPrefix FUSION -component FUSION_EDQCONFIG2 -component FMW_RUNTIME
   -component FUSION_EDQRESULTS1 -component FUSION_INTG_CURRENT -component
   FUSION_EDQRESULTS2 -component FUSION_RDF
   -component LCM_SUPER_ADMIN -component DVACCTMGR -component FUSION_INTG_PREVIOUS -
   component FUSION_INTG_FINAL
   -component FUSION_GRC -component DVOWNER -component FUSION_EDQCONFIG1 -component
   LCM_OBJECT_ADMIN -component LCM_EXP_ADMIN -component FUSION_EDQFUSION
   -component FUSION_RO -component LCM_USER_ADMIN  -component FUSION_BIA_CLOUD
   -component FUSION_ERO  -component HED_FUSION_MDS_SOA  -component FUSION_OPSS  -
   component HED_FUSION_SOAINFRA
   ```

4. Provide the passwords for the following components:

   ```
   Sys password
   FUSION_EDQCONFIG2 password
   FMW_RUNTIME password
   FUSION_INTG_CURRENT password
   FUSION_EDQRESULTS1 password
   FUSION_EDQRESULTS2 password
   FUSION_RDF password
   LCM_SUPER_ADMIN password
   DVACCTMGR password
   FUSION_INTG_PREVIOUS password
   FUSION_INTG_FINAL password
   FUSION_GRC password
   DVOWNER password
   FUSION_EDQCONFIG1 password
   LCM_OBJECT_ADMIN password
   LCM_EXP_ADMIN password
   FUSION_EDQFUSION password
   FUSION_RO password
   LCM_USER_ADMIN password
   FUSION_BIA_CLOUD password
   FUSION_ERO password
   HED_FUSION_MDS_SOA password
   FUSION_OPSS password
   HED_FUSION_SOAINFRA password
   ```

3.6 Enable Oracle Java Virtual Machine in the Database

Enable Oracle Java Virtual Machine (OJVM) by performing the following steps:

1. Download the `ojvmctrl` patch 23341410 from My Oracle Support.
2. Unzip the patch to a stage directory, for example, *`STAGE_DIR`*.
3. Run the following command:

   ```
   cd $STAGE_DIR/bin
   ```

4. Enable JAVA Development by running the following command:

   ```
   sh ojvmctrl.sh -mode enable -appbase APPLICATIONS_BASE -stage
   ```

3.7 Enable RDF Option in the Database

Perform this step only after you complete the Enable Oracle Java Virtual Machine in the Database step and if the upgrade to Release 12 is from Release 8 or Release 9. Skip this step if the upgrade starting point is Release 10. OSN components introduced in 11.1.10.x.0 require the enablement of the Resource Description Framework (RDF) option in the database prior to the upgrade. This option must be enabled only in the Oracle Fusion Applications database.

To enable RDF, connect to the database as the SYS user with SYSDBA privileges (SYS AS SYSDBA, and enter the SYS account password when prompted). Then, start SQL*Plus, and enter the following statement:

```
Unix: @$ORACLE_HOME/md/admin/catsem.sql
```

For more information, see Enabling RDF Semantic Graph Support in a New Database Installation in the *Oracle Spatial and Graph RDF Semantic Graph Developer's Guide*.

4
Prepare for Upgrade

Oracle Virtual Directory (OVD) is not a supported component in Fusion Applications (FA) Release 11.12.x.0.0. Therefore, if you are using OVD in your FA setup, you must remove it before starting your FA upgrade from Release 8 or 9 to Release 12.

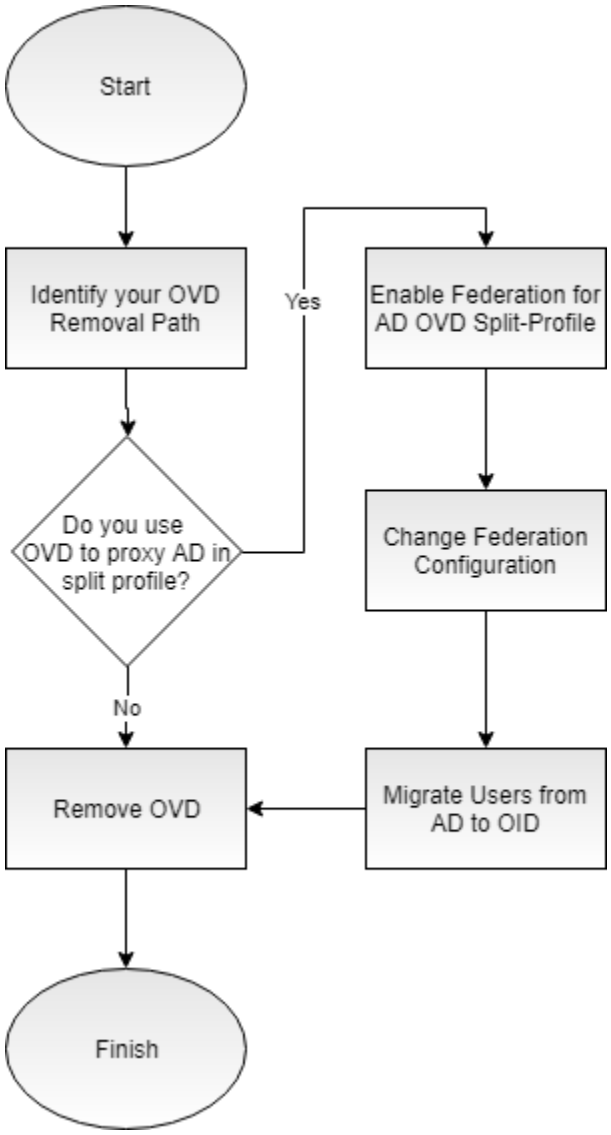
This chapter provides the steps to remove OVD including the scenarios where you have OVD backed by an Oracle Internet Directory (OID), or where OVD is used in split profiles to talk to Microsoft Active Directory (AD) and OID. For more information about split profiles, see Split Profiles with AD and OID for Fusion Apps IDM in the *Oracle A-Team Chronicles*.

This chapter contains the following topics:

4.1 OVD Removal Roadmap

Review the following flowchart for an overview of the typical Oracle Virtual Directory (OVD) removal process including the scenario where OVD is used to proxy Active Directory (AD) in split-profile.

Figure 4-1 OVD Removal Process Flowchart



The following table lists the high-level steps that you need to perform to remove OVD from your environment:

Table 4-1 Tasks for Removing OVD from your Environment

Task	Required	Description
Identify your OVD Removal Path	Required	Identify your removal path to choose the right procedure for your system. See Identify your OVD Removal Path.
Enable Federation for AD OVD Split-Profile	Required only if you use OVD to proxy AD in split profile	Configure your OIF with an Identity Provider on the IDM environment. See Enable Federation for AD OVD Split-Profile.

Table 4-1 (Cont.) Tasks for Removing OVD from your Environment

Task	Required	Description
Change Federation Configuration	Required only if you use OVD to proxy AD in split profile	Configure your OIF bundled with IDM to talk to AD. See Change Federation Configuration.
Migrate Users from AD to OID	Required only if you use OVD to proxy AD in split profile	Copy users from AD to OID by running the migration tool. See Migrate Users from AD to OID.
Remove OVD	Required	Remove the OVD authenticator and replace it with the OID authenticator. Update the respective product configurations with OID details and bring down OVD. See Remove OVD.

4.2 Identify your OVD Removal Path

The path that you must take to remove your OVD component depends on how you are using OVD. Use the following table to identify the path you need to follow when removing OVD from your environment.

Table 4-2 OVD Removal Paths

If your current use of OVD is:	Then you need to:
To proxy OID	Update your domain and dependent product configurations to use authenticators that talk to OID instead of OVD.
To proxy AD in split profile	Enable federation, then remove the OVD authenticator, and run the AD to OID user migration tool. Once the AD to OID migration is complete, Weblogic domains are updated to use OID.

4.3 Enable Federation for AD OVD Split-Profile

> **Note:**
>
> The steps in this section are only applicable if you use OVD to proxy AD in split profile. If you use OVD to proxy OID, skip to Remove OVD.

To remove the OVD authenticator and replace it with the OID authenticator, perform the steps as described in the following sections:

- Configure OIF with an Identity Provider
- Import ADFS-IdP Metadata to OIF-SP

- Import OIF-SP to ADFS IdP
- Protect a Resource

4.3.1 Configure OIF with an Identity Provider

The steps in this section are applicable to either Release 8 or 9. To enable federation and to configure Oracle Identity Federation (OIF) Service Provider (SP) with an Identity Provider (IdP) (or OIF as IdP /ADFS) on and IDM environment prior to upgrade, perform the following steps:

1. Verify if OIF is enabled by checking if the `oif_startup.conf` file exists in the setup's binary or `config` location. If yes, then check if the following properties are set to true in that file. If true, then OIF is enable, otherwise it is not:

   ```
   'OIF_ENABLED=true' & ' OPMN_EMAGENT_MANAGED_BY_OIF_SCRIPT=true'
   ```

2. Enable OIF if it is not already enabled:

   a. Find the `oifAutomation.properties` file at the following location, where relX refers to rel8, rel9:

      ```
      OIF_HOME/scripts/fa/relX/oifAutomation.properties
      ```

      Where

      `OIF_HOME`: location of OIF installation.

   b. Back up the `oifAutomation.properties` file.

   c. Update the `oifAutomation.properties` file with the appropriate environment information.

   d. Ensure all servers are up.

   e. Ensure your Perl version is v5.8.8 or above.

   f. Download the `jce_policy-6.zip` file from Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6.

   g. Go to the location of the `oifAutomation.pl` script and run the following:

      ```
      cd OIF_HOME/scripts/fa/relX
      perl oifAutomation.pl oifAutomation.properties enableOIF -enableOIF true -
      enableOPMN true -initializeOIF -updateJCECrypto <download location of
      jce_policy-6.zip>
      perl oifAutomation.pl oifAutomation.properties enableOIFTest true
      ```

3. Configure Single Sign-on (SSO) with federation as follows:

   ```
   perl oifAutomation.pl oifAutomation.properties configureSSO -sso federation
   chooser nofedmobile
   ```

4. Create a user through OIM with an email address. For example, *username* and *username*@example.com.

5. Enable the Identity Provider (IdP) as follows:

   a. Log in to Enterprise Manager Fusion Middleware Control Console.

   b. Expand **Identity and Access** folder, and choose **OIF(11.1.1.2.0)**.

   c. Expand the **Oracle Identity Federation** menu, and go to **Administration**.

   d. Click **Identity Provider**.

e. Ensure that the **Enable Identity Provider** check box is checked.

4.3.2 Import ADFS-IdP Metadata to OIF-SP

If you have linked to OIF-IdP already, skip to Import OIF-SP to ADFS IdP. If OIF is IdP, then you can skip all AD related steps and go directly to Protect a Resource.

Import Active Directory Federation Services (ADFS) IdP metadata to OIF-SP as follows:

1. Ensure all servers are up.
2. Ensure your Perl version v5.8.8 or above.
3. Run the following command:

```
perl oifAutomation.pl oifAutomation.properties configureIdPPartner -metadata
FederationMetadata.xml -nameid email -ssoprofile post (-nameid unspecified if
you want to use uid)
```

4.3.3 Import OIF-SP to ADFS IdP

To import OIF-SP to ADFS IdP, perform the following steps:

1. Connect to the remote desktop *myhost*`.example.com` and log in with your username and password.
2. Save the `https://sso_lbr server: PORT URL fed/sp/metadata` to a `sp_metadata.xml` file on the desktop.
3. Launch the AD FS 2.0 Management by going to **Start**, then **Programs**, then **Administrative Tools**, and **AD FS 2.0 Management**.

> **Note:**
>
> Note that the steps provided are for AD FS 2.0. If you are running a later version, then consult the latest Microsoft documentation.

4. Expand the **Trust Relationships** folder and right-click **Relying Party Trusts**, then choose **Add Relying Party Trust**.
5. Click **Start**, then go to **Select Data Source**.
6. Choose **Select Import data about the relying party from file**, and then browse the `metadata.xml` file, and then click **Next**.
7. Enter the Display name of *myhost*, and then click **Next**.
8. Select Default Permit for all users to access this relying party, and then click **Next**.
9. Click Next, then mark the check box **Open the Edit Claim Rules...when wizard closes**, and then click **Close**.

   The Edit Claim Rules wizard appears and shows the message “EmailID and Email Transform claim rules are needed”.
10. Click **Add Rule**, then choose **Send LDAP Attributes as Claims**, and then click **Next**.
11. Provide the following details:

- For Claim rule Name, enter `EmailID`
- For Attribute store, enter `Active Directory`
- For LDAP Attribute, enter `E-Mail Addresses`
- For Outgoing Claim Type, enter `E-Mail Addresses`

12. Click **Finish**.
13. Click **Add Rule**, then choose **Transform an Incoming Claim**, and then click **Next**.
14. Provide the following details:
    - For Claim rule Name, enter `EmailID Transform`
    - For Incoming claim type, enter `E-Mail Address`
    - For Outgoing claim type, enter `Name ID`
    - For Outgoing name ID format, enter `Unspecified`
15. Click **Finish**.
16. Change to SHA–1 for Secure hash algorithm as follows:
    a. Right-click the newly created Relying Party.
    b. Choose **Properties** and click the **Advanced** tab.
    c. On the Secure hash algorithm, choose **SHA-1**.
    d. Click **Apply**.
17. Create an user with the same email address on AD users as follows:
    a. Launch the AD Users and Computers by clicking **Start**, then **Programs**, **Administrative Tools**, and **Active Directory Users and Computers**.
    b. Click to expand the domain name `adfs.fed.example.com`, then **Users**, and right-click **New User**.
    c. Enter the following values on the create user wizard, and then click **Next**.
       - First name: *username*
       - Full name: *username*
       - User logon name: oif*username*
    d. Deselect **User must change password at next logon**, and then check **Password never expires**.
    e. In Enter Password/Confirm Password, enter *password*, and then click **Finish**.
    f. Right-click the new example user and choose **Properties**.
    g. Update the E-mail address with *username*`@example.com`, and then click **Apply**.

4.3.4 Protect a Resource

Protect the `IAMSuiteAgent:/welcome_webcenter.html` resource with `FAAuthScheme` using Oracle Access Manager (OAM) as follows:

1. Log in to the OAM Console and navigate to **Application Domains**.
2. Go to **IAM Suite**, and then click **OIFAuthnPolicy**.

3. Click the add **+** sign to add the resource.
4. Choose `IAMSuiteAgent:/welcome_webcenter.html` from the drop down list.
5. Click **Apply**.

4.4 Change Federation Configuration

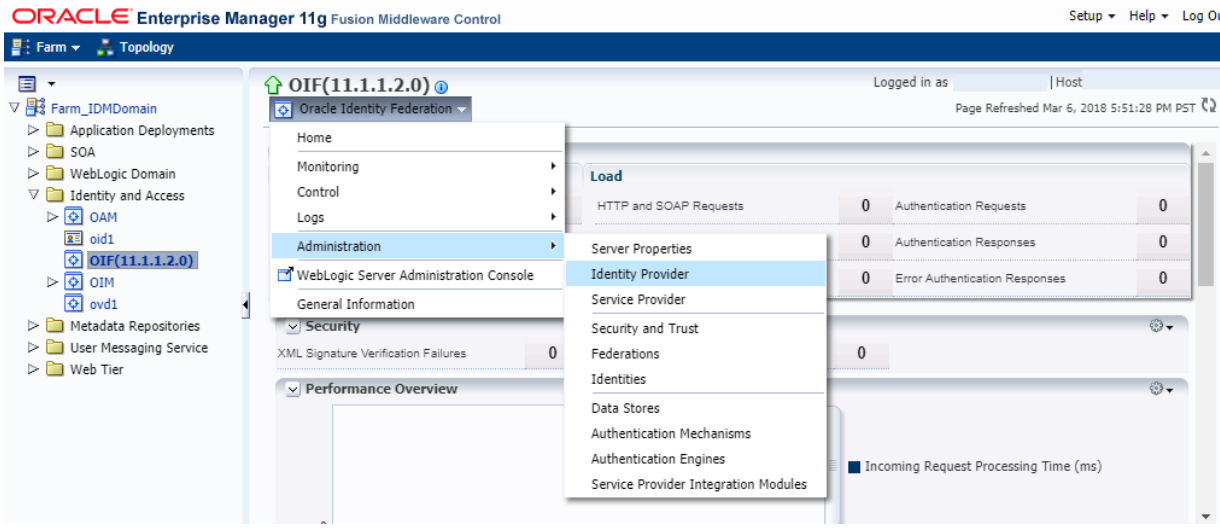
> **Note:**
>
> The steps in this section are only applicable if you use OVD to proxy AD in split profile. If you use OVD to proxy OID, skip to Remove OVD.

To configure Oracle Identity Federation (OIF) using Enterprise Manager (EM) console, see Adding Oracle Identity Federation to an Existing Fusion Applications Deployment Part 1. Alternatively, perform the following steps:

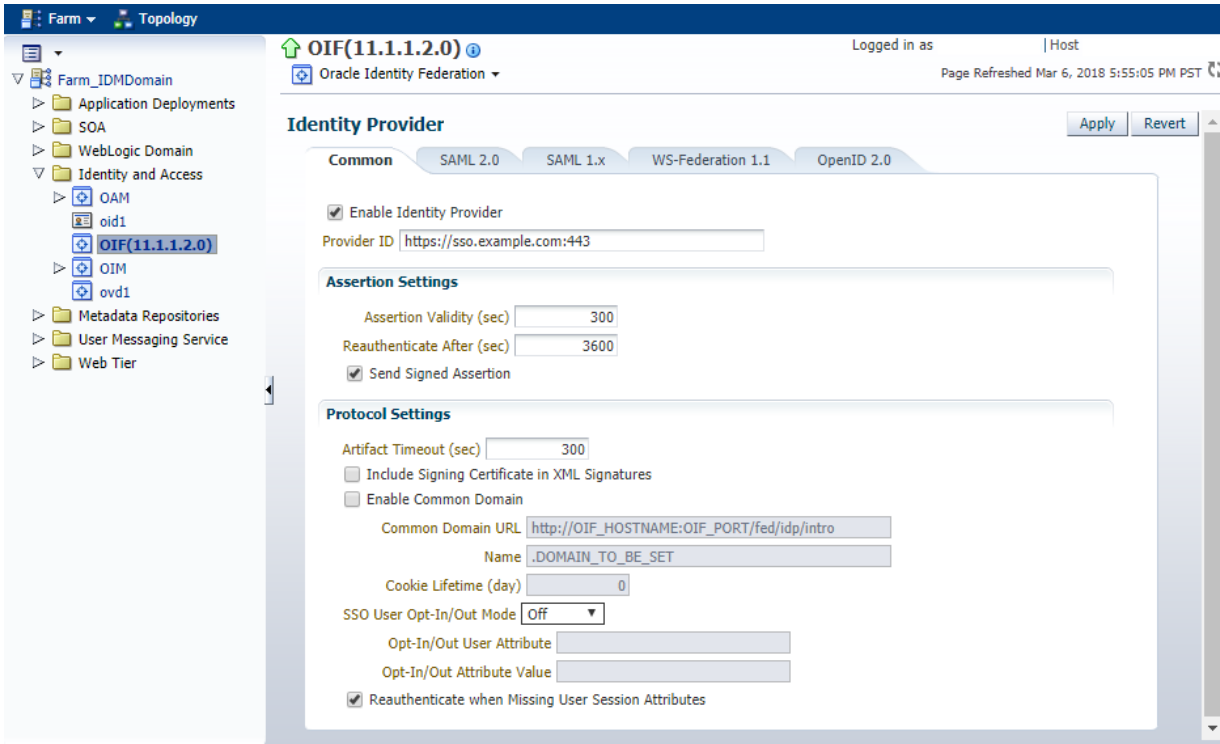
- Configure Identity Providers - Common Properties
- Configure Identity Providers - SAML 2.0 IdP Properties
- Configure Data Stores
- Configure Service Provider
- Configure Service Provider Integration Modules
- Configure OAM
- Verify If Resource Is Protected

4.4.1 Configure Identity Providers - Common Properties

1. Log in to Enterprise Manager Fusion Middleware Control Console.
2. Expand **Identity and Access** folder, and choose **OIF(11.1.1.2.0)**.
3. Expand the **Oracle Identity Federation** menu, and go to **Administration**.
4. Click **Identity Provider** as shown in the following figure:



5. Click the **Common** tab.
6. Ensure that the **Enable Identity Provider** box is checked.
7. Specify the Provider ID as `SSO_URL/fed/idp`. For example, `https://sso.example.com:443`:

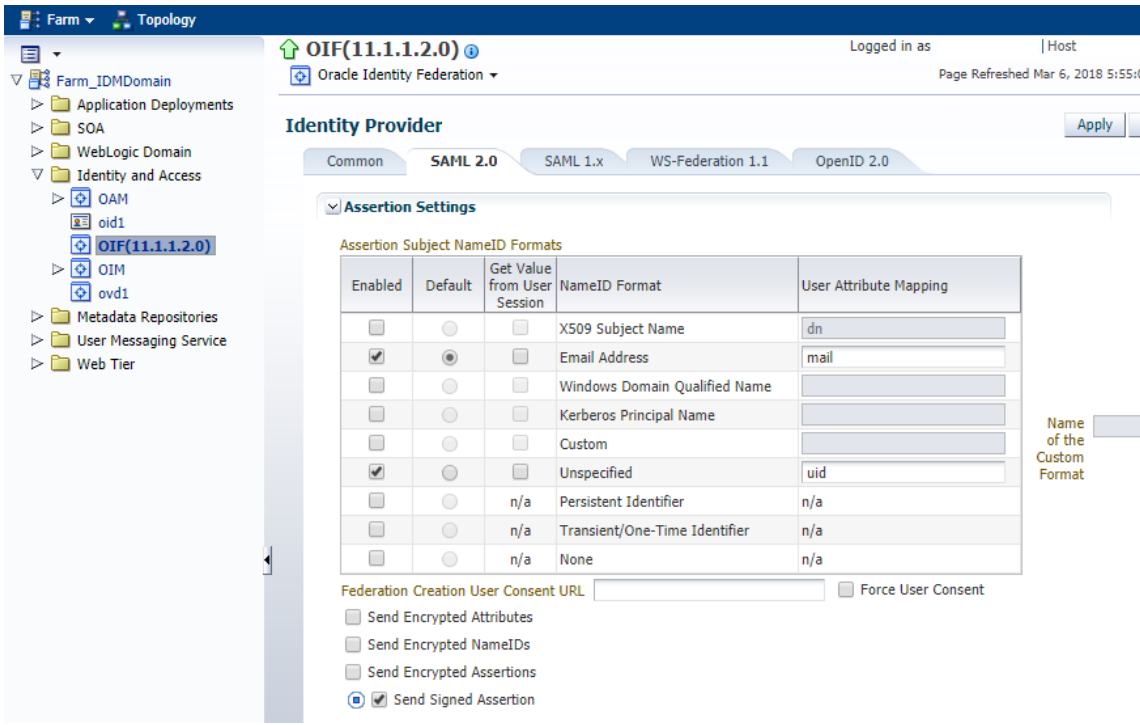


8. Click **Apply**.

4.4.2 Configure Identity Providers - SAML 2.0 IdP Properties

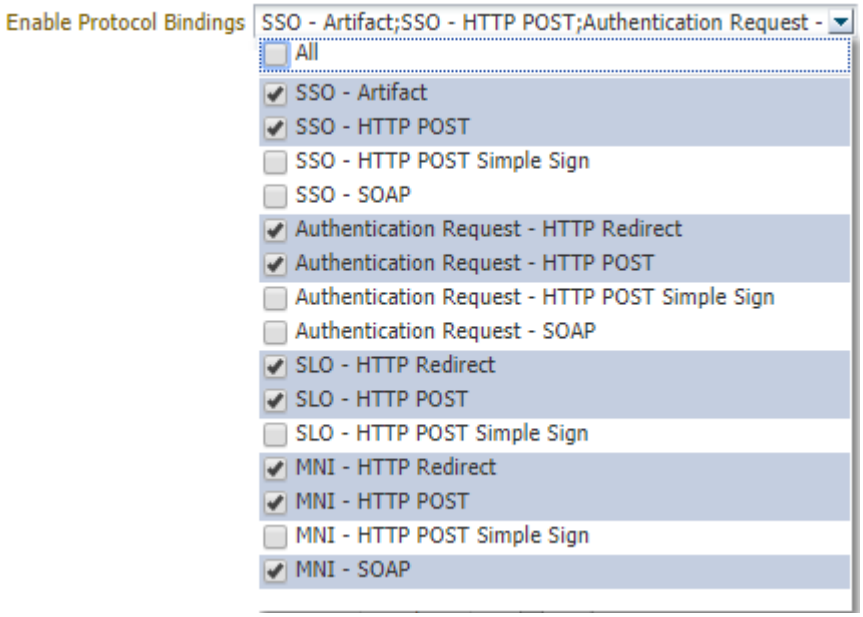
This section describes how to configure the SAML 2.0 Identity Provider (IdP) properties.

1. Log in to Enterprise Manager Fusion Middleware Control Console.
2. Expand **Identity and Access** folder, and choose **OIF(11.1.1.2.0)**.
3. Expand the **Oracle Identity Federation** menu, and go to **Administration**.
4. Click **Identity Provider**.
5. Click the **SAML 2.0** tab.
6. In the **Assertion Subject NameID Formats** table, ensure that the following formats are enabled:
   - **Email Address** and enter the attribute `mail`.
   - **Unspecified** and enter the attribute `uid`.

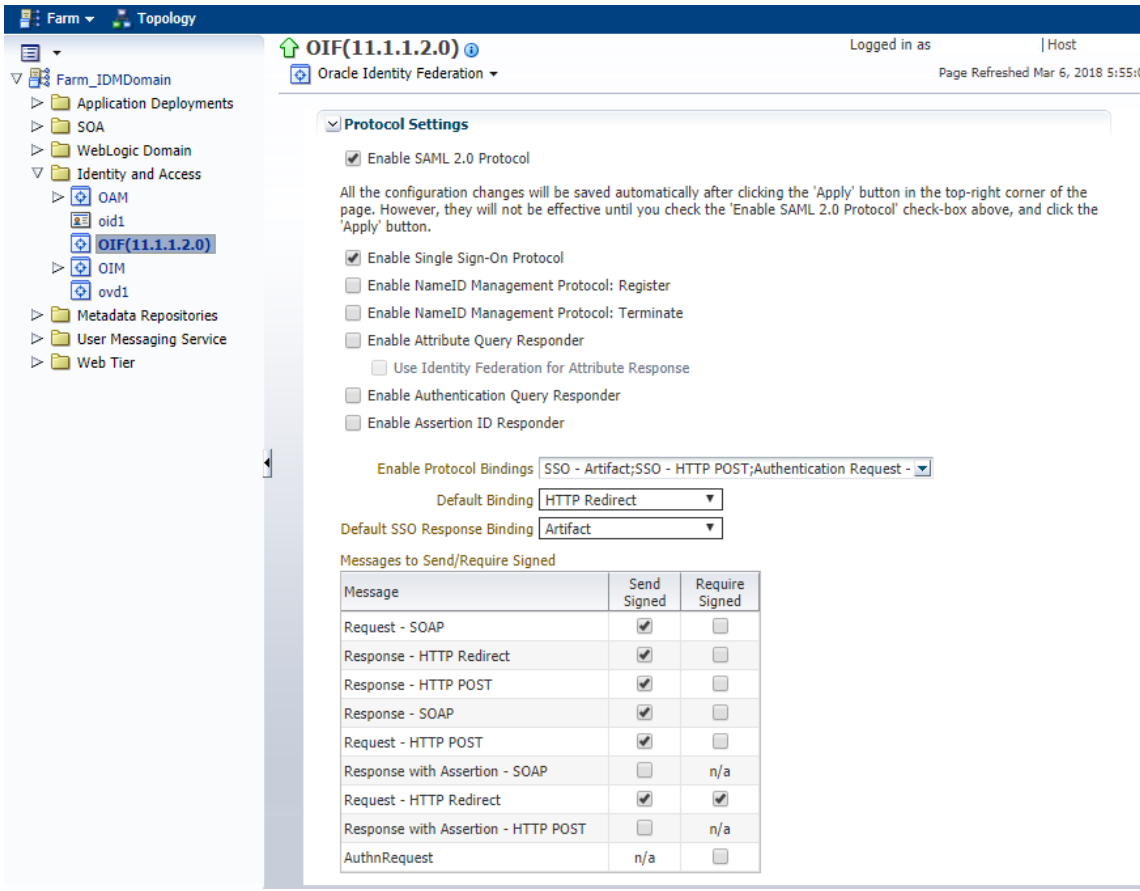


7. In the Protocol Settings, ensure that the following boxes are checked:
   - Enable SAML 2.0 Protocol
   - Enable Single Sign-On Protocol
8. Ensure that the following protocol bindings are selected from the **Enable Protocol Bindings** drop down list as shown in the figure:
   - SSO - Artifact
   - SSO - HTTP POST
   - Authentication Request - HTTP Redirect

- Authentication Request - HTTP Post
- SLO - HTTP Redirect
- SLO - HTTP Post
- MNI - HTTP Redirect
- MNI - HTTP Post
- MNI - SOAP



9. Ensure that `HTTP Redirect` is selected from the **Default Binding** drop down list.
10. Ensure that `Artifact` is selected from the **Default SSO Response Binding** drop down list.
11. In the **Messages to Send/Require Signed** table, ensure that the **Send Signed** box is checked for the following messages:
    - Request - SOAP
    - Response - HTTP Redirect
    - Response - HTTP Post
    - Response - SOAP
    - Request - HTTP POST
    - Request - HTTP Redirect
12. In the **Messages to Send/Require Signed** table, ensure that the **Require Signed** box is checked for the Request - HTTP Redirect message.

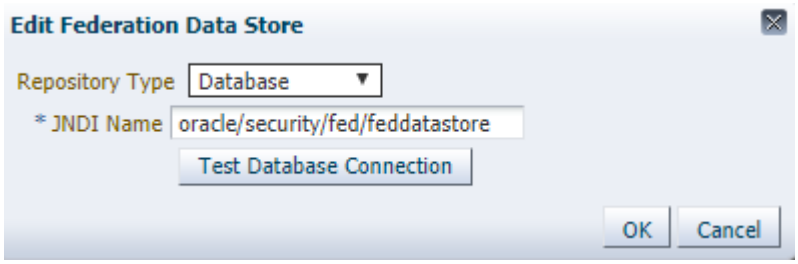


13. Click **Apply**.

4.4.3 Configure Data Stores

Configure Oracle Identity Federation to use Oracle Database as data stores as follows:

1. Log in to Enterprise Manager Fusion Middleware Control Console.
2. Expand **Identity and Access** folder, and choose **OIF(11.1.1.2.0)**.
3. Expand the **Oracle Identity Federation** menu, and go to **Administration**.
4. Click **Data Stores**.
5. In the Federation Data Store section, click **Edit**.
6. Select **Database** from the **Repository Type** drop down list.
7. Ensure that the **JNDI Name** is `oracle/security/fed/feddatastore` as shown in the following figure:

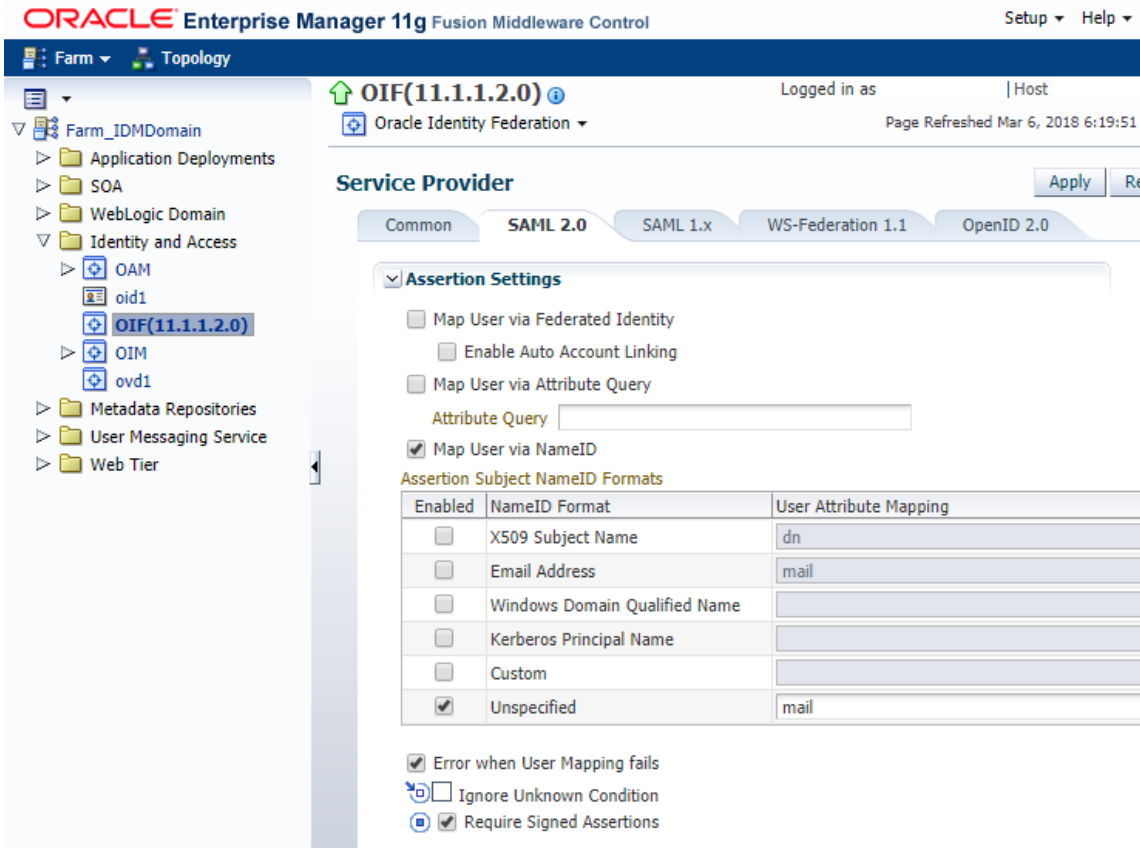


8. Click **OK**.
9. In the User Session Data Store and Message Data Store section, click **Edit** and perform Steps 6 through 8.
10. In the Configuration Data Store section, click **Edit** and perform Steps 6 through 8.

4.4.4 Configure Service Provider

To configure your SAML 2.0 Service Provider properties, perform the following steps:

1. Log in to Enterprise Manager Fusion Middleware Control Console.
2. Expand **Identity and Access** folder, and choose **OIF(11.1.1.2.0)**.
3. Expand the **Oracle Identity Federation** menu, and go to **Administration**.
4. Click **Service Provider**.
5. Click the **SAML 2.0** tab.
6. Ensure the **Map User via NameID** box is checked.
7. In the Assertion Subject NameID Formats table, ensure the **Unspecified** NameID Format is enabled, and then give it the value `mail` as shown in the following figure:



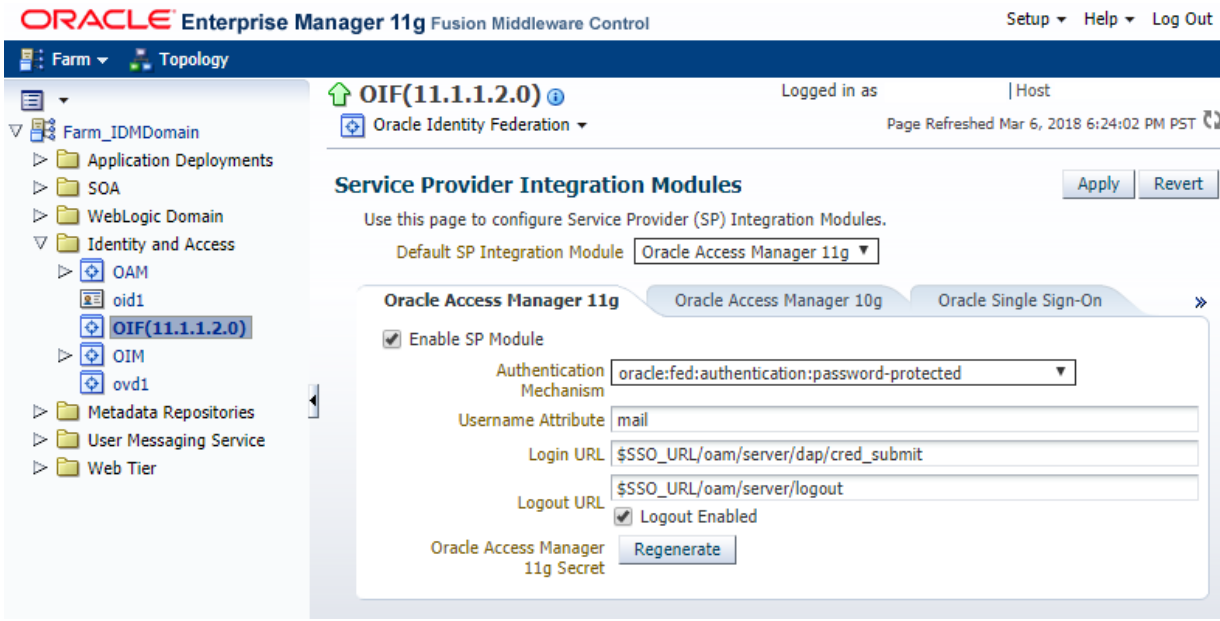
8. Ensure that the following boxes are checked:
   - Error when User Mapping fails
   - Require Signed Assertions
   - Enable SAML 2.0 Protocol.
   - Enable Single Sign-On Protocol
   - Allow Federation Creation
9. Ensure that the following options are selected from the **Enable Protocol Bindings** drop down list:
   - `SSO - Artifact`
   - `SSO - HTTP POST`
   - `SLO - HTTP Redirect`
10. Ensure that `HTTP Redirect` is selected from the **Default Binding** drop down list.
11. Ensure that `HTTP POST` is selected from the **Default SSO Request Binding** drop down list.
12. Ensure that `HTTP POST` is selected from the **Default SSO Response Binding** drop down list.
13. Ensure that `Unspecified` is selected from the **Default Authentication Request NameID Format** drop down list.
14. Ensure that `None` is selected from the **Request Authentication Context Mechanism** drop down list.

15. Ensure that `None` is selected from the **Request Authentication Context Comparison** drop down list.
16. Click **Apply**.

4.4.5 Configure Service Provider Integration Modules

To configure your service provider integration module, perform the following steps:

1. Log in to Enterprise Manager Fusion Middleware Control Console.
2. Expand **Identity and Access** folder, and choose **OIF(11.1.1.2.0)**.
3. Expand the **Oracle Identity Federation** menu, and go to **Administration**.
4. Click **Service Provider Integration Modules**.
5. In the **Oracle Access Manager 11g** tab, ensure that the **Enable SP Module** box is checked.
6. Select `oracle:fed:authentication:password-protected` from the **Authentication Mechanism** drop down list.
7. Provide the following details:
   - For Username Attribute, enter `mail`.
   - For Login URL, enter `$SSO_URL/oam/server/dap/cred_submit`.
   - For Logout URL, enter `$SSO_URL/oam/server/logout`.

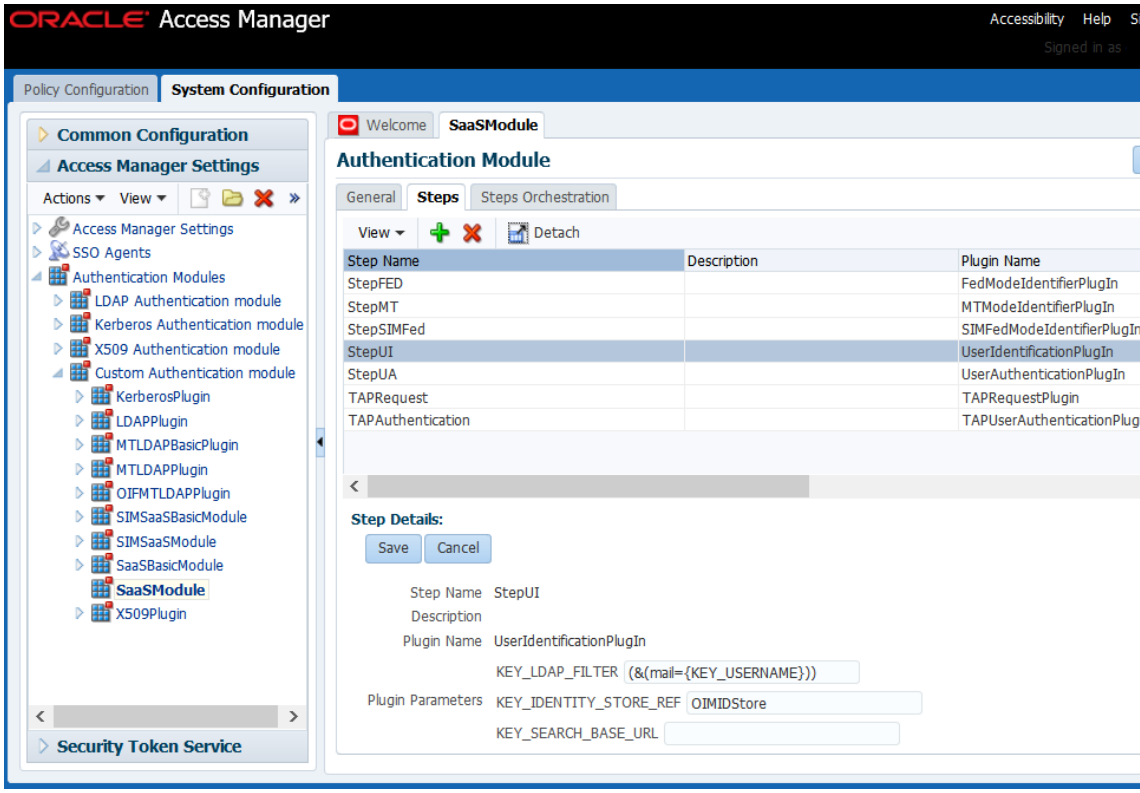


8. Ensure that the **Logout Enabled** box is checked.
9. Click **Apply**.

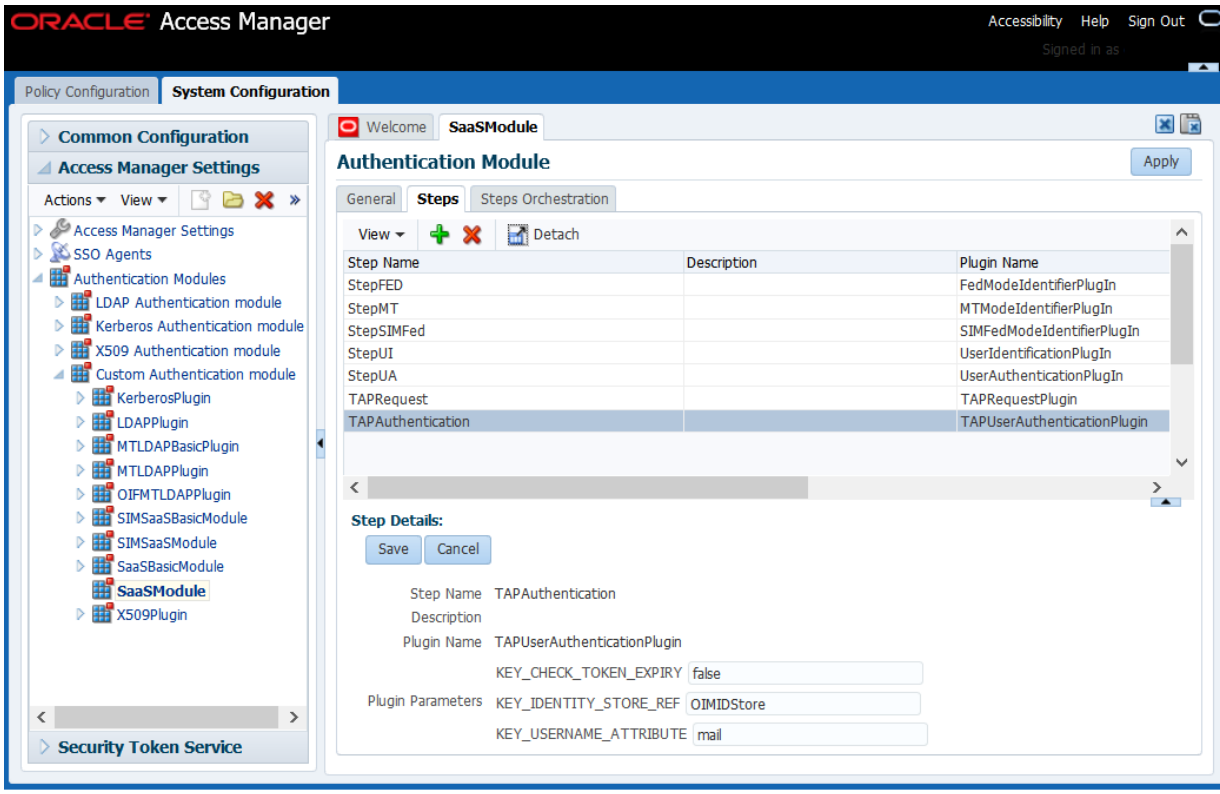
4.4.6 Configure OAM

To configure Oracle Access Manager (OAM), perform the following steps:

1. Log in to the OAM console.
2. Click the **System Configuration** tab, and expand **Access Manager Settings**.
3. Expand the **Authentication Module** and the **Custom Authentication Module**.
4. Double click **SaaS Module**.
5. Click the **Steps** tab.
6. Choose **StepUI** from the **Step Name** column.
7. Update the value of the `KEY_LDAP_FILTER` parameter from `uid` to `mail` as shown in the following figure:



8. Click **Save**.
9. Choose **TAPAuthentication** from the **Step Name** column.
10. Update the value of the `KEY_USERNAME_ATTRIBUTE` parameter from `uid` to `mail` as shown in the following figure:

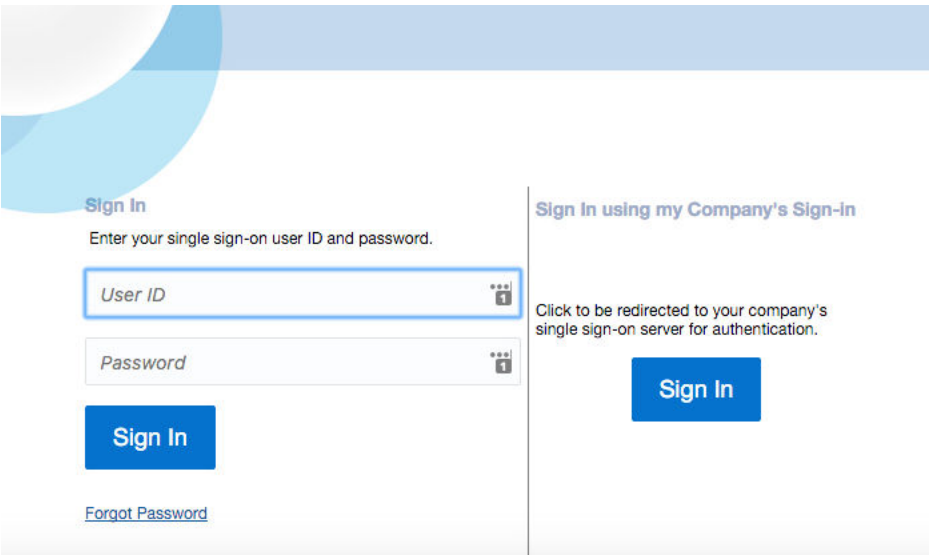


11. Click **Save**.
12. Click **Apply**.

4.4.7 Verify If Resource Is Protected

To verify if the `IAMSuiteAgent:/welcome_webcenter.html` resource is protected, perform the following steps:

1. Go to `https://sso_lbr server: PORT URL/welcome_webcenter.html`.
    - If you configured your Single Sign-On (SSO) with federation as described in Configure OIF with an Identity Provider, Step 4, then the login page shows two login options as shown in the following figure. One login option is a local FA and the other one is an IdP login.

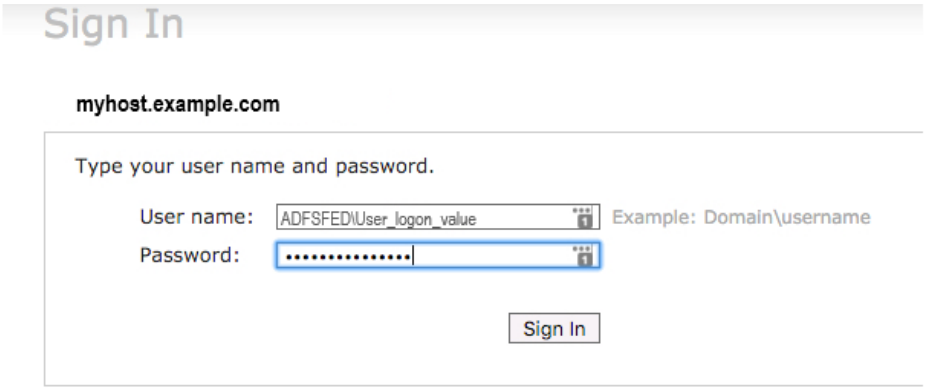


a. Click **Sign In** in the "Sing In using my Company's Sign-in" section.

   You are redirected to the IdP login page.

b. Log in using the Domain\Username and your password.

- If you did not configure your SSO with federation, then the login page shows only the IdP login option.



  – Log in using your Domain/username and your password.

2. Perform SSO and Single Logout (SLO).

4.5 Migrate Users from AD to OID

> **Note:**
>
> The steps in this section are only applicable if you use OVD to proxy AD in split profile. If you use OVD to proxy OID, skip to Remove OVD.

When OVD is set up in split profile, most of your data comes from Active Directoy (AD), and some FA specific attributes get stored in OID under a different branch. This branch is referred to as Remote Base in Adapter configuration cn=shadowentries. To remove the AD dependency, you must copy the user attributes needed by FA and make them available in the bundled OID. Note that AD still remains the source of truth and FA specific attributes will be saved in OID.

To migrate users from AD to OID, you must run the tool that is bundled with the IDM patch 25734394 and perform the following tasks:

- Run the ldifde Tool
- Run IDM Migrate Utility

4.5.1 Run the ldifde Tool

To export users from AD to a `ldif` file, perform the following steps:

1. Run the `ldifde` tool on the AD machine as follows:

   ```
   ldifde -s <AD Host machine name> -t <AD port> -a <AD Domain name>\<user>
   <password> -d "<AD user base DN>" -p subtree -f c:\<path to a ldif file> -l
   "dn,sn,uid,mail,objectclass" -c "<AD user base DN>" "<oid user base DN>"
   ```

   For example:

   ```
   ldifde -s myhost.example.com -t 389 -a ADFSFED\windows <password> -
   d "CN=Users,DC=adfs,DC=fed,DC=example,DC=com" -p subtree -f c:\ad_users.ldif -
   l "dn,sn,uid,mail,objectclass" -
   c "CN=Users,DC=adfs,DC=fed,DC=example,DC=com" "cn=Users, dc=example,dc=com"
   ```

   You can obtain the values for the user base DN from the OVD adapter configuration.

2. Copy the generated `ldif` file from the AD Windows machine to the `*nix` box that is hosting IDM for FA.

4.5.2 Run IDM Migrate Utility

The steps in this section take the ldif file generated in Run the ldifde Tool and loads the AD users data in a bundled OID.

To run the migrate utility, perform the following steps:

1. Set the following environment variables:
   - `MW_HOME` to the directory middleware home
   - `ORACLE_HOME` to the OID oracle home
   - `JDK_HOME` to the jdk6 path
2. Run the following command:

   ```
   cd <idm patch unzip location>/idmUpgrade/IDMFAOnPremiseUpgrade/bin
   bash LoadADusers2OID.sh -H <OID Host> -D <OID Bind DN> -f <path to
   AD users ldif file> -G "cn=groups,dc=example,dc=com" -O "cn=shadowentries" -
   N "cn=users,dc=example,dc=com"
   ```

   Command usage:

   ```
   bash LoadADusers2OID.sh <options> [-p|--port <port>]
   ```

Where <options>

- `-H|--HOST`: [Required] OID host name
- `-p|--port`: [Optional] OID Server port. Default port `3060`
- `-D|--bindDN`: [Required] OID Server bind DN
- `-f|--ad_users_ldif_file`: [Required] path of exported AD users `ldif` file to be imported in OID
- `-G|--oid_group_base`: [Required] OID group search base
- `-O|--old_ad_container_dn`: [Required] Shadow entries container (For example, `cn=shadowentries`) of AD users in OID
- `-N|--new_ad_container_dn`: [Required] New user container DN to be used for AD users

For example:

```
bash LoadADusers2OID.sh -H <OID host> -p|--port  <OID server port> -D <OID Bind
DN> -f|--ad__users_ldif_file <path to AD users ldif file-G <OID group search
base> -O <Old AD container DN> -N <new AD container DN in OID>

bash LoadADusers2OID.sh --HOST <OID Host> --bindDN <OID Bind DN>  --
ad_users_ldif_file ./AD_users.ldif --
oid_group_base "cn=groups,dc=example,dc=com" --
old_ad_container_dn "cn=shadowentries" --
new_ad_container_dn "cn=users,dc=example,dc=com"
```

Note that this scripts prompts you for the `bindDN` password.

This command takes backup of users and groups in OID, and then loads the AD users into OID. After the command is run users from AD appears in the OID under user search base DN.

4.6 Remove OVD

To remove Oracle Virtual Directory (OVD), follow the steps as described in the following sections:

- Update WLS Authenticator Configuration
- Update OAM Configuration
- Update OIM Configuration
- Update Federation Configuration
- Remove OVD Authenticator
- Remove OVD Component
- Update OID Authenticator
- Verify OID Authenticator Configuration
- Update JPS Configuration
- Post OVD Removal Task

4.6.1 Update WLS Authenticator Configuration

To update your WebLogic Server (WLS) authenticator configuration, perform the following steps:

1. Log in to the WebLogic Server Administration Console.
2. Click **Lock & Edit**.
3. Navigate to **Security Realm** under **IDMDomain**.
4. Go to **myrealm**, then click the **Providers** tab.
5. Click **New** and add a new `OracleInternetDirectoryAuthenticator` authenticator and name it `OIDAuthenticator`.

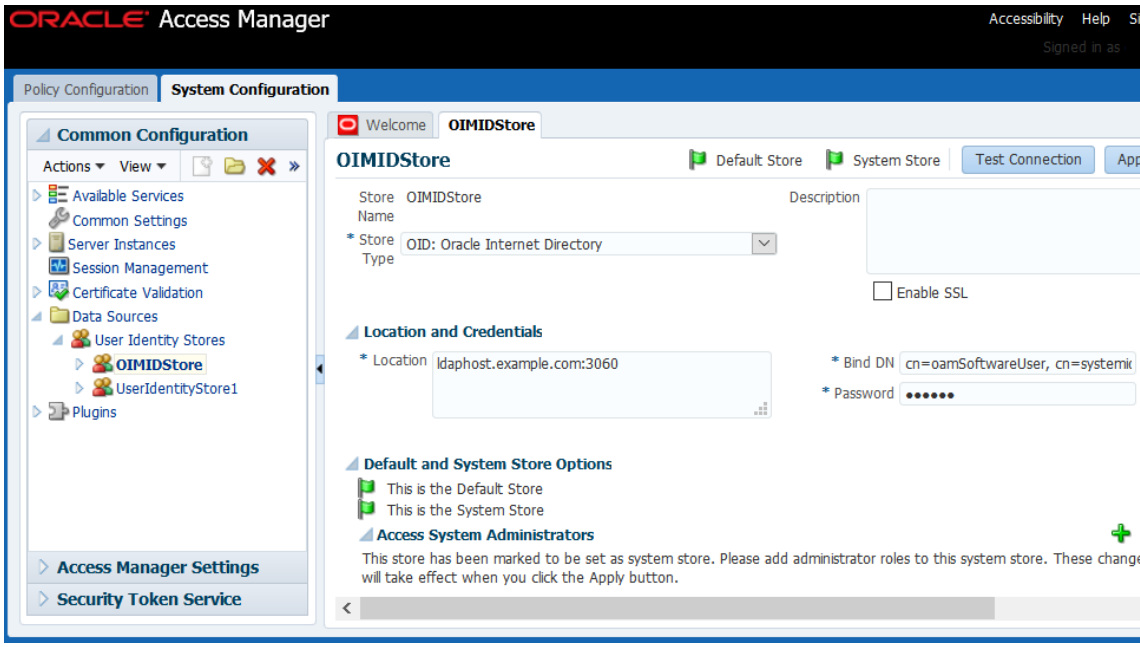
> **Note:**
>
> Ensure there are no spaces in the authenticator name.

6. Set the OPTIONAL control flag to SUFFICIENT.
7. Update the configuration of that OVD, except for the port's SUFFICIENT flag.
8. Enter the OID port in the **Port** field, and click **Save**.
9. Reorder the authenticator and place it below the OVD authenticator.

4.6.2 Update OAM Configuration

To update your Oracle Access Manager (OAM) configuration, perform the following steps:

1. Log in to the OAM console.
2. Click the **System Configuration** tab, and expand **Common Configuration**.
3. Expand **Data Sources** and **User Identity Store**.
4. Click **OIMIDStore**.
5. Update the value of **Store Type** to **OID: Oracle Internet Directory** as shown in the following figure:



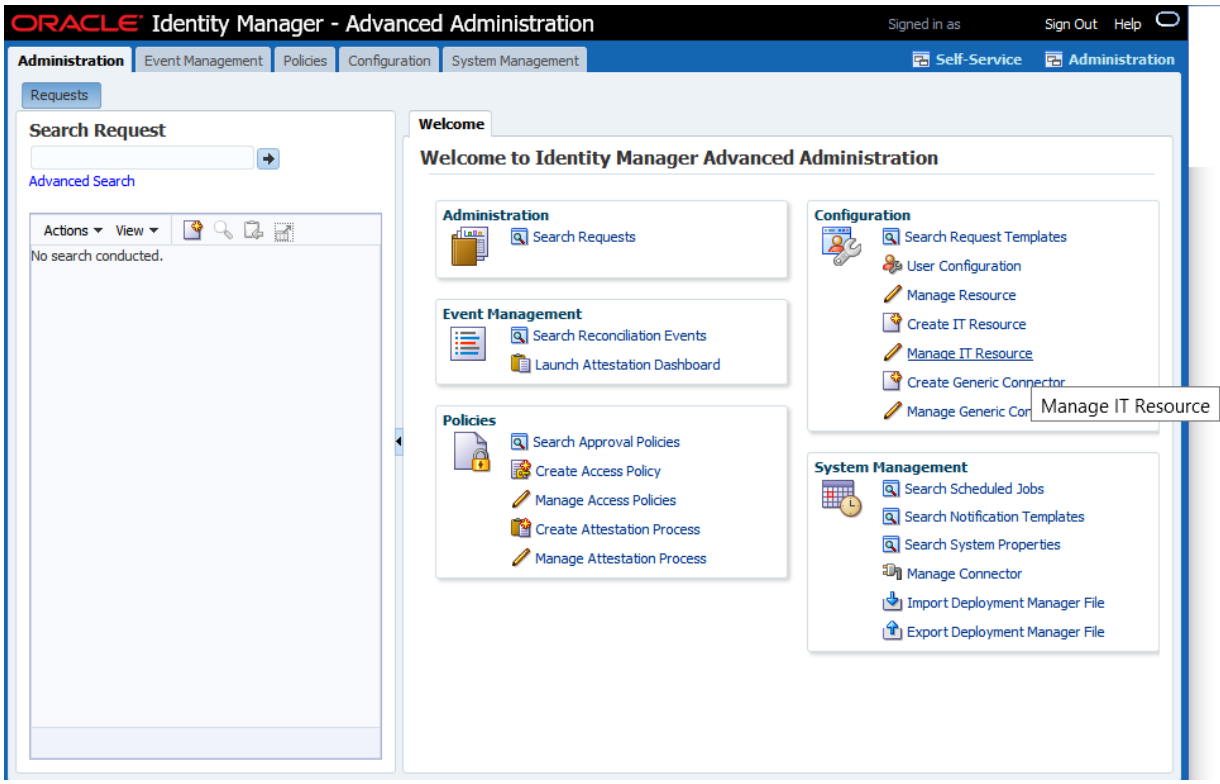
6. Click **Apply**.

If you have any issues updating the values, see OAM Configuration Update Fails for OVD Removal.

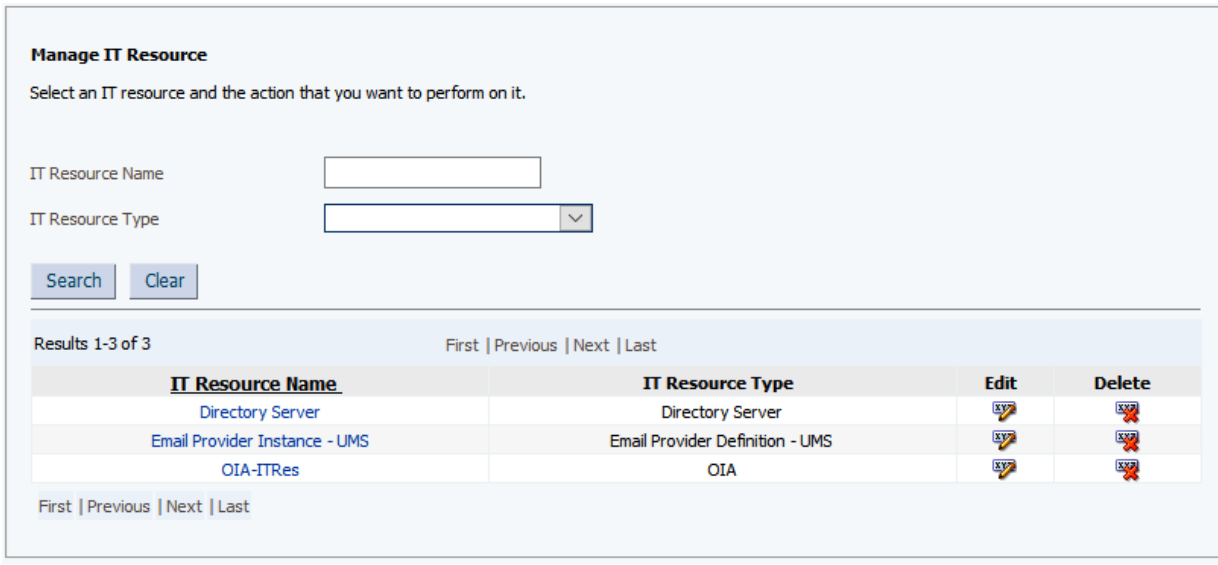
4.6.3 Update OIM Configuration

To update your Oracle Identity Manager (OIM) configuration, perform the following steps:

1. Log in to the OIM console.
2. Navigate to **Advanced**, then go to **Manage IT Resource** under **Configuration** as shown in the following figure:



3. Click **Search** and choose **Directory Server** as shown in the following figure:



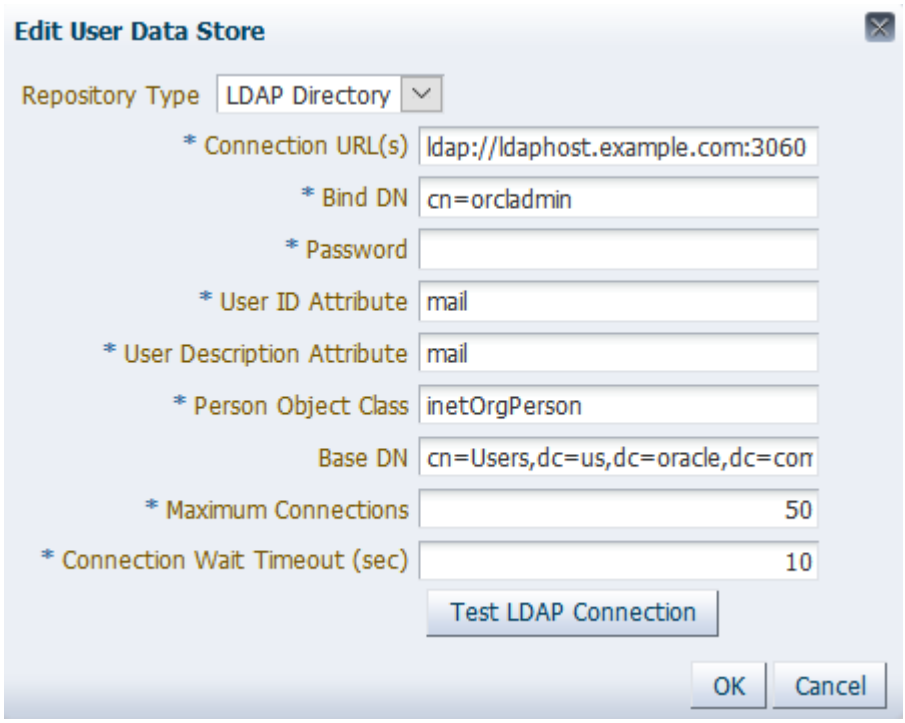
4. Click **Edit**.
5. Update the values for the following parameters:
   - **Server SSL URL** to `ldaps://ldaphost.example.com:3131`
   - **Server URL** to `ldap://ldaphost.example.com:3060`
6. Click **Update**.

4.6.4 Update Federation Configuration

> **Note:**
>
> This step is only applicable if you use OVD to proxy AD in split profile. If you use OVD to proxy OID, skip to Remove OVD Authenticator.

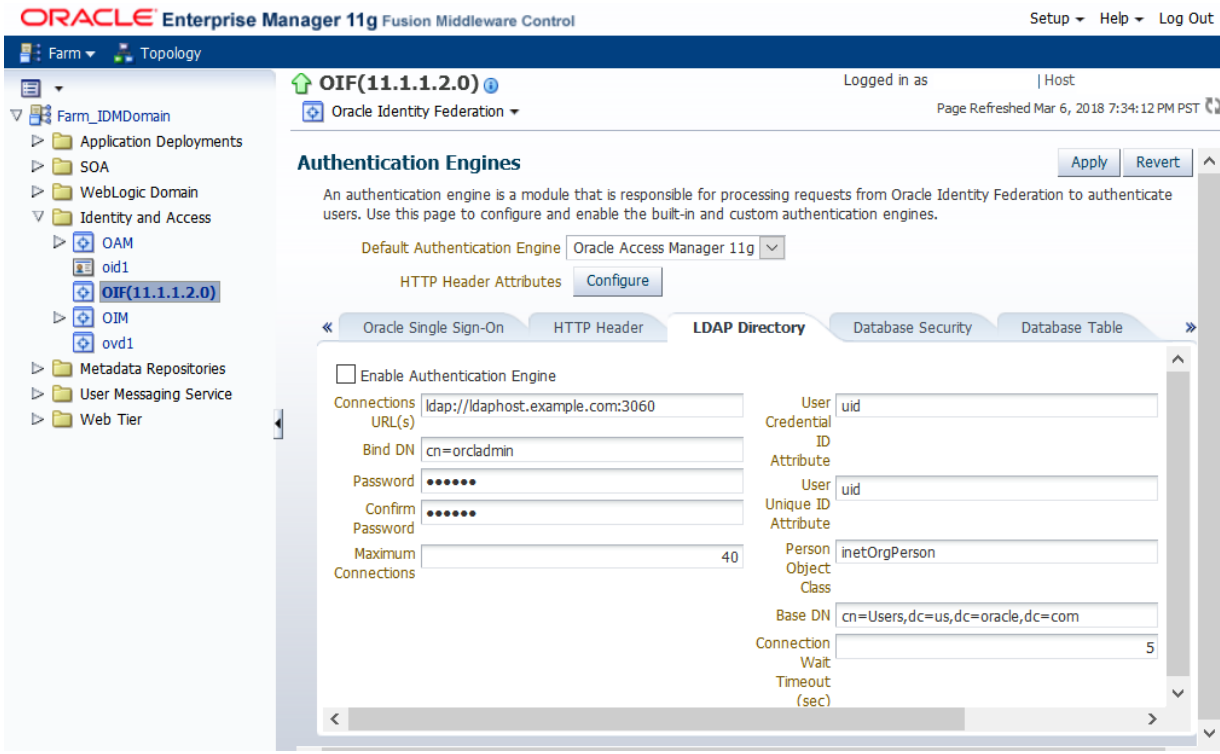
To update the LDAP ports in the Data Store and in the Authentication Engines, perform the following steps:

1. Log in to Enterprise Manager Fusion Middleware Control Console.
2. Expand **Identity and Access** folder, and choose **OIF(11.1.1.2.0)**.
3. Expand the **Oracle Identity Federation** menu, and go to **Administration**.
4. Click **Data Stores**.
5. In the User Data Store section, click **Edit**.
6. Update the **Connection URL(s)** to `ldap://ldaphost.example.com:3060` as shown in the following figure:



7. Click **OK**.
8. Navigate to the **Oracle Identity Federation** menu, and go to **Administration**.
9. Click **Authentication Engines**.
10. Click the **LDAP Directory** tab.

11. Update the **Connection URL(s)** to `ldap://ldaphost.example.com:3060` as shown in the following figure:



12. Click **Apply**.

4.6.5 Remove OVD Authenticator

To remove your OVD authenticator, perform the following steps:

1. Log in to the WebLogic Server Administration Console.
2. Click **Lock & Edit**.
3. Navigate to **Security Realm** under **IDMDomain**.
4. Go to **myrealm**, then click the **Providers** tab.
5. Click **OVDAuthenticator**.
6. Delete the OVD authenticator in the **Provider Configuration** page.
7. Restart the Admin server and all of the other servers.

4.6.6 Remove OVD Component

This step is only applicable to scenarios where OVD is part of the OID instance. Skip this step if OID and OVD are separate in your environment.

To remove your OVD component, perform the following steps:

1. Shut down OID.
2. Back up the `opmn.xml` file under the OID instance.

3. Remove the OVD `ias-component` tag.
4. Restart OID.

4.6.7 Update OID Authenticator

This step is only applicable if you use OVD to proxy AD in split profile. Skip this step if you use OVD to proxy OID.

To update your OID authenticator, perform the following steps:

1. Log in to the WebLogic Server Administration Console.
2. Click **Lock & Edit**.
3. Navigate to **Security Realm** under **IDMDomain**.
4. Go to **myrealm**, then click the **Providers** tab.
5. Click **OIDAuthenticator**, and then update its Users and Groups as follows:
   - Users: "`cn=users,dc=example,dc=com`"
   - Groups: "`cn=groups,dc=example,dc=com`"
6. Click **Save** and apply the changes.

4.6.8 Verify OID Authenticator Configuration

To verify if your OID authenticator configuration is correct, perform the following steps:

1. Ensure the WebLogic Server (WLS) is in `RUNNING` mode again.
2. Log in to the WebLogic Server Administration Console.
3. Click **Lock & Edit**.
4. Navigate to **Security Realm** under **IDMDomain**.
5. Go to **myrealm**, then click the **Users and Groups** tab.

   If the configuration is correct, the **Users** sub-tab is selected by default and you can see the browsed users. Also, note that each user has the Provider listed as `OIDAuthenticator`.

4.6.9 Update JPS Configuration

To update your JPS configuration, perform the following steps:

1. Run the following command:

   ```
   cd $DOMAIN_HOME/config/fmwconfig
   ```

2. Update the following values under `idstore.ldap serviceInstance` in the `jps-config.xml` file:
   a. Update the value of the `idstore.type` property to `OID`.
   b. Point the `ldap.url` to the OID server and port:

   ```
   <serviceInstance name="idstore.ldap" provider="idstore.ldap.provider">
       <property name="idstore.type" value="OID"/>
       <property name="ldap.url" value="ldap://myhost.example.com:3060"/>
   </serviceInstance>
   ```

> **Note:**
>
> If `idstore.type` and `ldap.url` are not already present in the file, add them. Then, change the ldap host and port appropriately.

3. Bounce the environment.

4.6.10 Post OVD Removal Task

After OVD removal, ensure that basic IDM operations such as logins and SSO are working fine.

5
Run Pre-Downtime Checks

This section describes how to ensure system reliability by running pre-downtime checks. The following topics are discussed:

- Run the Health Checker Utility
- Run the Prevalidation Check on IDM Hosts

5.1 Run the Health Checker Utility

Health Checker is a command line utility that performs a set of validation checks against an Oracle Fusion Applications environment to ensure that the environment meets recommended standards. When Health Checker runs, it uses a specific manifest file that performs the appropriate checks. Health Checker provides a list of corrective actions for any checks that fail validation. The suggested corrective actions must be run manually to fix the issue before proceeding with the upgrade. The following topics are discussed in this section:

- Pre-Downtime Health Checker Manifests
- Run Health Checker on the Primordial Host
- Run Health Checker on the Midtier Host
- Run Health Checker on the OHS Host

5.1.1 Pre-Downtime Health Checker Manifests

When running Health Checker during pre-downtime, the following manifests are run:

- `GeneralSystemHealthChecks.xml`: Run on the Primordial, Midtier, and OHS hosts
- `PreDowntimeUpgradeReadinessHealthChecks.xml`: Run on the Primordial, Midtier, and OHS hosts
- `DataQualityChecks.xml`: Run on the Primordial host only

For more information about the checks performed by Health Checker, see Health Checker Plug-ins.

5.1.2 Check for Supported Perl Versions

Ensure that a supported Perl version is running. The following are the only versions that are supported:

- 5.8.8 (default in OEL5)
- 5.10.0 (bundled with MW_HOMEs)
- 5.10.1 (default in OEL6)

5.1.3 Run Health Checker on the Primordial Host

Before running Health Checker (HC) on the Primordial host, verify that the preupgrade JRE locations is as follows:

APPLICATIONS_BASE/fusionapps/jdk6/

After the location has been verified, run Health Checker on the Primordial host by performing the following steps:

1. Confirm that all Oracle Fusion Applications, database and Oracle Identity Management services are up and running.
2. Set the following environment variables:
   - *APPLICATIONS_BASE*: The directory that contains Oracle Fusion Applications. For example, if Oracle Fusion Applications is installed in /u01/APPTOP/fusionapps, then set the APPLICATIONS_BASE environment variable to /u01/APPTOP.
   - *DOWNLOAD_PATCH_DIR*: The location where post-release patches were downloaded, *SHARED_LOCATION*/11.12.x.0.0_post_repo_patches, in Download and Unzip Mandatory Post-Release 12 Patches.
   - *HC_OVERRIDE_FILES*: The location of any Health Checker overrides that may have been created, as described in Download Patches for the Health Checker Exclusion List. If the HC_OVERRIDE_FILES variable is not set, the default location is *APPLICATIONS_BASE*/instance/fapatch/healthchecker. Note that when Health Checker is run through orchestration, this environment variable is set by orchestration, to *SHARED_UPGRADE_LOCATION*/healthchecker/*POD_NAME*.

     It is possible to skip this environment variable if there are no Health Checker overrides.
   - *RUP_OVERRIDE*: The location of the override file for RUP Installer, that may have been created in Create an Override File for RUP Installer. If there is not an override file for RUP Installer, skip this environment variable.
   - REPOSITORY_LOCATION: The directory that contains the repository SHARED_LOCATION/11.12.x.0.0/Repository. See Download and Unzip the Release 12 Repository.
3. Run Health Checker for each manifest:

   Note that this is one command.

```
(UNIX)
ORCH_LOCATION/fusionapps/applications/lcm/hc/bin/hcplug.sh -hostType PRIMORDIAL
-manifest
ORCH_LOCATION/fusionapps/applications/lcm/hc/config/
GeneralSystemHealthChecks.xml [-DlogLevel=log_level]

ORCH_LOCATION/fusionapps/applications/lcm/hc/bin/hcplug.sh -hostType PRIMORDIAL
-manifest
ORCH_LOCATION/fusionapps/applications/lcm/hc/config/
PreDowntimeUpgradeReadinessHealthChecks.xml [-DlogLevel=log_level]

ORCH_LOCATION/fusionapps/applications/lcm/hc/bin/hcplug.sh -hostType PRIMORDIAL
-manifest
ORCH_LOCATION/fusionapps/applications/lcm/hc/config/DataQualityChecks.xml [-
DlogLevel=log_level]
```

4. If any health checks fail, refer to the Health Checker log files and reports to find the corrective actions to resolve the issue. The suggested corrective actions must be run manually to fix the issue before proceeding with the upgrade. Then rerun Health Checker to ensure all checks are successful. Optionally, use the `-checkpoint true` option when restarting Health Checker, so that only the failed plug-ins or the plug-ins that did not run are executed.

   If the failure is a known issue and the check needs to be excluded, see Override Health Checks.

   The following table provides the location of log files and reports on the primordial host. Health Checker log directories are created with reference to version being upgraded from. For example:

   - If the upgrade is from 11.1.8.0.0 to 11.1.11.0.0, the log directory is 11.1.8.0.0.
   - If the upgrade is from 11.1.9.2.0, the log directory is 11.1.9.2.0.
   - If the upgrade is from 11.1.10.0.0, the log directory is 11.1.10.0.0.
   - If the upgrade is from 11.1.11.0.0, the log directory is 1.1.11.0.0

Table 5-1 Health Checker Log Files and Reports on the Primordial Host

Manifest File Name	Log File Location	Report Location - html and xml formats
GeneralSystemHealthChecks.xml	*APPLICATIONS_CONFIG*/lcm/logs/11.1.11.0.0/healthchecker/primordial_*hostname*-GeneralSystemHealthChecks_*timestamp*.log	*APPLICATIONS_CONFIG*/lcm/logs/11.1.11.0.0/healthchecker/primordial_*hostname*-GeneralSystemHealthChecks_*timestamp*.html *APPLICATIONS_CONFIG*/lcm/logs/11.1.11.0.0/healthchecker/primordial_*hostname*-GeneralSystemHealthChecks_*timestamp*.xml
PreDowntimeUpgradeReadinessHealthChecks.xml	*APPLICATIONS_CONFIG*/lcm/logs/11.1.11.0.0/healthchecker/primordial_*hostname*-PreDowntimeUpgradeReadinessHealthChecks_*timestamp*.log	*APPLICATIONS_CONFIG*/lcm/logs/11.1.11.0.0/healthchecker/primordial_*hostname*-PreDowntimeUpgradeReadinessHealthChecks_*timestamp*.html *APPLICATIONS_CONFIG*/lcm/logs/11.1.11.0.0/healthchecker/primordial_*hostname*-PreDowntimeUpgradeReadinessHealthChecks_*timestamp*.xml

Table 5-1 (Cont.) Health Checker Log Files and Reports on the Primordial Host

Manifest File Name	Log File Location	Report Location - html and xml formats
DataQualityChecks.xml	*APPLICATIONS_CONFIG*/lcm/logs11.1.11.0.0/healthchecker/primordial_*hostname*-DataQualityChecks_*timestamp*.log	*APPLICATIONS_CONFIG*/lcm/logs/11.1.11.0.0/healthchecker/primordial_*hostname*-DataQualityHealthChecks_*timestamp*.html *APPLICATIONS_CONFIG*/lcm/logs/11.1.11.0.0/healthchecker/primordial_*hostname*-DataQualityChecks_*timestamp*.xml

5.1.4 Run Health Checker on the Midtier Host

Before running Health Checker (HC) on the midtier host, verify that the preupgrade JRE locations is as follows:

APPLICATIONS_BASE/fusionapps/jdk6/

After the location has been verified, run Health Checker on the midtier host by performing the following steps:

1. Set the following environment variables:
   - *APPLICATIONS_BASE*: The directory that contains Oracle Fusion Applications. For example, if Oracle Fusion Applications is installed in /u01/APPTOP/fusionapps, then set the APPLICATIONS_BASE environment variable to /u01/APPTOP.
   - *REPOSITORY_LOCATION*: The directory where the repository is staged, *SHARED_LOCATION*/11.12.x.0.0/Repository.
   - *HC_OVERRIDE_FILES:* The location of any Health Checker overrides that may have been created, as described in Download Patches for the Health Checker Exclusion List. If the HC_OVERRIDE_FILES variable is not set, the default location is *APPLICATIONS_BASE*/instance/fapatch/healthchecker. Note that when Health Checker is run through orchestration, this environment variable is set by orchestration, to *SHARED_UPGRADE_LOCATION*/healthchecker/*POD_NAME*.

     It is possible to skip this environment variable if there are no Health Checker overrides.
2. Run Health Checker for each manifest as follows:

   Note that this is one command.

```
(UNIX)
ORCH_LOCATION/fusionapps/applications/lcm/hc/bin/hcplug.sh  -hostType MIDTIER -
manifest
ORCH_LOCATION/fusionapps/applications/lcm/hc/config/
GeneralSystemHealthChecks.xml  [-DlogLevel=log_level]

ORCH_LOCATION/fusionapps/applications/lcm/hc/bin/hcplug.sh -hostType MIDTIER -
manifest
```

```
ORCH_LOCATION/fusionapps/applications/lcm/hc/config/
PreDowntimeUpgradeReadinessHealthChecks.xml [-DlogLevel=log_level]
```

3. If any health checks fail, refer to the Health Checker log files and reports to find the corrective actions to resolve the issue. The suggested corrective actions must be run manually to fix the issue before proceeding with the upgrade. Then rerun Health Checker to ensure all checks are successful. Optionally, use the `-checkpoint true` option when restarting Health Checker, so that only the failed plug-ins or the plug-ins that did not run are executed.

   If the failure is a known issue and the check needs to be excluded, see Override Health Checks.

   The following table provides the location of log files and reports on the Midtier host. Health Checker log directories are created with reference to version being upgraded from. For example:

   - If the upgrade is from 11.1.8.0.0 to 11.1.10.3.0, the log directory is 11.1.8.0.0.
   - If the upgrade is from 11.1.9.2.0, the log directory is 11.1.9.2.0.

Table 5-2 Health Checker Log Files and Reports on the Midtier Host

Manifest File Name	Log File Location	Report Location - html and xml formats
GeneralSystemHealthChecks.xml	*APPLICATIONS_CONFIG*/lcm/logs/11.1.11.0.0/healthchecker/midtier_*hostname*-GeneralSystemHealthChecks_*timestamp*.log	*APPLICATIONS_CONFIG*/lcm/logs/11.1.11.0.0/healthchecker/midtier_*hostname*-GeneralSystemHealthChecks_*timestamp*.html *APPLICATIONS_CONFIG*/lcm/logs/11.1.11.0.0/healthchecker/midtier_*hostname*-GeneralSystemHealthChecks_*timestamp*.xml
PreDowntimeUpgradeReadinessHealthChecks.xml	*APPLICATIONS_CONFIG*/lcm/logs/11.1.11.0.0/healthchecker/midtier_*hostname*-PreDowntimeUpgradeReadinessHealthChecks_*timestamp*.log	*APPLICATIONS_CONFIG*/lcm/logs/11.1.11.0.0/healthchecker/midtier_*hostname*-PreDowntimeUpgradeReadinessHealthChecks_*timestamp*.html *APPLICATIONS_CONFIG*/lcm/logs/11.1.11.0.0/healthchecker/midtier_*hostname*-PreDowntimeUpgradeReadinessHealthChecks_*timestamp*.xml

5.1.5 Run Health Checker on the OHS Host

Before running Health Checker (HC) on the OHS host, verify that the preupgrade JRE locations is as follows:

APPLICATIONS_BASE/fusionapps/jdk6/

After the location has been verified, run Health Checker on the OHS host by performing the following steps:

1. Confirm that ORCH_LOCATION is set up correctly and is ready for running Health Checker on the OHS host by verifying that the ORCH_LOCATION/webtier_mwhome directory exists. If this directory does not exist, run orchsetup.py as described in Set Up Upgrade Orchestrator on a Shared Location.
2. Set the following environment variables:
   - *APPLICATIONS_BASE:* The variable APPLICATIONS_BASE is required to point to ORCH_LOCATION to run HC on the OHS host only. This variable was created in Unzip Orchestration.zip.
   - *REPOSITORY_LOCATION*: The directory where the repository is staged, *SHARED_LOCATION*/11.12.x.0.0/Repository.
   - *JAVA_HOME*: The jdk location under the applications base on the OHS host, for example, /APPTOP/webtier_mwhome/webtier/jdk6. Do not use the jdk under the orchestration directory. Note that this same location is used for the -jreloc argument when running the commands in this section.
   - *WT_MW_HOME*: Location of the Web Tier *MW_HOME*, for example, /APPTOP/webtier_mwhome.
   - *WT_ORACLE_HOME*: Location of the Web Tier directory, which is a subdirectory under *WT_MW_HOME*, for example:/APPTOP/webtier_mwhome/webtier.
   - *WT_CONFIG_HOME*: Location of the Web Tier instance configuration home, for example: /u01/mw_home/Oracle_WT1/instance/CommonDomain_webtier.
   - *OHS_INSTANCE_ID*: The OHS instance ID on the host. Normally this is ohs1 and is the value for ias-component id in the opmn.xml file.
   - *OHS_UPGRADE_BINARIES_HOSTNAME*: A comma separated list of your OHS host names, which do not share binaries. For example, if there are a main OHS host and a scaled out OHS host, both pointing to the same binaries, this environment variable should list only the main OHS host, since the scaled out OHS host is using shared binaries. Note that this parameter is optional.
   - *CURRENT_FA_RELEASE_VERSION*: The current version on the environment before the upgrade, such as 11.1.11.0.0.
   - *DOWNLOAD_PATCH_DIR*: The location of downloaded post-release patches, *SHARED_LOCATION*/11.12.x.0.0_post_repo_patches, which was downloaded in Download and Unzip Mandatory Post-Release 12 Patches.
   - *HC_OVERRIDE_FILES*: The location of any Health Checker overrides that may have been created, as described in Download Patches for the Health Checker Exclusion List. If the HC_OVERRIDE_FILES variable is not set, the default location is *APPLICATIONS_BASE*/instance/fapatch/healthchecker. Note that when Health Checker is run through orchestration, this environment variable is set by orchestration, to *SHARED_UPGRADE_LOCATION*/healthchecker/*POD_NAME*. See Override Health Checks.

     It is possible to skip this environment variable if there are no Health Checker overrides.
3. Run Health Checker for each manifest as follows:

   Note that this is one command.

```
(UNIX)
ORCH_LOCATION/fusionapps/applications/lcm/hc/bin/hcplug.sh -hostType OHS -
manifest
ORCH_LOCATION/fusionapps/applications/lcm/hc/config/
GeneralSystemHealthChecks.xml [-DlogLevel=log_level] -jreLoc JDK_LOCATION -
logDir /u01/logs/OHS

ORCH_LOCATION/fusionapps/applications/lcm/hc/bin/hcplug.sh -hostType OHS -
manifest
ORCH_LOCATION/fusionapps/applications/lcm/hc/config/
PreDowntimeUpgradeReadinessHealthChecks.xml [-DlogLevel=log_level] -jreLoc
JDK_LOCATION -logDir /u01/logs/OHS
```

4. If any health checks fail, refer to the Health Checker log files and reports to find the corrective actions to resolve the issue. The suggested corrective actions must be run manually to fix the issue before proceeding with the upgrade. Then rerun Health Checker to ensure all checks are successful. Optionally, use the `-checkpoint true` option when restarting Health Checker, so that only the failed plug-ins or the plug-ins that did not run are executed.

   If the failure is a known issue and the check needs to be excluded, see Override Health Checks.

   The following table provides the location of log files and reports on the OHS host:

Table 5-3 Health Checker Log Files and Reports on the OHS Host

Manifest File Name	Log File Location	Report Location - html and xml formats
GeneralSystemHealthChecks.xml	*logdir_argument_location*/logs/healthchecker/OHS_*hostname*-GeneralSystemHealthChecks_*timestamp*.log	/u01/logs/OHS/logs/healthchecker/OHS_*hostname*-GeneralSystemHealthChecks_*timestamp*.html /u01/logs/OHS/logs/healthchecker/OHS_*hostname*-GeneralSystemHealthChecks_*timestamp*.xml
PreDowntimeUpgradeReadinessHealthChecks.xml	*logdir_argument_location*/logs/healthchecker/OHS_*hostname*-PreDowntimeUpgradeReadinessHealthChecks_*timestamp*.log	/u01/logs/OHS/logs/healthchecker/OHS_*hostname*-PreDowntimeUpgradeReadinessHealthChecks_*timestamp*.html /u01/logs/OHS/logs/healthchecker/OHS_*hostname*-PreDowntimeUpgradeReadinessHealthChecks_*timestamp*.xml

5.2 Run the Prevalidation Check on IDM Hosts

Follow the steps in this section only if the environment meets the following criteria:

- Runs on a Linux or Solaris platform
- Supports type 1 and type 2 IDM upgrade scenarios. For more information about these upgrade types, see IDM for FA Upgrade Roadmap.

Otherwise, proceed to Upgrade to Oracle Fusion Applications Release 12 when the upgrade is ready to begin.

5.2.1 Confirm Prerequisite Steps Are Complete

Ensure that the steps in Copy and Unzip idmUpgrade.zip were completed.

5.2.2 Set Environment Variables

The steps for setting the environment variables on each node vary by platform. Refer to one of the following sections that is appropriate for the platform:

- Environment Variables Required for Linux
- Environment Variables Required for Solaris

For more information about IDM environment variables, see About Identity Management Domain, Nodes and Oracle homes.

5.2.2.1 Environment Variables Required for Linux

On Linux, use the following system Perl:

- Perl version 5.8.8 on Oracle Enterprise Linux version 5
- Perl version 5.10.1 on Oracle Enterprise Linux version 6

Set `LD_LIBRARY_PATH`, only if Oracle Identity Management is not installed in the default location of `/u01/IDMTOP`, as shown in the following example:

- On OID and OIM nodes:

```
LD_LIBRARY_PATH=OID_ORACLE_HOME/lib
 export LD_LIBRARY_PATH
```

- On the OHS node:

```
 LD_LIBRARY_PATH=OHS_ORACLE_HOME/lib
 export LD_LIBRARY_PATH
```

5.2.2.2 Environment Variables Required for Solaris

On Solaris, use the perl that is part of the OID or OHS home, which is perl version 5.10.0.

- Set `LD_LIBRARY_PATH`
  - On the OID and OIM nodes:

```
LD_LIBRARY_PATH=OID_ORACLE_HOME/lib
export LD_LIBRARY_PATH
```

  - On the OHS node:

```
 LD_LIBRARY_PATH=OHS_ORACLE_HOME/lib
 export LD_LIBRARY_PATH
```

- Set `PERL5LIB` to the *`ORACLE_HOME`*`/perl` location.
  - On the OID and OIM nodes:

    ```
    PERL5LIB=OID_ORACLE_HOME/perl/lib/site_perl/5.10.0:OID_ORACLE_HOME/perl/lib/
    5.10.0
    export PERL5LIB
    ```

  - On the OHS node:

    ```
    PERL5LIB=OHS_ORACLE_HOME/perl/lib/site_perl/5.10.0:OHS_ORACLE_HOME/perl/lib/
    5.10.0
    export PERL5LIB
    ```

- Set `PATH` to `ORACLE_HOME/perl/bin` to use the 64-bit perl version 5.10.0.
  - On the OID and OIM nodes:

    ```
    PATH=OID_ORACLE_HOME/perl/bin:$PATH
     export PATH
    ```

  - On the OHS node

    ```
    PATH=OHS_ORACLE_HOME/perl/bin:$PATH
     export PATH
    ```

- Set PATH to `/usr/xpg4/bin` to use `awk` for Solaris.
  - On the PRIMORDIAL node:

    ```
    PATH=/usr/xpg4/bin:$PATH
     export PATH
    ```

5.2.3 Run preValidateOnPremise.pl on Each Node

To run the preValidate scripts on all IDM nodes, choose the procedure that applies to your IDM upgrade environment. You can skip this step now and perform it once you get to Upgrade Oracle Identity Management to Release 12.

- If you have a type 1 environment, perform the steps as listed in Run preValidate Script.
- If you have a type 2 environment, perform the steps as listed in Run preValidate Script.

5.2.4 Ensure Free Tablespace for OTBI Schema

Before beginning upgrade from Release 11 (11.1.11) to Release 12 (11.12.x.0.0), ensure that the Oracle Transactional Business Intelligence (OTBI) schema has at least 2GB free space in `FUSION_TS_TOOLS` tablespace. For more information about disk space requirements, see Table 2-2.

6

Upgrade to Oracle Fusion Applications Release 12

This section describes the steps that must be performed to upgrade to Oracle Fusion Applications Release 12 (11.12.x.0.0). The following topics are discussed:

- Perform Pre-Upgrade Steps During Downtime
- Upgrade to Release 12
- Pause Point Steps

6.1 Perform Pre-Upgrade Steps During Downtime

The following steps must be performed before starting the upgrade during downtime:

- Run the LCM Schema Seed Utility to Add LCM Schemas
- Prepare to Register Database Schema Information
- Prepare to Register System User Information
- Direct Upgrade JAZN
- Run OPSS Dup Tool

6.1.1 Run the LCM Schema Seed Utility to Add LCM Schemas

Perform the steps in this section only if the upgrade to Release 12 is from Release 8 or Release 9. Skip this step if your starting point is Release 10. Starting in Release 10, all LifeCycle Management (LCM) operations use LCM schemas instead of SYS schemas. The LCM Schema Seed utility updates the environment so that Release 12 upgrade tasks use LCM users instead of the SYS user.

Before running this utility, check if the environment has Database Vault enabled. If it is enabled, then DVOWNER credentials must be available in the Credential Store Framework (CSF).

To run the utility, perform the following steps :

1. Create a work directory with read and write permissions, referred to as *`WORK_DIR`*.
2. Download and unzip patch 21167623 in *`WORK_DIR`*, which creates the following directories:
    - bin
    - ext/jlib/ext_jlib_jars/fapatchset/techpatch.jar
    - pcu/pcubundle.zip
    - sql
    - config
    - patches (the required patches are located in the following subdirectory)

  - fusionapps/patch/
- rcu (this directory is used for the next step)

3. Download `appsrcu` from the *`REPOSITORY_LOCATION`* to the `rcu` directory created in the previous step.

```
cp REPOSITORY_LOCATION/installers/apps_rcu/linux/rcuHome_fusionapps_linux.zip
WORK_DIR/rcu
cd WORK_DIR/rcu
unzip rcuHome_fusionapps_linux.zip
```

4. Run the `lcmSchemaSeedUtil.sh` utility from the bin directory created in Step 3 as follows:

   This utility assumes that `rcuHome_fusionapps_linux.zip` was unzipped in *`WORK_DIR`*`/rcu` unless a different location using the `-rculoc` parameter is specified.

```
cd WORK_DIR/bin
lcmSchemaSeeding.sh -appbase APPLICATIONS_BASE [-rculoc directory_name]
```

5. Review the log files located in *`APPLICATIONS_CONFIG`*`/lcm/lss_logs`.

LCM Schema Seed Utility for Solaris

The LCM Schema Seed Utility performs the following activities, which are internally orchestrated using the Tech Patch Utility (TPU) framework:

- Applies the required LCM patches using OPatch
- Runs a Password Change Utility (PCU) to seed the credentials for the 6 new schemas in the CSF
- Runs the Repository Creation Utility (RCU) to create the new schemas
- Runs the various SQL grant scripts to configure the new schemas properly

To make the LCM Seed Utility work for Solaris environments, run RCU separately by performing the following steps:

1. Create a work directory with read and write permissions, referred to as *`WORK_DIR`*.
2. Download `apps_rcu_11g` from the *`REPOSITORY_LOCATION`* to the `rcu` directory created in Step 1 as shown in the following example:

```
cp REPOSITORY_LOCATION/installers/apps_rcu_11g/linux/
rcuHome_fusionapps_linux.zip WORK_DIR/rcu
cd WORK_DIR/rcu
unzip rcuHome_fusionapps_linux.zip
```

3. Set `JAVA_HOME` and `PATH` on the Solaris Machine.
4. Download and unzip patch 21189887 into a *`WORK_DIR`* on the Solaris machine and run the *`WORK_DIR`*`/bin/lcmSchemaSeeding.sh` in `preRCU` mode. The Schema Seed Utility will apply the patches, run PCU, and then pause/exit. For example:

```
./lcmSchemaSeeding.sh -appbase <APPTOP> -rculoc <RCU location> -mode preRCU
```

5. Ensure that the `JAVA_HOME` environment variable is set properly on the Linux machine.
6. Extract `rcu` to the Linux Machine as follows:

```
cp REPOSITORY_LOCATION/installers/apps_rcu_11g/linux/
rcuHome_fusionapps_linux.zip WORK_DIR/rcu
```

```
cd WORK_DIR/rcu
unzip rcuHome_fusionapps_linux.zip
```

7. Unzip patch 21189887 into a *WORK_DIR* on the Linux machine and run the *WORK_DIR*/bin/rcuWrapper_solaris.sh script as follows:

   ```
   ./rcuWrapper_solaris.sh -rculoc <RCU location> -jdbcstring <JDBC connect string
   of database> -instancedir <Complete network path of instance dir>
   ```

8. Provide the credentials for the SYS schema and for the following 6 new schemas. These credentials must be retrieved from the CSF:

   ```
   LCM_SUPER_ADMIN
   LCM_USER_ADMIN
   LCM_EXP_ADMIN
   LCM_OBJECT_ADMIN
   DVACCTMGR
   DVOWNER
   ```

9. After creating the schemas, run the lcmSchemaSeeding.sh script in postRCU mode from the Solaris machine as follows:

   ```
   ./lcmSchemaSeeding.sh -appbase <APPTOP> -rculoc <RCU location> -mode postRCU
   ```

6.1.2 Prepare to Register Database Schema Information

To ensure that all database schemas are registered in the credential store, perform the following steps on the primordial host, only once:

1. Create the *PCU_LOCATION*/fusionapps/applications directory. *PCU_LOCATION* is a folder specified as a property in PRIMORDIAL.properties. This location must be within *APPLICATIONS_CONFIG*. For example:

   ```
   APPLICATIONS_CONFIG/lcm/tmp/pcu
   ```

2. Unzip *SHARED_LOCATION*/11.12.x.0.0/Repository/installers/pre_install/pcubundle.zip into *PCU_LOCATION*/fusionapps/applications.

3. Go to the PCU bin directory as follows:

   ```
   cd PCU_LOCATION/fusionapps/applications/lcm/util/bin
   ```

4. Set the JAVA_HOME environment variable before running any commands in this section as follows:

   ```
   setenv JAVA_HOME=java_home_location
   ```

   All commands in this section must be run from *PCU_LOCATION*/fusionapps/applications/lcm/util/bin.

5. Run the templateGen utility to create the csf_template.ini template file as follows:

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

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

   Refer to the following example commands:

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

The `templateGen` utility generates the following template files in the *`PCU_LOCATION`*`/fusionapps/applications/lcm/util/config` directory when the `-codebase` option is used:

- `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.

6. Make a copy of `csf_template.ini` from the *`PCU_LOCATION`*`/fusionapps/applications/lcm/util/config` directory. In this example, the copy is named `csf_plain.ini`.
7. Manually edit `csf_plain.ini` as follows:
   - Set the `master_password` property to the Master Orchestration Password you previously selected.
   - For each line that contains `#text#` or `#password#`, replace `#text#` or `#password#` with the correct value for the 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.
   - Do not replace `#text<WLS.USER>#`,`#password<WLS.PASSWORD>#` as they are used internally by PCU preseeding tools.

   To prevent incorrect results, do not alter `csf_plain.ini` beyond these changes.
8. 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, which 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 master_password | ./lcmcrypt.sh -nonInteractive -encrypt -inputfile
   complete_directory_path/csf_plain.ini
   ```
9. 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 master_password | ./lcmcrypt.sh -nonInteractive -decrypt -inputfile
   complete_directory_path/csf_plain.ini.enc | ./iniGen.sh -nonInteractive -
   templatefile PCU_LOCATION/fusionapps/applications/lcm/util/config/
   csf_template.ini -outputfile PCU_LOCATION/fusionapps/applications/lcm/util/
   config/csf_encrypted.ini -appbase APPLICATIONS_BASE -codebase PCU_LOCATION
   ```

   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.

10. Update the `CSF_ENCRYPTED_FILE` property in *`ORCH_LOCATION`*`/config/`*`POD_NAME`*`/PRIMORDIAL.properties` with the full directory path and file name for *`PCU_LOCATION`*`/fusionapps/applications/lcm/util/config/csf_encrypted.ini`. For more information, see Table 11-2.

Do not use special characters, such as @, _, $, or #, when seeding passwords. The native Repository Creation Utilities (RCUs) for Enterprise Data Quality (EDQ) and Business Intelligence Cloud (BI_CLOUD) do not support creating the schema with special characters. If special characters are used, the password must be enclosed in quotes. However, the native RCUs for EDQ and BI_CLOUD do not support such characters.

On the clean up, the log files are copied from `<staging directory>/fusionapps/applications/lcm/util/logs` to `<normal_mode_log_directory>/preupg_<timestamp>` and the configuration files are copied from `<staging directory>/fusionapps/applications/lcm/util/config` to `<normal_mode_template_directory>/preupg_<timestamp>`. These include the wallets that were also generated in wallet directory `<staging directory>/fusionapps/applications/lcm/util/config`.

For more information about the utilities used in this process, see Password and Certificate Management in the *Oracle Fusion Applications Administrator's Guide*.

6.1.3 Prepare to Register System User Information

Perform this procedure only if the upgrade to Fusion Applications Release 12 is from Release 8 or Release 9. Skip this step if the starting point is Release 10.

To prepare passwords for system users, perform the following steps:

1. Make a copy of `system_user_template.ini` from the *`PCU_LOCATION`*`/fusionapps/applications/lcm/util/config` 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 previously selected.
   - For each line that contains #text# or #password#, replace #text# or #password# with the correct value for the 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.
   - Do not replace `#text<WLS.USER>#`, and `#password<WLS.PASSWORD>#`. They are used internally by the `SchemaPasswordChangeTool`.

   MANDATORY: To prevent incorrect results, do not alter `system_user_plain.ini` beyond these changes.
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, which 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
```

4. Run `iniGen.sh` in non-interactive mode. Running this script also requires a decryption tool to take an encrypted file and a passphrase, and write the decrypted contents into 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 PCU_LOCATION/fusionapps/applications/lcm/util/config/
system_user_template.ini -outputfile PCU_LOCATION/fusionapps/applications/lcm/
util/config/system_user_encrypted.ini -appbase APPLICATIONS_BASE -codebase
PCU_LOCATION
```

   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.

6.1.4 Direct Upgrade JAZN

Before upgrading the Fusion Applications environment from Release 8 to Release 12 or from Release 9 to Release 12 for Jazn patching, perform the following steps during upgrade downtime:

1. Back up the Java Authorization (JAZN) files listed in the following table from `fusionapps` Release 8 or Release 9 instance:

Table 6-1 Jazn Patches

Product	JAZN Path Relative to APPLICATIONS_BASE/fusionapps	Patch Number
HCM	./applications/hcm/security/policies/system-jazn-data.xml	23100321
CRM	./applications/crm/security/policies/system-jazn-data.xml	23345997
FSCM	./applications/fscm/security/policies/system-jazn-data.xml	23100488
FA-BI	./applications/com/acr/security/jazn/bip_jazn-data.xml	23307572

Table 6-1 (Cont.) Jazn Patches

Product	JAZN Path Relative to `APPLICATIONS_BASE/fusionapps`	Patch Number
Applcore	`./atgpf/atgpf/modules/oracle.applcp.centralui_11.1.1/exploded/EssUiApp.ear/META-INF/jazn-data.xml` `./atgpf/atgpf/applications/exploded/FndSetup.ear/META-INF/jazn-data.xml`	23307676 • ATG 11.1.1.7.2 (Release 8) • ATG 11.1.1.7.3 (Release 9)
FSM	`./atgpf/setupEss/jazn-data.xml` `./atgpf/setup/jazn-data.xml`	23322216

2. Download the patches mentioned in Table 6-1 from My Oracle Support (MOS) as follows:
   a. Go to My Oracle Support.
   b. Click **Sign In** and log in using your My Oracle Support login name and password.
   c. Click the **Patches and Updates** tab.
   d. In the **Patch Search** section, select the **Search** tab, and click **Number/Name or Bug Number (Simple)**.
   e. Select the **Patch Name or Number** field and enter the following patch numbers: `23100321`, `23345997`, `23100488`, `23307572`, `23307676`, `23322216`.
   f. Click **Search**.

      The Patch Search Results are displayed.
   g. Click the patch number and then click **Download**. Patches are released for both Release 8 and Release 9, check the version when downloading.
   h. Unzip all the zip files for the Release being upgraded from. There are six zip files for each release. The following example is for Release 8:
      i. Create a folder called **Patch** and download all the patches:

```
Patch
|-- p23100321_111800_Fusion_GENERIC.zip
|-- p23100488_111800_Fusion_GENERIC.zip
|-- p23307572_111800_Fusion_GENERIC.zip
|-- p23307676_111172_Generic.zip
|-- p23322216_111800_Fusion_GENERIC.zip
`-- p23345997_111800_Fusion_GENERIC.zip
```

      ii. Unzip all zip files using `'*.zip'`:

```
Patch/
|-- 23100321
|-- 23100488
|-- 23307572
```

```
|-- 23307676
|-- 23322216
|-- 23345997
|-- p23100321_111800_Fusion_GENERIC.zip
|-- p23100488_111800_Fusion_GENERIC.zip
|-- p23307572_111800_Fusion_GENERIC.zip
|-- p23307676_111172_Generic.zip
|-- p23322216_111800_Fusion_GENERIC.zip
`-- p23345997_111800_Fusion_GENERIC.zip
```

3. Run the following LDAP queries to identify the version for the HCM, CRM, and FSCM stripes:

   - HCM: `ldapsearch -X -h <hostname> -p 3060 -D <admin username> -w <password> -b "cn=hcm,cn=FusionDomain,cn=JPSContext,cn=FAPolicies" -s base "objectclass=*" orclversion`
   - CRM: `ldapsearch -X -h <hostname> -p 3060 -D <admin username> -w <password> -b "cn=crm,cn=FusionDomain,cn=JPSContext,cn=FAPolicies" -s base "objectclass=*" orclversion`
   - FSCM: `ldapsearch -X -h <hostname> -p 3060 -D <admin username> -w <password> -b "cn=fscm,cn=FusionDomain,cn=JPSContext,cn=FAPolicies" -s base "objectclass=*" orclversion`

   Where

   `<hostname>`: Policy store LDAP

   `<admin username>`: Admin username. For example: `cn=orcladmin`

   `<password>`: Admin password

   For each query, there is an output. The following example shows an HCM output:

   ```
   # LDAPv3
   # base<cn=hcm,cn=FusionDomain,cn=JPSContext,cn=FAPolicies> with scope baseObject
   # filter: objectclass=*
   # requesting: orclversion
   #

   # hcm, FusionDomain, JPSContext, FAPolicies
   dn: cn=hcm,cn=FusionDomain,cn=JPSContext,cn=FAPolicies
   orclversion: 11.1.8.0.0
   ```

4. Replace the version field in the jazn xml with the version obtained from the LDAP query for these three patches 23100321 (HCM), 23345997 (CRM), and 23100488 (FSCM) as follows:

   - HCM: `vi ./23100321/23100321_MW/files/hcm/security/policies/system-jazn-data.xml`
   - CRM: `vi ./23345997/crm/security/policies/system-jazn-data.xml`
   - FSCM: `vi ./23100488/fscm/security/policies/system-jazn-data.xml`

   The following example shows how to replace the version field in the JAZN patch for HCM:

   ```
   <policy-store>
    <applications>
     <application locale="en_US" version="fusionapps/hcm/deploy/system-jazn-
   data.xml:20160513010336_23256548.0">
     <name>hcm</name>
     <app-roles>
   ```

Change it as follows:

```
<policy-store>
 <applications>
  <application locale="en_US" version="11.1.8.0.0">
  <name>hcm</name>
  <app-roles>
```

5. Copy the JAZN files from the patch folder to the `fusionapps` instance. The following is an example for Release 8 mentioned in Step 2:

```
cp  ./23322216/setup/jazn-data.xml APPLICATIONS_BASE/fusionapps/atgpf/setup/jazn-
data.xml
cp  ./23322216/setupEss/jazn-data.xml APPLICATIONS_BASE/fusionapps/atgpf/
setupEss/jazn-data.xml
cp  ./23100321/23100321_MW/files/hcm/security/policies/system-jazn-data.xml
APPLICATIONS_BASE/fusionapps/applications/hcm/security/policies/system-jazn-
data.xml
cp  ./23100488/fscm/security/policies/system-jazn-data.xml APPLICATIONS_BASE/
fusionapps/applications/fscm/security/policies/system-jazn-data.xml
cp  ./23307676/files/atgpf/modules/oracle.applcp.centralui_11.1.1/exploded/
EssUiApp.ear/META-INF/jazn-data.xml APPLICATIONS_BASE/fusionapps/atgpf/modules/
oracle.applcp.centralui_11.1.1/exploded/EssUiApp.ear/META-INF/jazn-data.xml
cp  ./23307676/files/atgpf/applications/exploded/FndSetup.ear/META-INF/jazn-
data.xml APPLICATIONS_BASE/fusionapps/atgpf/applications/exploded/FndSetup.ear/
META-INF/jazn-data.xml
cp  ./23345997/crm/security/policies/system-jazn-data.xml APPLICATIONS_BASE/
fusionapps/applications/crm/security/policies/system-jazn-data.xml
cp  ./23307572/com/acr/security/jazn/bip_jazn-data.xml APPLICATIONS_BASE/
fusionapps/applications/com/acr/security/jazn/bip_jazn-data.xml
```

6.1.5 Run OPSS Dup Tool

Run the OPSS dup tool by following the steps listed in *OPSS: How to Delete Duplicate Permission Entries in Fusion Apps Environment (Doc ID 2223825.1)* available on My Oracle Support. To view this document, perform the following steps:

1. Go to My Oracle Support.
2. Click **Sign In** and log in using your My Oracle Support login name and password.
3. Click the **Knowledge** tab.
4. In the **Enter search terms** field, enter “Doc ID 2223825.1”

   The Knowledge Base Search Results are displayed.
5. Click the document's hyperlink to view it.

6.2 Upgrade to Release 12

Perform the following steps to upgrade to Oracle Fusion Applications Release 12 (11.12.x.0.0):

- Update the Database and Middle Tier Credential Stores
- Run Upgrade Orchestrator During Downtime
- Pause Point 1 - Run RUP Lite for OVM in Pre-Root Mode (Oracle VM Only)
- Update Status to Success (Oracle VM Only)
- Resume Upgrade Orchestrator (Oracle VM Only)

- Pause Point 2- Upgrade Oracle Identity Management to Release 12
- Pause Point 3 - Reload Orchestration
- Update Status to Success (Reload Orchestration)
- Resume Upgrade Orchestrator (Reload Orchestration)
- Pause Point 4- 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 5 - Create the Incremental Provisioning Response File
- Update Status to Success (Incremental Provisioning Response File)
- Resume Upgrade Orchestrator (Incremental Provisioning Response File)
- Pause Point 6 - Perform Incremental Provisioning
- Update Status to Success (Incremental Provisioning)
- Resume Upgrade Orchestrator
- Upgrade Orchestrator Completes Successfully
- Clean Up the Middle Tier Credential Store

6.2.1 Update the Database and Middle Tier Credential Stores

Before running RUP Installer, the following pre-upgrade steps must be performed:

- Run Database Credential Store Retrofit Utility in Pods Where EM is Not Present
- Run the CSF Cache Utility Manually in Pods Where EM is Not Present

6.2.1.1 Run Database Credential Store Retrofit Utility in Pods Where EM is Not Present

The Database Credential Store (DBCS) Wallet Retrofit Utility runs on the Fusion Applications (FA) middle tier. As part of the DBCS Wallet Retrofit process, you must extract the credentials for all common users, the TDE wallet password (if any), and the Credential Store Framework (CSF) on the FA middle tier to a temporary wallet file. Then, run CCU on one of the database (DB) hosts in a special mode, which merges the contents of the temporary wallet into the DBCS wallet, creating the DBCS wallet in case it does not already exist. Finally, copy the updated DBCS wallet file to the other DB host.

Run the DBCS Wallet Retrofit Utility on the FA middle tier by performing the following steps:

1. Create the *PCU_LOCATION*/fusionapps/applications directory. *PCU_LOCATION* is a folder specified as a property in PRIMORDIAL.properties. This location must be within *APPLICATIONS_CONFIG*. For example:

   APPLICATIONS_CONFIG/lcm/tmp/pcu

2. Unzip *SHARED_LOCATION*/11.12.x.0.0/Repository/installers/pre_install/pcubundle.zip into *PCU_LOCATION*/fusionapps/applications.

3. Go to the PCU bin directory as follows:

```
cd PCU_LOCATION/fusionapps/applications/lcm/util/bin
```

4. Set the `JAVA_HOME` environment variable before running any commands in this section as follows:

   ```
   setenv JAVA_HOME=java_home_location
   ```

   All commands in this section must be run from *PCU_LOCATION*`/fusionapps/applications/lcm/util/bin`.

5. Create a wallet by looking up the common user credentials from CSF on the FA midtier. The following commands will produce a password-protected wallet at the output wallet location:

   ```
   cd PCU_LOCATION/fusionapps/applications/lcm/util/bin
   echo <wallet-password> | ./csfLookup.sh -appbase APPLICATIONS_BASE -codebase
   PCU_LOCATION -common -schemalist ALL -outputwallet <ouput-wallet-location> -
   ccumerge -loglevel finest
   ```

   Back up the wallet in a location for future archival.

6. Move the wallet onto the DB host RAC node 1 to a certain location, which will be the input wallet location.

7. Download patch 24948508 and explode the patch zip in a stage directory on the DB host. After unzipping, `pcubundle` zip will be located at the following location inside the stage directory:

   ```
   24948508/files/sysman/metadata/swlib/pcu/11.12.0.0.0/upgradeemdp/components/
   pcubundle.zip
   ```

8. Set up PCU in `codebase` mode on the DB host as follows:

   ```
   export ZIP_LOC="<stage-dir>/24948508/files/sysman/metadata/swlib/pcu/11.12.0.0.0/
   upgradeemdp/components/"
   ......
   export APP_BASE="<stage-dir>"
   export CODE_BASE="$APP_BASE/instance/tmp/pcu"
   mkdir -p $CODE_BASE/fusionapps/applications/lcm
   cd $CODE_BASE/fusionapps/applications
   echo "Zip location.. $ZIP_LOC/pcubundle.zip"
   cp $ZIP_LOC/pcubundle.zip $CODE_BASE/fusionapps/applications
   cd $CODE_BASE/fusionapps/applications/lcm
   rm -rf util
   rm -rf credstoreutil
   cd ..
   unzip pcubundle.zip
   cd lcm/util/bin/
   ```

   Replace the values accordingly.

9. Ensure that there are valid entries in the `/etc/oratab` for the respective oracle `uniquename` in the proper format. For example, if the oracle unique name is `fadb` and the oracle home is `/u01/app/oracle/product/11.2.0`, then the valid entry that should exist in `/etc/oratab` is the following:

   ```
   fadb : /u01/app/oracle/product/11.2.0 :
   ```

10. Run the following commands on the DB host:

    ```
    touch <codebase>/fusionapps/applications/lcm/util/config/ORACLE_UNQNAME.pcu
    echo "ORACLE_UNQNAME=<oracle unique name>"
    echo "<oracle unique name>" > <codebase>/fusionapps/applications/lcm/util/config/
    ORACLE_UNQNAME.pcu
    ```

```
export ORACLE_UNQNAME=<oracle unique name>
export PCU_BUNDLE_ZIP="<patch-unzip-location>/24948508/files/sysman/metadata/
swlib/pcu/11.12.0.0.0/upgradeemdp/components/pcubundle.zip"

export CDB_JDBC_CONNECT_STRING="jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)
(ADDRESS=(PROTOCOL=TCP)(HOST=<ip-address>)(PORT=<port>))(ADDRESS=(PROTOCOL=TCP)
(HOST=<ip-address>)(PORT=<port>))(CONNECT_DATA=(SERVER=DEDICATED)
(SERVICE_NAME=<oracle unique name>)))"

cd <codebase>/fusionapps/applications/lcm/util/bin
echo <wallet-password> | ./dbcsUpdate.sh -appbase APPLICATIONS_BASE
 -codebase PCU_LOCATION -inputwallet <input wallet location> -jdbcconnectstring
<jdbc connect string> -loglevel finest
```

Where:

`<oracle unique name>`: The DB unique name of that particular DB.

In the example value for `CDB_JDBC_CONNECT_STRING` shown above, replace the following values:

- `<ip-address>` with the IP address of your Sql*Net listener process
- `<port>` with the port number the Sql*Net listener is using
- `<oracle unique name>` with the unique name for this database (it should match the `db_unique_name` initialization parameter)

Note that the sample value for `CDB_JDBC_CONNECT_STRING` assumes a RAC database. If your database is not RAC, replace the text after "`jdbc:oracle:thin:`" with the appropriate value.

11. The tool will delete the input wallet that is transferred. After the tool is complete, verify the creation of the DBCS wallet by running the following commands:

```
$ORACLE_HOME/bin/mkstore -wrl $ORACLE_HOME/dbs/dbcs/$ORACLE_UNQNAME/wallet -list
$ORACLE_HOME/bin/mkstore -wrl $ORACLE_HOME/dbs/dbcs/$ORACLE_UNQNAME/wallet -
viewEntry SYS
```

Where:

`$ORACLE_HOME/bin/mkstore -wrl $ORACLE_HOME/dbs/dbcs/$ORACLE_UNQNAME/wallet -list` should get more than or equals to 3 entries.

12. Copy the DBCS wallet in RAC node 1 from `$ORACLE_HOME/dbs/dbcs/<oracle unique name>/wallet` to RAC node 2 at `$ORACLE_HOME/dbs/dbcs/<oracle unique name>/wallet`.

Run Utilities*Oracle Fusion Applications Administrator's Guide*

6.2.1.2 Run the CSF Cache Utility Manually in Pods Where EM is Not Present

To run the Credential Store Framework (CSF) cache utility manually, perform the following steps:

1. On the DB host, create master password payload wallet in either one of the following steps:

```
echo <master-password>| ./ walletTool.sh -appbase APPLICATIONS_BASE -codebase
PCU_LOCATION -write -schema MASTER_PASSWORD -outputwallet PCU_LOCATION/MP_WALLET
```

or

```
$ORACLE_HOME/bin/mkstore -wrl <codebase>/MP_WALLET/ -createALO
$ORACLE_HOME/bin/mkstore -wrl <codebase>/MP_WALLET/ -createEntry MASTER_PASSWORD
```

Note that `MASTER_PASSWORD` is not the master password value, but a literal text that should not be changed. The tool will prompt you for the password. Type in the master password twice.

2. On the DB host, generate password protected payload wallet from the DBCS wallet as follows:

```
echo <master-password>| ./dbcslookup.sh -appbase APPLICATIONS_BASE -codebase
PCU_LOCATION -outputwallet PCU_LOCATION/WALLET -schemalist SYS -auto –loglevel
finest
```

3. Move the wallet directories `WALLET` and `MP_WALLET` to the the admin host in a directory called `wallets`. Call the wallets directory `<wallet-dir>`. Note that wallets directory contains `WALLET` and `MP_WALLET` directories. In other words, `WALLET` and `MP_WALLET` are siblings and children to wallets directory as shown in the following example:

```
|
|-------WALLET
|
|-------MP_WALLET
```

4. On the admin host, run the following command to update the CSF entry for SYS:

```
./csfUpdate.sh -appbase APPLICATIONS_BASE -codebase PCU_LOCATION  -schemalist
SYS -inputwallet /fsnadmin/11.12.x.0.0/crmad/wallet -loglevel finest
```

6.2.2 Run Upgrade Orchestrator During Downtime

Review the following steps before starting Upgrade Orchestrator:

- Ensure that the steps in Prepare for the Release 12 Upgrade Before Downtime, Update the Oracle Fusion Applications and Oracle Identity Management Databases, and Run Pre-Downtime Checks have been successfully completed.
- Optionally, perform the mandatory backup of Oracle Fusion Applications at this time. If this is chosen, it is possible to immediately resume orchestration when reaching the pause point for this backup.
- If running on a Solaris platform, set the environment variables that are described in Environment Variables Required for Solaris.

Start Upgrade Orchestrator during downtime by running the following commands on all host types, including the respective scaled out hosts. See Options for the Orchestration Command When Starting Orchestration. The value *POD_NAME*, for the `-pod` argument, refers to the directory created in Unzip Orchestration.zip. The Master Orchestration Password, which was created in Preliminary Steps, is required.

If the DISPLAY variable is set, confirm it is accessible. If the DISPLAY variable is not set, run `unset/unsetenv DISPLAY` before running orchestration.

To run Upgrade Orchestrator, perform the following steps:

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]
```

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]
```

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]
```

4. Run the following command to start orchestration on each IDM host associated with 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]
```

Upgrade Orchestrator runs the tasks listed in the following table:

Table 6-2 Tasks Run During the PreDowntime and DowntimePreFA Phase

Task Name	Phase Name	Task ID	Host Types	Notes
Verify current environment setup	PreDowntime	VerifySetupPlugin	Primordial	NA
Validate Mandatory Orchestration Properties	PreDowntime	PropertyValidationPlugin	All	NA
Validate Host Type	PreDowntime	HostTypeValidatePlugin	All	NA
Validate RUP Lite for OVM Properties	PreDowntime	RupLiteOvmValidatePlugin	All	NA
Register Database Schema Information	PreDowntime	RegisterDBSchemaInfo	Primordial	NA
Validate Oracle Identity Management Setup	PreDowntime	IDMPreValidate	IDM and Configuration	This task may fail. If it fails, ignore the error and proceed.

Table 6-2 (Cont.) Tasks Run During the PreDowntime and DowntimePreFA Phase

Task Name	Phase Name	Task ID	Host Types	Notes
Download Email Template from OIM	PreDowntime	DownloadEmailTemplate	IDM	This task may fail. If it fails, ignore the error and proceed.
Run PreUpgrade Tasks	DowntimePreFA	PreUpgradeTasks	Primordial	NA
Export OWSM Repository	DowntimePreFA	ExportOWSMRepository	Primordial	NA
Back up files in Smart Clone Environment (Oracle VM only)	DowntimePreFA	BackupFilesForSmartClone	Primordial	NA
Disable Index Optimization	DowntimePreFA	DisableIndexOptimization	Primordial	NA
Back Up the OPSS Security Store	DowntimePreFA	Backup OPSS	Primordial	NA
Stop All Servers	DowntimePreFA	StopAllServers	Primordial, Midtier	NA
Set CrashRecoveryEnabled Property to False	DowntimePreFA	DisableCrashRecoveryEnabled	Primordial	NA
Stop OPMN Control Processes	DowntimePreFA	StopOPMNProcesses	Primordial, OHS, Midtier	NA
Stop Node Managers	DowntimePreFA	StopNodeManager	Primordial, Midtier	NA
Stop IIR Server on Midtier host	DowntimePreFA	StopIIRPlugin	Midtier	NA
Uninstall IIR Server (If IIR is configured on primordial or Midtier)	DowntimePreFA	UninstallIIRPlugin	Primordial	NA
Stopping Oracle Identity Management - AUTHOHS	DowntimePreFA	StopOHS	IDM	This task may fail. If it fails, ignore the error and proceed.

Table 6-2 (Cont.) Tasks Run During the PreDowntime and DowntimePreFA Phase

Task Name	Phase Name	Task ID	Host Types	Notes
Stopping Oracle Identity Management - OIM	DowntimePreFA	StopOIM	IDM	This task may fail. If it fails, ignore the error and proceed.
Stopping Oracle Identity Management -OID	DowntimePreFA	StopOID	IDM	This task may fail. If it fails, ignore the error and proceed.

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 resume Orchestrator using the commands specified in this section.

For information about monitoring the progress of the upgrade, see Monitor Upgrade Orchestration Progress.

For information about troubleshooting, see the Monitor and Troubleshoot the Upgrade .

If the orchestration commands result in any hanging tasks on any host, do not use ctrl-C or ctrl-Z to exit. Update the status of the task that is hanging by using the commands in Upgrade Orchestrator Hangs. After exiting and fixing the issue that caused the hanging, restart Upgrade Orchestrator, using the commands specified in this section, on the hosts that were forced to exit.

6.2.3 Pause Point 1 - Run RUP Lite for OVM in Pre-Root Mode (Oracle VM Only)

If Oracle Fusion Applications is *not* running on an Oracle VM environment, proceed to Pause Point 2- Upgrade Oracle Identity Management to Release 12.

If Oracle Fusion Applications is running on an Oracle VM environment, orchestration pauses RUP Lite for OVM can be run in pre-root mode as the root user on the primordial, OHS, Midtier, and IDM hosts. Perform the steps in Run RUP Lite for OVM in Pre-Root Mode (Oracle VM Only).

6.2.4 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` by performing the following steps:

1. Update the task status on the primordial host as follows:

```
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname
host_name -release 11.12.x.0.0 -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 as follows:

```
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype OHS -hostname host_name
-release 11.12.x.0.0 -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 as follows:

```
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype MIDTIER -hostname
host_name -release 11.12.x.0.0 -phase DowntimePreFA -taskid
RupLiteOvmPreRootPausePointPlugin -taskstatus success
```

4. Update the task status on each IDM host that is listed in the 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 11.12.x.0.0 -phase DowntimePreFA -taskid
RupLiteOvmPreRootPausePointPlugin -taskstatus success
```

6.2.5 Resume Upgrade Orchestrator (Oracle VM Only)

Resume orchestration on all host types, including the respective scaled out hosts, using the commands in Run Upgrade Orchestrator During Downtime, Steps 1 through 4.

6.2.6 Pause Point 2- Upgrade Oracle Identity Management to Release 12

For the steps to upgrade Oracle Identity Management (IDM) that are appropriate for your environment, see Upgrade Oracle Identity Management to Release 12.

6.2.7 Pause Point 3 - Reload Orchestration

Orchestration pauses after first RUP installer is completed. No manual step is required.

Recover From CAS Corruption Caused by Out of Memory Error During Attaching CAS Store (Solaris Only)

An out of memory error during attaching CAS store may happen in the first RUP Installer. You can check for these errors in the `APPTOP/fusionapps/applications/cfgtoollogs/opatch/obrepoXXX.log`.

The following errors may be seen:

```
[Jan 21, 2017 12:03:50 PM] [INFO] [OPSR-TIME] Loading CAS libraries
[Jan 21, 2017 12:03:50 PM] [INFO] [OPSR-TIME] CAS library loaded
[Jan 21, 2017 12:03:50 PM] [INFO] [OPSR-TIME] CAS - attaching cas store
[Jan 21, 2017 1:39:07 PM] [INFO] attachMain error: Corrupt master view:
java.lang.OutOfMemoryError: Direct buffer memory
[Jan 21, 2017 1:39:07 PM] [INFO] Stack Description:
oracle.glcm.opatch.content.errors.FileWriteException: Corrupt master view:
java.lang.OutOfMemoryError: Direct buffer memory
```

The errors shown above may corrupt the CAS master view. If these errors are seen, perform the following steps during this Pause Point:

1. Remove the `.cas` directory from the `APPLTOP/fusionapps/applications/` directory.
2. Fix the memory setting in the `oraparam.ini` under `APPLTOP/fusionapps/applications/oui` by updating the memory setting for `JRE_MEMORY_OPTIONS` from `-mx1024m` to `-mx3072m`.
3. Run the following `obrepo attach` command:

   ```
   OH/OPatch/obrepo attach -oh
   <OH location> -jdk <jdk location> -invPtrLoc <inventory pointer location for
   oraInst.loc>
   ```

   For example:

   ```
   APPLTOP/fusionapps/applications/OPatch/obrepo attach -oh
   APPLTOP/fusionapps/applications -jdk /u01/repository/jdk -invPtrLoc /u01/APPLTOP/
   fusionapps/applications/oraInst.loc
   ```

4. Resume with second RUP Installer.

6.2.8 Update Status to Success (Reload Orchestration)

Update the task status to success on all hosts by performing the following steps:

1. Update the task status on the primordial host as follows:

   ```
   (Unix)
   cd ORCH_LOCATION/bin
   ./orchestration.sh updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname
   host_name -release 11.12.x.0.0 -phase DowntimeDuringFA -taskid
   ReloadOrchPausePoint -taskstatus success
   ```

2. Update the task status on each Midtier host that is listed in the `HOSTNAME_MIDTIER` property in the `pod.properties` file as follows:

   ```
   (Unix)
   cd ORCH_LOCATION/bin ./orchestration.sh updateStatus -pod POD_NAME -hosttype
   MIDTIER -hostname host_name -release 11.12.x.0.0 -phase DowntimeDuringFA -taskid
   ReloadOrchPausePoint -taskstatus success
   ```

3. Update the task status on each OHS host that is listed in the `HOSTNAME_OHS` property in the `pod.properties` file as follows:

   ```
   (Unix)
   cd ORCH_LOCATION/bin ./orchestration.sh updateStatus -pod POD_NAME -hosttype OHS
   -hostname host_name -release 11.12.x.0.0 -phase DowntimeDuringFA -taskid
   ReloadOrchPausePoint -taskstatus success
   ```

4. Update the task status on each IDM host that is listed in the following properties in the `pod.properties` file as shown in the following example:

- HOSTNAME_IDMOID
- HOSTNAME_IDMOIM
- HOSTNAME_IDMOHS

```
(Unix)
cd ORCH_LOCATION/bin ./orchestration.sh updateStatus -pod POD_NAME -hosttype IDM
-hostname host_name -release 11.12.x.0.0 -phase DowntimeDuringFA -taskid
ReloadOrchPausePoint -taskstatus success
```

6.2.9 Resume Upgrade Orchestrator (Reload Orchestration)

Resume orchestration on all host types, including the respective scaled out hosts, by performing Steps 1 through 4 as listed in Run Upgrade Orchestrator During Downtime.

Table 6-3 Tasks Run During Various Downtime Phases

Task Name	Phase Name	Task ID	Host Types
Run RUP Lite for Domain Configuration	DowntimeDuringFA Phase	RunRUPLiteForDomainsConfig	Primordial, Midtier
Start Node Managers	DowntimeDuringFA Phase	StartNodeManager	Primordial, Midtier
Start OPMN Control Processes	DowntimeDuringFA Phase	StartOPMNProcesses	Primordial, OHS, Midtier,
Update Topology Information and Worker Details	DowntimeDuringFA Phase	UpdateTopologyInfoPlugin	Primordial, Midtier
Run Oracle Fusion Applications RUP Installation Part 2 of 2	DowntimeDuringFA Phase	RunSecondRUPInstaller	Primordial
Start Remote Workers for Applying Database Patches in Distributed Mode	DowntimeDuringFA Phase	StartRemoteWorkersPlugin	Primordial, Midtier
Clean up Worker Details Information for the Topology	DowntimeDuringFA Phase	CleanupTopologyInfoPlugin	Primordial, Midtier
Run Vital Signs Checks	DowntimePostFA Phase	VitalSignsChecks	Primordial
Prepare for Oracle Fusion Applications Web Tier Upgrade	DowntimePostFA Phase	CopyWebtierUpgradeToCentralLoc	Primordial
Stop Oracle Fusion Applications - APPOHS	DowntimePostFA Phase	StopOPMNProcesses	OHS
Remove Conflicting Patches for Oracle Fusion Applications Web Tier Oracle Homes	DowntimePostFA Phase	RemoveConflictingPatches	OHS
Upgrade Oracle Fusion Applications OHS Binaries	DowntimePostFA Phase	UpgradeOHSBinary	OHS

Table 6-3 (Cont.) Tasks Run During Various Downtime Phases

Task Name	Phase Name	Task ID	Host Types
Upgrade Oracle Fusion Applications OHS Configuration	DowntimePostFA Phase	UpgradeOHSConfig	OHS
Star OPMN Control Processes	DowntimePostFA Phase	StartOPMNProcesses	OHS
Run RUP Lite for BI	DowntimePostFA Phase	RunRUPLiteForBI	Midtier
Run RUP Lite for Domain Configuration in online mode	DowntimePostFA Phase	RunRUPLiteForDomains ConfigOnline	Primordial, Midtier
Run RUP Lite for OVM in Online Mode as Application User	DowntimePostFA Phase	RupLiteOvmOnline	Primordial, OHS, Midtier, IDM

6.2.10 Pause Point 4- Run RUP Lite for OVM in Post-Root Mode (Oracle VM Only)

If Oracle Fusion Applications is *not* running on an Oracle VM environment, proceed to Pause Point 5 - Create the Incremental Provisioning Response File.
If Oracle Fusion Applications is running on an Oracle VM environment, orchestration pauses RUP Lite for OVM can be run in post-root mode as the root user on the primordial, OHS, Midtier, and IDM hosts. Perform the steps listed in Run RUP Lite for OVM in Post-Root Mode (Oracle VM Only) .

6.2.11 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 as follows:

```
cd ORCH_LOCATION/bin
 ./orchestration.sh updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname
host_name -release 11.12.x.0.0 -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 as follows:

```
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype OHS -hostname host_name
-release 11.12.x.0.0 -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 as follows:

```
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype MIDTIER -hostname
host_name -release 11.12.x.0.0 -phase DowntimePostFA -taskid
RupLiteOvmPostRootPausePointPlugin -taskstatus success
```

4. Update the task status on each IDM host that is listed in the 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 11.12.x.0.0 -phase DowntimePostFA -taskid
RupLiteOvmPostRootPausePointPlugin -taskstatus success
```

6.2.12 Resume Upgrade Orchestrator (Oracle VM Only)

Resume orchestration on the Midtier hosts using the command in Run Upgrade Orchestrator During Downtime, Step 2.

Upgrade Orchestrator runs the tasks in the following table:

Table 6-4 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
Run Data Quality Checks	DataQualityChecks	Primordial

6.2.13 Pause Point 5 - Create the Incremental Provisioning Response File

Orchestration pauses if one of the conditions described in Prepare Incremental Provisioning is met, so a response file for running incremental provisioning can be created. Perform the steps in Create an Extended Provisioning Response File in *Oracle Fusion Applications Installation Guide*.

Then, proceed to Update Status to Success (Incremental Provisioning Response File).

6.2.14 Update Status to Success (Incremental Provisioning Response File)

After successfully creating the response file for manual incremental provisioning, update the task status to `success` on the primordial host as follows:

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname
host_name -release 11.12.x.0.0 -phase DowntimePostFA -taskid
CreateIpResponseFilePausePointTask -taskstatus success
```

6.2.15 Resume Upgrade Orchestrator (Incremental Provisioning Response File)

Resume orchestration on the primordial host, using the commands in Run Upgrade Orchestrator During Downtime, Step 1.

6.2.16 Pause Point 6 - Perform Incremental Provisioning

If the `PERFORM_INCREMENTAL_PROVISIONING` property is set to `true` in the pod.properties file, orchestration pauses at this point, so incremental provisioning can be performed manually. Perform the steps listed in Perform Incremental Provisioning in the *Oracle Fusion Applications Installation Guide*.

Perform the following after Incremental Provisioning has been completed adding new provisioning offerings. This is only required if Incremental Provisioning is run, not otherwise:

- Edit `<APPTOP>/instance/fapatch/FUSION_env.properties` on the CommonDomain AdminServer host. The values of the following properties in the file should be edited to specify the host and port of the OID where the OPSS policy store lives:
  - `POLICY_STORE_LDAP_HOSTNAME=<fully qualified OID host name>`
  - `POLICY_STORE_LDAP_PORT=<OID port>`
  - `POLICY_STORE_CONNECT_PROTOCOL_SSL=<Yes/No>`

    Set the value to Yes or No depending on whether the policy store communicates with Fusion Application in secure mode or not.

Note the following:

- This is required to be done only if Incremental Provisioning is run to add new provisioning offerings during upgrade and should be done only after Incremental Provisioning is complete and before `'postUpgradeCleanup'` step of upgrade is run as part of the resumed upgrade flow.
- If the policy store OID host and port is not known, please refer to the response file used to provision the environment initially. The values are found in properties `OAM_OPSS_HOST and OAM_OPSS_PORT` respectively of the response file.

Then, proceed to Update Status to Success (Incremental Provisioning).

If the `PERFORM_INCREMENTAL_PROVISIONING` property is set to false, this pause point does not occur and orchestration continues with the tasks listed in Table 6-5.

6.2.17 Update Status to Success (Incremental Provisioning)

After successfully performing manual incremental provisioning, update the task status to `success` on the primordial, OHS, and Midtier hosts:

1. Update the task status on the primordial host as follows:

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname
host_name -release 11.12.x.0.0 -phase DowntimePostFA -taskid
```

```
RunIncrementalProvisioningManually -taskstatus success
```

2. Update the task status on each Midtier host that is listed in the `HOSTNAME_MIDTIER` property in the pod.properties file as follows:

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype MIDTIER -hostname
host_name -release 11.12.x.0.0 -phase DowntimePostFA -taskid
RunIncrementalProvisioningManually -taskstatus success
```

3. Update the task status on each OHS host that is listed in the `HOSTNAME_OHS` property in the pod.properties file as follows:

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype OHS -hostname host_name
-release 11.12.x.0.0 -phase DowntimePostFA -taskid
RunIncrementalProvisioningManually -taskstatus success
```

6.2.18 Resume Upgrade Orchestrator

Resume orchestration on all host types, including the respective scaled out hosts, using the commands in Run Upgrade Orchestrator During Downtime, Steps 1 through 3.

Upgrade Orchestrator runs the tasks shown in the following table:

Table 6-5 Tasks Run For the Language Pack Upgrade

Task Name	Task ID	Host Types
Run Post Incremental Provisioning Health Checks	PostIPChecks	Primordial, OHS, Midtier
Run Post Upgrade GeneralSystem Health Checks	GeneralSystemChecks	Primordial, OHS, Midtier
Update Topology Information and Worker Details	UpdateTopologyInfoPlugin	Primordial, Midtier
Runs Configuration Actions for all Installed Languages	LanguagePackConfig	Primordial, Midtier
Run Post Language Pack Health Checks	PostLangPackChecks	Primordial
Perform Post Upgrade Configuration	PostUpgradeConfiguration	Primordial
Run Post Upgrade Cleanup Tasks	PostUpgradeCleanup	Primordial

6.2.19 Upgrade Orchestrator Completes Successfully

Upgrade Orchestrator generates the Oracle Fusion Applications Orchestration Report upon successful completion of the upgrade, which is reviewed as a post-upgrade task. To continue with the upgrade after all tasks complete successfully, proceed to Run Post-Upgrade Tasks .

6.2.20 Clean Up the Middle Tier Credential Store

After running RUP Installer, the following post-upgrade step must be performed to clean up the middle tier credential store:

- Run the CSF Cleanup Utility Manually

6.2.20.1 Run the CSF Cleanup Utility Manually

The Credential Store Framework (CSF) Cleanup Utility runs on the Fusion Applications (FA) middle tier and removes all common users from CSF. To run the CSF Cleanup Utility manually, perform the following steps:

1. Go to the following directory on the FA admin host:

   ```
   $CODE_BASE/fusionapps/applications/lcm/util/bin
   ```

2. Run the following command:

   ```
   ./csfClean.sh -appbase <appbase> -codebase <codebase>
   ```

   Where:

   - `-appbase`: The *`APPLICATIONS_BASE`* directory, which is the root directory under which all of the middle tier Fusion Applications (FA) and Fusion Middleware (FMW) code is installed.
   - `-codebase`: The base directory under which the utility code is installed or staged. By default, it is the same as `-appbase`. However, when running any utility on the database (DB) host, `-codebase` must be specified and `-appbase` should not since there is no `APPLICATIONS_BASE` directory on the DB host.

   For more information about the CSF Cleanup Utility, see Run Utilities in the *Oracle Fusion Applications Administrator's Guide*.

6.3 Pause Point Steps

This section describes the detailed steps required only by the following default pause points:

- Upgrade the Oracle Identity Management Domain to Release 12 (11.12.x.0.0)
- Run RUP Lite for OVM in Pre-Root Mode (Oracle VM Only)
- Run RUP Lite for OVM in Post-Root Mode (Oracle VM Only)

6.3.1 Upgrade the Oracle Identity Management Domain to Release 12 (11.12.x.0.0)

Before performing an upgrade to Release 12 (11.12.x.0.0), check the *Oracle Fusion Applications Technical Known Issues - Release 12 (Doc ID 2224140.1)* for the latest information on required patches.

Perform the following steps to manually upgrade the Oracle Identity Management domain to Release 12 (11.12.x.0.0):

- Perform Preinstallation and Upgrade Tasks

For more information about the Oracle Identity Management domain, see Overview of Upgrade Patches and About Identity Management Domain, Nodes and Oracle homes.

6.3.1.1 Overview of Upgrade Patches

Oracle Identity Management for Oracle Fusion Applications 11*g*, Release 12 (11.12.x.0.0) includes patches for the following products that are installed in the Oracle Identity Management domain:

- Oracle IDM Tools
- Oracle Access Manager
- Oracle WebGate
- Oracle Internet Directory

The Oracle Fusion Applications Release 12 Identity Management software and patches for the appropriate platform are available in the Oracle Fusion Applications repository under *SHARED_LOCATION*/11.12.x.0.0/Repository/installers. Review the individual patch Readme files before applying them.

6.3.1.2 About Identity Management Domain, Nodes and Oracle homes

This section describes the nodes and Oracle homes in the Identity Management domain for Oracle Fusion Applications 11*g* Release 12 (11.12.x.0.0).

- **Identity Management (IDM) Node**
  - *WEBLOGIC_ORACLE_HOME*: (For IDM provisioned environments, this is *IDM_BASE*/products/dir/wlserver_10.3):
    - Oracle WebLogic Server
  - *IDM_ORACLE_HOME*: This is also known as the *OID_ORACLE_HOME*. (For IDM provisioned environments, this is *IDM_BASE*/products/dir/oid). 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*: (For IDM provisioned environments, this is *IDM_BASE*/products/dir/oracle_common). The following Oracle Identity Management products are installed in this Oracle home:
    - Oracle Platform Security Services (OPSS)
    - Oracle Web Services Manager (OWSM)
- **Database Node**
  - *RDBMS_ORACLE_HOME*: This is the *ORACLE_HOME* of the Oracle Database. Apply mandatory database patches to this Oracle home.

6.3.1.3 Perform Preinstallation and Upgrade Tasks

Perform the following tasks to upgrade Oracle Identity Management:

- Verify Prerequisites

- Stop the Servers and Processes
- Create Backups
- Patch the Database (RDBMS_ORACLE_HOME)
- Patch the Database Clients

6.3.1.3.1 Verify Prerequisites

Ensure that the environment meets the following requirements before installing or uninstalling the patch:

- 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 the 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`

For more information about OPatch, see the Patching Oracle Fusion Middleware with Oracle OPatch section in the *Oracle Fusion Middleware Patching Guide*.

6.3.1.3.2 Stop the Servers and Processes

To stop the servers and processes, perform the following steps:

- In the Oracle Identity Management domain, stop all Oracle Identity Management services and processes using the following sequence. Do not stop the database:

  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

For more information about specific commands for stopping components, see Stop and Start Identity Management Related Servers.

6.3.1.3.3 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
- The database

  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$`.
- The Configurations and Stores—specifically, all data under the root node of the LDAP store
- Any Oracle Identity Federation Java Server Pages (JSP) that was customized

  The patching process overwrites JSPs included in the `oif.ear` file. After completing the patching process, restore the custom JSPs.

In addition to the preceding backups, Oracle recommends performing your organization's typical backup processes.

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.

6.3.1.3.4 Patch the Database Clients

The Database Client patches are available under the *`SHARED_LOCATION`*`/11.12.x.0.0/Repository/installers/dbclient/patch` directory. Follow the patch `Readme` and apply all patches in the directory. To apply all patches, proceed as follows:

1. Set the Oracle home to *`RDBMS_ORACLE_HOME`*, for example, `ORACLE_HOME/u01/oid/oid_home`.
2. Go to the patch directory as follows:

   ```
   cd SHARED_LOCATION/11.12.x.0.0/Repository/installers/dbclient/patch
   ```
3. Run `opatch` using the `napply` option.

6.3.1.3.5 Patch the Database (RDBMS_ORACLE_HOME)

Ensure the patches listed in Update 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.

To apply the patches, follow the steps listed in Update the Oracle Fusion Applications and Oracle Identity Management Databases.

6.3.2 Run RUP Lite for OVM in Pre-Root Mode (Oracle VM Only)

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 12 `rupliteovm/metadata` directory that was set up as part of the pre-upgrade preparation in Prepare RUP Lite for OVM . Run this command as super user (root) as follows:

```
setenv JAVA_HOME java_home_directory
cd /u01/lcm/rupliteovm
bin/ruplite.sh pre-root -i ORCH_LOCATION/config/POD_NAME/11.12.x.0.0/rupliteovm/
metadata
```

Then, proceed to Update Status to Success (Oracle VM Only).

6.3.3 Run RUP Lite for OVM in Post-Root Mode (Oracle VM Only)

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 12 `rupliteovm/metadata` directory that was set up as part of the pre-upgrade preparation in Prepare RUP Lite for OVM . Run this command as super user (root) as follows:

```
setenv JAVA_HOME java_home_directory
cd /u01/lcm/rupliteovm
bin/ruplite.sh post-root -I ORCH_LOCATION/config/POD_NAME/11.12.x.0.0/rupliteovm/
metadata
```

7

Upgrade Oracle Identity Management to Release 12

This chapter describes how to upgrade your existing Oracle Identity Manager (IDM) environment for Oracle Fusion Applications to Release 12 (11.12.x.0.0). Perform the steps in this chapter after you have completed Resume Upgrade Orchestrator (Oracle VM Only).

This chapter contains the following sections:

- Pre-Upgrade Requirements
- IDM for FA Upgrade Roadmap
- Identify your IDM Topology
- Disconnect Enterprise IDM Integrations
- Upgrade Type I IDM Environments
- Upgrade Type II IDM Environments
- Reconnect Enterprise IDM Integrations
- Update Status to Success
- Resume Upgrade Orchestrator to Upgrade Oracle Fusion Applications
- IDM for FA Upgrade Properties Files
- IDM Upgrade and Migration Log Files Location

7.1 Pre-Upgrade Requirements

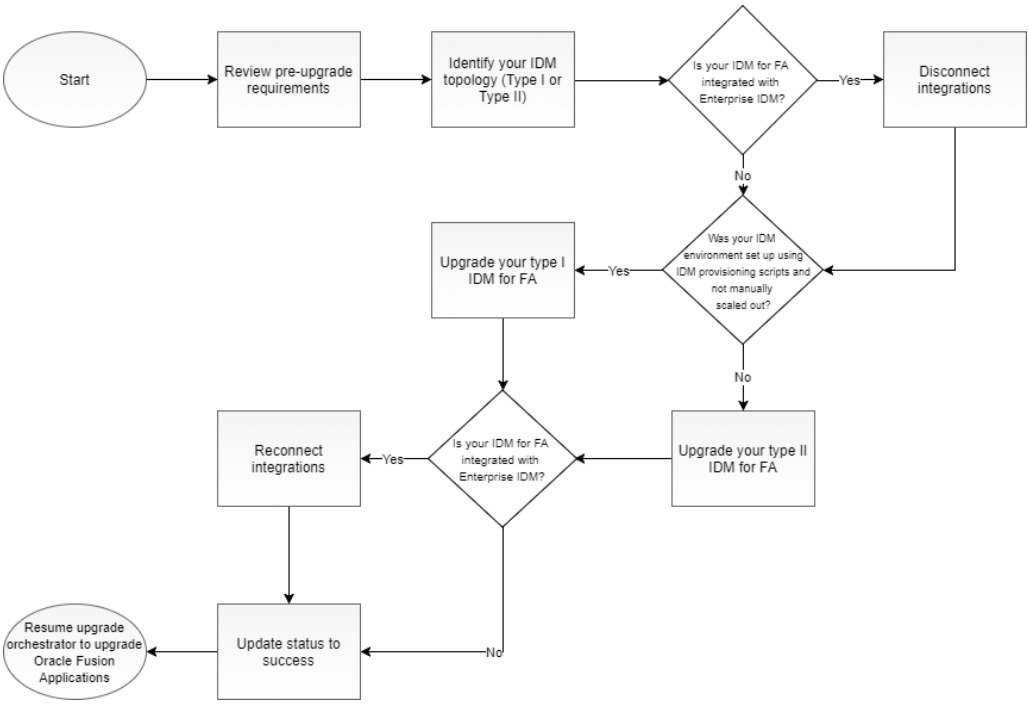
Before you begin the upgrade of your IDM environment for Oracle Fusion Applications (FA) to Release 12, ensure you have completed the tasks as listed in:

- Pre-Upgrade Tasks for IDM for FA Upgrade to Release 12
- Prepare for Upgrade

7.2 IDM for FA Upgrade Roadmap

Review the following flowchart and roadmap for an overview of the upgrade process for IDM for FA to Release 12.

Figure 7-1 Upgrade Process Flowchart for IDM for FA



The following table lists the high-level steps that you need to perform to upgrade to Oracle Fusion Applications Release 11.12.x.0.0:

Table 7-1 Tasks for Upgrading IDM for FA to Release 12

Task	Required	Description
Review pre-upgrade requirements	Required	The pre-upgrade requirements include having your Oracle Fusion Applications IDM on Release 8 or 9 and backing up the IDM middle tier and database. See Pre-Upgrade Requirements.
Identify your IDM topology	Required	Identify your IDM topology to choose the right upgrade procedure for your system. See Identify your IDM Topology.
Disconnect Enterprise IDM integrations	Required only if your IDM for FA is integrated with Enterprise IDM	If your IDM for FA is integrated with Enterprise IDM, you must disconnect integrations. See Disconnect Enterprise IDM Integrations.

Table 7-1 (Cont.) Tasks for Upgrading IDM for FA to Release 12

Task	Required	Description
Upgrade your type I IDM for FA	Required only if your IDM environment was set up using IDM provisioning scripts	After reviewing the requirements and confirming that you have the Type I IDM topology, run the upgrade steps. For the complete procedure, see Upgrade Type I IDM Environments.
Upgrade your type II IDM for FA	Required only if your IDM environment was not set up using IDM provisioning scripts	After reviewing the requirements and confirming that you have the Type II IDM topology, run the upgrade steps. For the complete procedure, see Upgrade Type II IDM Environments.
Reconnect Enterprise IDM integrations	Required only if your IDM for FA is integrated with Enterprise IDM	If your IDM for FA is integrated with Enterprise IDM and you disconnected integrations, you can now reconnect them. See Reconnect Enterprise IDM Integrations.
Update Status to Success	Required	After successfully upgrading your IDM, update the task status to “success” on the IDM host. See Update Status to Success.
Resume Upgrade Orchestrator to Upgrade Oracle Fusion Applications	Required	The IDM for FA upgrade process to Release 12 is complete. You can now resume Upgrade Orchestrator and continue with Pause Point 3. See Resume Upgrade Orchestrator to Upgrade Oracle Fusion Applications.

7.3 Identify your IDM Topology

The upgrade steps will vary according to the type of IDM installation you have.

Your topology will be one of the following:

- **Type I**: IDM installation that was performed using IDM provisioning scripts without any subsequent manual scale out steps
- **Type II**: IDM installation that was not performed using IDM provisioning scripts. This type also includes cases where a single node or EDG option was selected during your IDM provisioning and manual scale out was performed for second instances

If you are not sure about which type of IDM installation you have, verify if the `lcmconfig` folder exists under the shared configuration folder. For example:

```
<SHARED_CONFIG>/lcmconfig/topology/topology.xml
```

Where

- `<SHARED_CONFIG>`: `/u01/IDMTOP/config`

This folder is specific to the type I environment or provisioned using IDM provisioning scripts without any subsequent manual IDM scale out steps.

7.4 Disconnect Enterprise IDM Integrations

Perform this steps only if your IDM for FA is integrated with Enterprise IDM. You must disconnect integrations by cloning your IDM environment. The cloning process involves the following high-level steps:

Note that in this section, the original environment is called IDM1, and the cloned environment is called IDM2.

1. Clone the IDM1 environment using the clone tool.
2. Perform sanity testing to ensure IDM2 is working correctly.
3. Rewire FA to point to IDM2.
4. Perform sanity testing to ensure FA is working correctly.
5. Upgrade IDM1 to a supported version.

To set up your cloned environment, perform the following steps:

1. Clone your IDM environment by following the steps as listed in Cloning Procedure in the *Oracle Fusion Applications Cloning and Content Movement Administrator's Guide*.
2. Perform sanity tests on IDM2 to ensure it is working correctly by following the steps as listed in Perform Validation Steps in the *Oracle Fusion Applications Cloning and Content Movement Administrator's Guide*.
3. Rewire FA to point to IDM2 as follows:
   a. To have FA point to the IDM2, IDM specific entries in the `/etc/hosts` should now point to IDM2. FA interactions with IDM is controlled by entries in the `/etc/hosts` file of the FA machines. The following is an example file:

      ```
      192.0.2.1 hostname.example.com hostname
      192.0.2.1 idmhost1.osc.uk.example.com idmhost1
      192.0.2.1 fahost1.osc.uk.example.com fahost1
      192.0.2.1 scmhost1.osc.uk.example.com scmhost1
      192.0.2.1 policystore.osc.uk.example.com policystore
      192.0.2.1 idstore.osc.uk.example.com idstore
      ```

   b. Update your FA OHS configuration. OHS configuration contains information about URL redirects, for example, `sso.example.com`. This configuration needs to be updated to point to the new IP addresses of IDM2 instead of the existing IP of IDM1.
4. Perform sanity tests to ensure FA is working correctly.

7.5 Upgrade Type I IDM Environments

This section describes how to upgrade type I IDM environments.

This section contains the following topics:

- Prerequisites for Upgrading Type I IDM Environments
- Run preValidate Script
- Manually Download OIM Email Template
- Stop All IDM Services
- Upgrade Binaries
- Update IDM Configuration
- Run postValidate Script

Note the following:

- All of the perl files mentioned in the following sections are present under `SHARED_LOCATION/idmUpgrade`.
- All of the steps must be executed serially.

7.5.1 Prerequisites for Upgrading Type I IDM Environments

Before the upgrade of your type I IDM environment, perform the following tasks:

- Obtain `SHARED_LOCATION/11.12.x.0.0/idmUpgrade` as follows:
  1. Unzip the patch 25734394 that you downloaded in Copy and Unzip idmUpgrade.zip into the machine that contains the IDM nodes.
  2. Update the `upgradeOnPremise.properties` file in the unzipped location, then modify the default values as applicable and provide values for all properties listed in the file. For more information about these properties, see IDM for FA Upgrade Properties Files.

     > **Note:**
     >
     > Use the updated `upgradeOnPremise.properties` for all type I upgrade commands.

- Create the RCU folder as follows:
  1. Create the `rcu` folder under `FA_REPOSITORY/installers`.
  2. Unzip the contents of `<FA_REPOSITORY>/installers/fmw_rcu/linux/rcuHome.zip` into the `rcu` folder.
  3. Give 755 permissions to the `rcu` folder recursively:

     ```
     chmod -R 755 rcu
     ```

Note that in the following sections, operations will be executed on all the IDM nodes. You must perform the operations in the following order, except when stopping all IDM services:

- OID and OID scaled out (if present)
- OIM and OIM scaled out (if present)
- OHS and OHS scaled out (if present)

7.5.2 Run preValidate Script

The following `preValidateOnPremise.pl` script must be executed serially on each IDM node, including the scaled out nodes:

```
perl preValidateOnPremise.pl <node type> REPOSITORY_LOCATION/
installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches upgradeOnPremise.properties
```

Where

- *REPOSITORY_LOCATION*: Fusion Applications Release 12 repository.

Run the `preValidateOnPremise` command in the following order:

- OID

  ```
  perl preValidateOnPremise.pl OID REPOSITORY_LOCATION/installers,SHARED_LOCATION/
  11.12.x.0.0_post_repo_patches upgradeOnPremise.properties
  ```

  If the environment is scaled out, run the following command on the OID scaled out node:

  ```
  perl preValidateOnPremise.pl OID-SO REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches
  upgradeOnPremise.properties
  ```

- OIM

  ```
  perl preValidateOnPremise.pl OIM REPOSITORY_LOCATION/installers,SHARED_LOCATION/
  11.12.x.0.0_post_repo_patches upgradeOnPremise.properties
  ```

  If the environment is scaled out, run the following command on the OIM scaled out node:

  ```
  perl preValidateOnPremise.pl OIM-SO REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches
  upgradeOnPremise.properties
  ```

- OHS

  ```
  perl preValidateOnPremise.pl OHS REPOSITORY_LOCATION/installers,SHARED_LOCATION/
  11.12.x.0.0_post_repo_patches upgradeOnPremise.properties
  ```

  If the environment is scaled out, run the following command on the OHS scaled out node:

  ```
  perl preValidateOnPremise.pl OHS-SO REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches
  upgradeOnPremise.properties
  ```

Confirm that the status message at the end of the run is successful on each node. If the script gives an error, check the error message and resolve the issue. Rerun `preValidate` and ensure it is successful.

7.5.3 Manually Download OIM Email Template

After running the `preValidate` script on your type I environment, manually download the OIM email template as follows:

1. Log in to the OIM host.

2. Go to the `idmUpgrade` unzip location.
3. Execute `exportOIMDataOnPremise.pl` as follows:

   ```
   perl exportOIMDataOnPremise.pl upgradeOnPremise.properties
   <SHARED_UPGRADE_LOCATION>/<podName>/emailTemplateDir/emailtemplate.xml
   ```

   Where

   - `SHARED_UPGRADE_LOCATION`: It is located in `pod.properties`, and its default value is `/u01/sharedupgradelocation`.
4. Confirm that the status message at the end of the run is successful. If the script gives an error, check the error message and resolve the issue. Then, rerun `exportOIMDataOnPremise.pl` and ensure it is successful.

7.5.4 Stop All IDM Services

Stop all IDM services by running the following command on all IDM nodes:

```
perl stopIDMOnPremise.pl <node type> upgradeOnPremise.properties
```

Run the `stopIDMOnPremise.pl` command in the following order:

- OHS

  If the environment is scaled out, run the following command on the OHS scaled out node:

  ```
  perl stopIDMOnPremise.pl OHS-SO upgradeOnPremise.properties
  ```

  If the environment is not scaled out, run the following command on the OHS node:

  ```
  perl stopIDMOnPremise.pl OHS upgradeOnPremise.properties
  ```

- OIM

  If the environment is scaled out, run the following command on the OIM scaled out node:

  ```
  perl stopIDMOnPremise.pl OIM-SO upgradeOnPremise.properties
  ```

  If the environment is not scaled out, run the following command on the OIM node:

  ```
  perl stopIDMOnPremise.pl OIM upgradeOnPremise.properties
  ```

- OID

  If the environment is scaled out, run the following command on the OID scaled out node:

  ```
  perl stopIDMOnPremise.pl OID-SO upgradeOnPremise.properties
  ```

  If the environment is not scaled out, run the following command on the OID node:

  ```
  perl stopIDMOnPremise.pl OID upgradeOnPremise.properties
  ```

7.5.5 Upgrade Binaries

Upgrade the binary files used by IDM components by running the following command on all IDM nodes:

```
perl idmUpgradeOnPremise.pl -node=<node type> -repoLocs=REPOSITORY_LOCATION/
installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=./
upgradeOnPremise.properties -mode=binary
```

Where

- *REPOSITORY_LOCATION*: Fusion Applications Release 12 repository.

Run the `idmUpgradeOnPremise.pl` command in the following order:

- OID

  ```
  perl idmUpgradeOnPremise.pl -node=OID -repoLocs=REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=./
  upgradeOnPremise.properties -mode=binary
  ```

  If the environment is scaled out, run the following command on the OID scaled out node:

  ```
  perl idmUpgradeOnPremise.pl -node=OID-SO -repoLocs=REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=./
  upgradeOnPremise.properties -mode=binary
  ```

- OIM

  ```
  perl idmUpgradeOnPremise.pl -node=OIM -repoLocs=REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=./
  upgradeOnPremise.properties -mode=binary
  ```

  If the environment is scaled out, run the following command on the OIM scaled out node:

  ```
  perl idmUpgradeOnPremise.pl -node=OIM-SO -repoLocs=REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=./
  upgradeOnPremise.properties -mode=binary
  ```

- OHS

  ```
  perl idmUpgradeOnPremise.pl -node=OHS -repoLocs=REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=./
  upgradeOnPremise.properties -mode=binary
  ```

  If the environment is scaled out, run the following command on the OHS scaled out node:

  ```
  perl idmUpgradeOnPremise.pl -node=OHS-SO -repoLocs=REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=./
  upgradeOnPremise.properties -mode=binary
  ```

7.5.6 Update IDM Configuration

Update the IDM configuration to Release 12 level by running the following `config` upgrade commands on all IDM nodes:

```
perl idmUpgradeOnPremise.pl -node=<node type> -repoLocs=REPOSITORY_LOCATION/
installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=./
upgradeOnPremise.properties -mode=config
```

Where:

- *REPOSITORY_LOCATION*: Fusion Applications Release 12 repository.

Run the `idmUpgradeOnPremise.pl` command in the following order:

- OID

  ```
  perl idmUpgradeOnPremise.pl -node=OID -repoLocs=REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=./
  upgradeOnPremise.properties -mode=config
  ```

  If the environment is scaled out, run the following command on the OID scaled out node:

  ```
  perl idmUpgradeOnPremise.pl -node=OID-SO -repoLocs=REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=./
  upgradeOnPremise.properties -mode=config
  ```

- OIM

  ```
  perl idmUpgradeOnPremise.pl -node=OIM -repoLocs=REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=./
  upgradeOnPremise.properties -mode=config
  ```

  If the environment is scaled out, run the following command on the OIM scaled out node:

  ```
  perl idmUpgradeOnPremise.pl -node=OIM-SO -repoLocs=REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=./
  upgradeOnPremise.properties -mode=config
  ```

  If you are on a Solaris platform, after running this command on OIM perform the steps listed in Re-create IDM Schemas Manually (Solaris Only).

- OHS

  ```
  perl idmUpgradeOnPremise.pl -node=OHS -repoLocs=REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=./
  upgradeOnPremise.properties -mode=config
  ```

  If the environment is scaled out, run the following command on the OHS scaled out node:

  ```
  perl idmUpgradeOnPremise.pl -node=OHS-SO -repoLocs=REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=./
  upgradeOnPremise.properties -mode=config
  ```

7.5.6.1 Re-create IDM Schemas Manually (Solaris Only)

During IDM upgrade on Solaris platforms, the OIM Config step displays the following message in the IDM upgrade console:

```
On non-Linux platforms, run the rcu from a Linux machine.
Please follow the manual steps documented in the IDM Upgrade Guide to load the
required schemas and resume Upgrade.
```

Re-create the schemas and resume the upgrade as follows:

1. Unzip the following Oracle Fusion Middleware RCU zip file to *REPOSITORY_LOCATION*/installers/rcu:

   - Linux:

     REPOSITORY_LOCATION/installers/fmw_rcu/linux/rcuHome.zip

   - Windows:

     REPOSITORY_LOCATION/installers/fmw_rcu/windows/rcuHome.zip

Where:

- *REPOSITORY_LOCATION*: The Oracle Fusion Applications provisioning repository.

Use the Oracle Identity Management version of RCU, which now exists in that directory.

2. Drop the FA_OAM schema, and then manually create the FA_OAM, FA_OPSS, and FA_BIPLATFORM schemas in the Oracle Identity Management database by using the Fusion Applications Repository Creation Utility (RCU) *REPOSITORY_LOCATION*/installers/rcu, for example, IDMDB. Note that the schema prefix may vary from "*FA_*"
3. Export the following Solaris specific environment variables:
   - LD_LIBRARY_PATH
   - PERL5LIB
   - PATH

   For more information about exporting these Solaris variables, see Environment Variables Required for Solaris.
4. Add a checkpoint for schema creation by running the *IDM_UPGRADE_HOME*/addSchemaCheckPoint.pl script as shown in the following example:

   ```
   perl addSchemaCheckPoint.pl -node=OIM -repoLocs=REPOSITORY_LOCATION/installers -
   props= ./upgradeOnPremise.properties
   ```

   Where:

   - node: Node
   - repoLocs: Comma separated paths of repo
   - props: Properties files
5. Rerun OIM config upgrade mode.

7.5.7 Run postValidate Script

To confirm that the upgrade was successful, run the following post-upgrade validation command on all IDM nodes:

```
perl postvalidateOnPremise.pl <node type> upgradeOnPremise.properties
```

Run the idmUpgradeOnPremise.pl command in the following order:

- OID

  ```
  perl postvalidateOnPremise.pl OID upgradeOnPremise.properties
  ```

  If the environment is scaled out, run the following command on the OID scaled out node:

  ```
  perl postvalidateOnPremise.pl OID-SO upgradeOnPremise.properties
  ```
- OIM

  ```
  perl postvalidateOnPremise.pl OIM upgradeOnPremise.properties
  ```

  If the environment is scaled out, run the following command on the OIM scaled out node:

```
perl postvalidateOnPremise.pl OIM-SO upgradeOnPremise.properties
```

- OHS

  ```
  perl postvalidateOnPremise.pl OHS upgradeOnPremise.properties
  ```

  If the environment is scaled out, run the following command on the OHS scaled out node:

  ```
  perl postvalidateOnPremise.pl OHS-SO upgradeOnPremise.properties
  ```

Confirm that the status message at the end of the run is successful on each node. If the script gives an error, check the error message and resolve the issue.

After upgrade, you can start/stop the IDM components on a given node using the IDM provisioning start/stop scripts as described in Start and Stop All IDM Components on a Host.

7.6 Upgrade Type II IDM Environments

This section describes the upgrade process for the type II IDM environments that have been installed using Oracle's A-team's one click installation scripts or by following the instructions in Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management.

This upgrade process reuses the database from the old environment and creates an entirely new parallel IDM environment, and involves the following high-level steps:

1. Run the Discovery Tool to discover your environment topology and configuration.
2. Set up a parallel True-up IDM environment matching the release of the current environment.
3. Migrate the configuration and artifacts from the existing environment.
4. Upgrade the true-up environment.

> **Note:**
>
> Do not clean the source environment until after the entire upgrade of the true-up environment is completed.

This section contains the following topics:

- Prerequisites for Upgrading Type II IDM Environments
- Discover Topology
- Set Up True-Up Environment
- Perform Migration Tasks
- Verify True-Up Environment Is Up
- Run preValidate Script
- Manually Download OIM Email Template
- Stop All IDM Services
- Upgrade Binaries

- Update IDM Configuration
- Run postValidate Script

Note the following:

- All of the perl files mentioned in the following sections are present under `SHARED_LOCATION/idmUpgrade`.
- All of the steps must be executed serially.

7.6.1 Prerequisites for Upgrading Type II IDM Environments

Before the upgrade of your type II IDM environment, perform the following tasks:

- Ensure that the user running the upgrade is the same user used for the installation of the IDM home. This user must have read/write access to the staging directories throughout the upgrade cycle.
- Create `stagedir` folder under `SHARED_LOCATION`. `stagedir` is the directory in the `SHARED_LOCATION` that contains the artifacts generated by the Discovery tool.
- Confirm that you have permission on `stagedir` and that it is shared across all IDM hosts.
- Verify that Webgate is configured on the OHS SO Node. If it is not configured, follow the steps as listed in Webgate Is Not configured on the OHS SO Node.
- Choose the patch applicable to your starting release and environment. The following table shows the patch number for each release/environment:

Table 7-2 FA IDM Patches for Type II Upgrades

Release	Environment	Patch Number
Release 8	Linux non-provisioned environment	26504255
Release 8	Sparc non-provisioned environment	26504255
Release 9	Linux non-provisioned environment	26639496
Release 9	Sparc non-provisioned environment	26639496

- Obtain the `SHARED_LOCATION/11.12.x.0.0/idmUpgrade` file as follows:
  1. Unzip the patch 25734394 that you downloaded in Copy and Unzip idmUpgrade.zip into a location under `SHARED_LOCATION//11.12.x.0.0`.
- Ensure that an empty staging directory is available for the upgrade process and that it meets the following requirements:
  - The directory must be writable and have at least 100MB empty space.
  - If the environment is spread across multiple machines, then the staging directory needs to be on a network shared and write-accessible from all IDM nodes.
- Unzip the `idmUpgrade.zip` file parallel to `stagedir` in the `SHARED_DIR` directory.
- Ensure that the following directories are created and empty on all IDM nodes:

  - `/u01/IDMTOP`: Both `IDMTOP` and `stagedir` must be shared across the OID and the OIM hosts, including SO hosts. The only exception is for the OHS hosts when they are in DMZ.
  - `/u02/local/IDMTOP`: Local folder on each of the IDM hosts.
- Ensure the `u01` and `u02` folders are created under root (`"/"`) with the same user and group that the existing IDM environment has.
- Create the RCU folder as follows:
  1. Create the `rcu` folder under `FA_REPOSITORY/installers`.
  2. Unzip the contents of `<FA_REPOSITORY>/installers/fmw_rcu/linux/rcuHome.zip` into the `rcu` folder.
  3. Give 755 permissions to the `rcu` folder recursively:

     ```
     chmod -R 755 rcu
     ```

Note that in the following sections, operations will be executed on all the IDM nodes. You must perform the operations in the following order, except when running discovery and stopping all IDM services:

- OID and OID scaled out (if present)
- OIM and OIM scaled out (if present)
- OHS and OHS scaled out (if present)

7.6.2 Discover Topology

The topology discovery tool introspects the existing IDM environment to discover information that will be needed for setting up a parallel true-up environment.

Discovery also generates the following artifacts based on the existing environment to stage directory (`stagedir`). These artifacts are used during the migration and upgrade processes. No additional input is necessary:

- `credconfig`: Folder that contains the discovery wallet
- `upgradeProps`: Folder that contains the upgrade wallet
- `idmMigration`: Folder that contains the migration wallet
- `discoverycache`: Folder that contains a list of the files required for migration
- `upgradeOnPremise.properties`: File that contains auto-generated properties required for the On-Premise upgrade. There are 2 properties that you can customize, `OPSS_DB_PASSWORD` and `OIF_11GR2_SINGNING_KEY_PWD` as they are new passwords. For more information about this file, see IDM for FA Upgrade Properties Files.
- `topology.xml`: File that contains information about the IDM topology such as server hosts, ports, `mw_homes`, `oracle_homes`, etc. related to source environment.
- `dest-topology.xml`: File that contains information about the IDM topology such as server hosts, ports, `mw_homes`, `oracle_homes` etc. related to destination true-up tar.
- `logs`: Folder that contains logs of the discovery tool. By default, the migration and the upgrade logs are pointed to the same location.
- `idmMigration.properties`: File that contains the properties required for the On-Premise migration. There are certain optional parameters that you can customize in this auto-generated file, such as `LOG_DIR`.

This section contains the following topics:

- Prerequisites
- Run the Discovery Tool

7.6.2.1 Prerequisites

Before running the discovery tool, perform the following steps. Note that if your environment has OIF and it is not up during discovery, then OIF will not be part of the upgrade process.

1. Set the following environment variables:
   - `JAVA_HOME` to a valid JDK6 install in all IDM hosts.
   - `MW_HOME` on the Admin Server machine to a Middleware Home location, for example, `/u01/oracle/products/app`.
2. Ensure all IDM servers are up and running. If any of the servers is not running, the discovery fails and the next step of migration cannot be run.

Discovery must be executed in the following order:

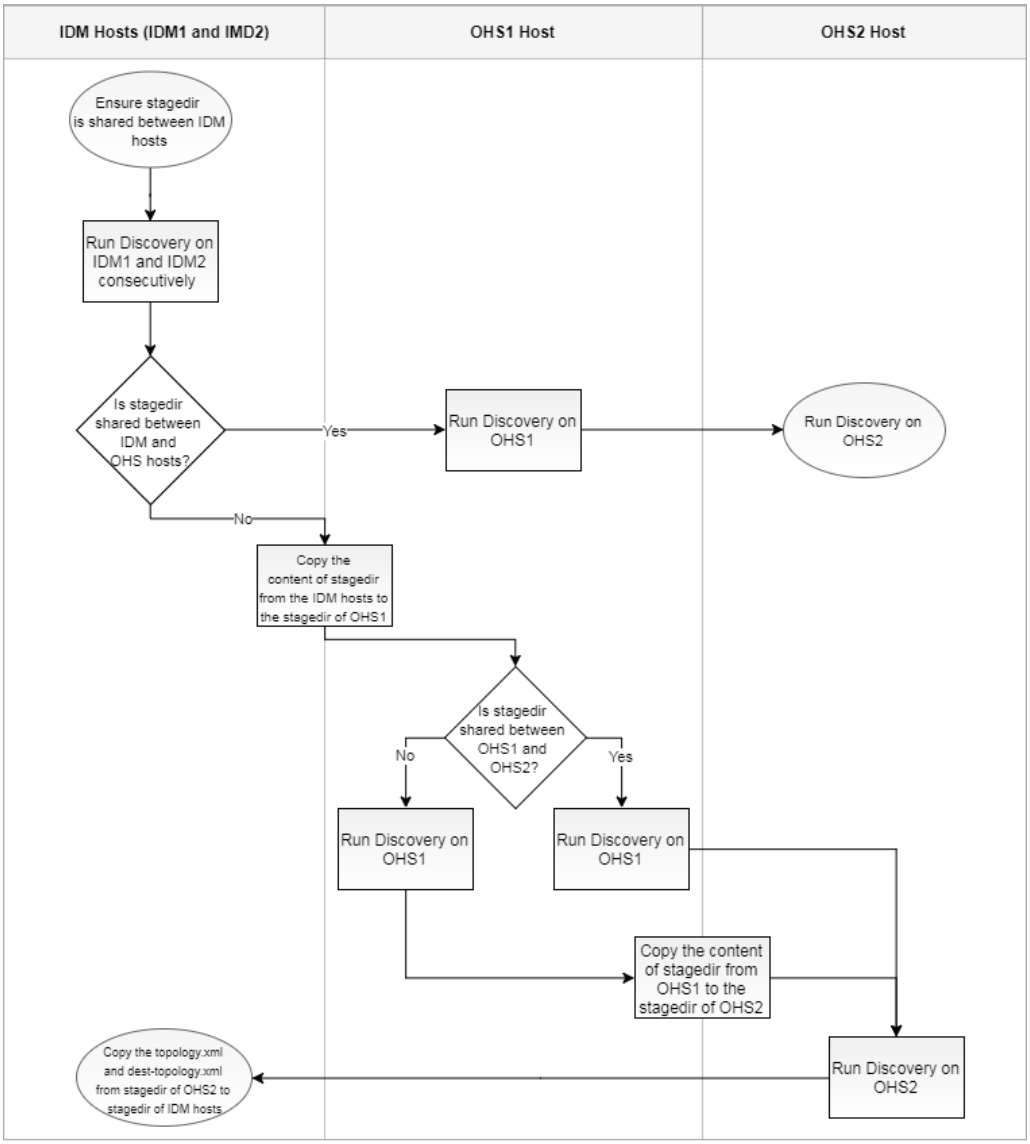
1. On the IDM host where adminserver is present, and then on other hosts.
2. If OID and OIM are on separate nodes, first run discovery on the OIM host where `adminserver` is present, then on the OIM scaled-out node, and then on the OID nodes.

7.6.2.2 Run the Discovery Tool

If your set up has IDM nodes on different machines (including scaled out support), the discovery tool will have to be run serially on each IDM node.

Review the following diagram that shows a typical discovery flow including OHS in Demilitarized Zone (DMZ) scenario:

Figure 7-2 Discovery Flow



To run the discovery tool, perform the following steps:

1. Ensure `stagedir` is shared between IDM hosts.
2. Run Discovery on IDM hosts as follows:

```
SHARED_LOCATION/idmUpgrade/discovery/bin
./idmdisc.sh -stagedir <location of the staging directory>
```

> **Note:**
>
> `SHARED_LOCATION` should be shared across all nodes. Since `idmUpgrade` and `stagedir` are under `SHARED_LOCATION`, they are automatically shared across machines.

`-topology`: The discovery tool updates the `topology.xml` file, which contains information about all IDM nodes. For more information about this file, see Discover Topology.

`-credconfig`: During the discovery process, the tool will prompt you for passwords to connect to IDM servers and services. These passwords will be stored in the `credconfig` file to be used during later stages of upgrade. Both the `topology.xml` file and `credconfig` will be created inside `stagedir`.

`-logDir`: The location of the file where all discovery logs will be placed.

3. Verify whether `stagedir` is shared between IDM and OHS hosts:
   - If it is shared, perform the following steps:
     a. Run Discovery on OHS1.
     b. Run Discovery on OHS2.
   - If it is not shared, perform the following steps:
     a. Copy the contents of the `stagedir` from the IDM hosts to the `stagedir` of OHS1.
     b. Verify whether `stagedir` is shared between OHS1 and OHS2.
        – If it is shared, perform the following steps:
          i. Run Discovery on OHS1.
          ii. Run Discovery on OHS2.
          iii. Copy the `topology.xml` and `dest-topology.xml` from the `stagedir` of OHS2 to the `stagedir` of the IDM hosts.
        – Otherwise, perform the following steps:
          i. Run Discovery on OHS1.
          ii. Copy the contents of the `stagedir` from the OHS1 to the `stagedir` of OHS2.
          iii. Run Discovery on OHS2.
          iv. Copy the `topology.xml` and `dest-topology.xml` from the `stagedir` of OHS2 to the `stagedir` of the IDM hosts.

          After running Discovery successfully, you see the following message:

          ```
          Oracle IDM Discovery Utility succeeded.
          ```

Discovery Questionnaire

The Discovery tool formulates some questions while being run. During the questionnaire, certain user names are set as defaults. Based on the relevance of values in your environment, you can either choose to use the same default user names as such by pressing enter or change them accordingly.

The following table shows the questions formulated by the discovery tool. The table also shows the answers you must provide and a brief description of each question if applicable:

> **Note:**
>
> The words in parenthesis are defaulted values. You must change them accordingly.

Table 7-3 Questions Formulated by the Discovery Tool

Question	Answer	Description
Is `stagedir` directory: `$STAGE_DIR` shared across all nodes of IDM (OID/OIM/OHS), including Scale-Out nodes (if any). Note that if the OHS host(s) is in DMZ and `stagedir` cannot be shared, you need to manually copy contents of `stagedir` of OID/OIM node to `stagedir` of OHS host(s) before running discovery on OHS node(s) and then after discovery completes on OHS node(s), copy back the `topology.xml` and `dest-topology.xml` from `stagedir` of OHS host(s) to `stagedir` of the OID/OIM node. [Y/N]:	Y	Verify if the `stagedir` directory is shared across all IDM nodes, including scale out nodes (if any) and if it is, then enter **Y**. If you enter **N**, the discovery tool exits.
Are all IDM servers up and running, please confirm? [Y/N]:	Y	Verify that the servers are up and running. If they are, then enter **Y**. If you enter **N**, the discovery tool exits.
Enter Weblogic Server (WLS) admin user name for domain `IDMDomain` (`weblogic_idm`):	Your username	If the IDM Domain administrator is `weblogic_idm`, you do not need to enter a value, it will be completed by default. Otherwise, you must enter the value.
Enter password:	Your password	The IDM domain administrator password.
Enter Oracle Identity Manager (OIM) admin user (`xelsysadm`) password:	Your password	The OIM admin user's (usually `xelsysadm`) password.
Enter IDStore policy RW user, under user search DN (`PolicyRWUser`):	Your username	The `PolicyRWUSer` name, usually present under user search DN in LDAP.
Enter IDStore policy RW user password:	Your password	The `PolicyRWUSer` password.
Enter Oracle Access Manager (OAM) admin user name (`oamadmin`):	Your username	The OAM admin user, also used to login to the OAM console. Here since it is different to the default, the value provided is oamAdminUser.

Table 7-3 (Cont.) Questions Formulated by the Discovery Tool

Question	Answer	Description
Enter password for admin user DN cn=oamadmin,cn=Users,dc=us,dc=oracle,dc=com:	Your password	The OAM admin user password.
Enter OIM DB sys password:	Your password	The OIM DB sys user password.
Enter Oracle Internet Directory(OID) admin user name (cn=orcladmin):	Your username	The OID admin user.
Enter Oracle Internet Directory(OID) admin password for cn=orcladmin:	Your password	The OID admin user password.
Enter OID DB sys password: (OID DB sys user password)	Your password	The OID DB sys user password.
Enter Oracle Virtual Directory (OVD) admin user name (cn=orcladmin):	Your username	The OVD admin user.
Enter Oracle Virtual Directory(OVD) admin password for cn=orcladmin:	Your password	The OVD admin user password.

7.6.3 Set Up True-Up Environment

A true-up environment is an entirely new IDM environment, which behaves exactly like the current IDM installation. Your true-up environment will conform to the layout and structure of an environment that has been provisioned using the IDM provisioning scripts provided by Oracle.

This section contains the following topics:

- Prerequisites for Setting Up True-Up Environment
- Set Up Binaries

7.6.3.1 Prerequisites for Setting Up True-Up Environment

Before setting up your true-up environment, ensure you meet the following prerequisites:

- The true-up environment must be set up on the `/u01/IDMTOP` and `/u02/local/IDMTOP` directories.
- Ensure that the directories are owned by the same user who owns the current IDM installation.

7.6.3.2 Set Up Binaries

To set up the binary files, you need the True-up tars.

To obtain these tars, use the patch 26504255 you downloaded in Copy and Unzip idmUpgrade.zip. The tars must be unzipped accordingly under root.

The patch contains the following zip files:

For Linux:

- p26504255_111230_Linux-x86-64_1of5.zip
- p26504255_111230_Linux-x86-64_2of5.zip
- p26504255_111230_Linux-x86-64_3of5.zip
- p26504255_111230_Linux-x86-64_4of5.zip
- p26504255_111230_Linux-x86-64_5of5.zip

For Solaris:

- p26504255_111230_SOLARIS64_1of6.zip
- p26504255_111230_SOLARIS64_2of6.zip
- p26504255_111230_SOLARIS64_3of6.zip
- p26504255_111230_SOLARIS64_4of6.zip
- p26504255_111230_SOLARIS64_5of6.zip
- p26504255_111230_SOLARIS64_6of6.zip

To ensure that the files are not corrupted, you can compare the checksum of the files listed above against the digests after downloading them.

This patch also contains the following true-up tars:

- ohs.tar.gz
- oid.tar.gz
- oimX.tar.gz

  Where

  – X: is a digit.

Depending on the topology setup, choose the tar corresponding to the node type viz OID, OIM, OHS and unzip them in the machines hosting those nodes, including the scaled out nodes. For example:

- On the OID and OID-SO (if it exists) node, run the following command:

  ```
  cd /
  tar -zxvf <stagedir>/oid.tar.gz --keep-old-files
  ```

- On the OIM node, run the following command:

  If the OIM node is scaled out, extract the OIM tar on the scaled out OIM.

  ```
  cd /
  tar -zxvf <stagedir>/oim.tar.gz --keep-old-files
  ```

- On the OHS and OHS-SO (if it exists) node, run the following command:

  ```
  cd /
  tar -zxvf <stagedir>/ohs.tar.gz --keep-old-files
  ```

> **Note:**
>
> Do not use the option `'--keep-old-files'` with the tar command on Solaris platforms.

The tars will set up oracle homes and instance homes for IDM components inside the `/u01` and `/u02` directories.

7.6.4 Perform Migration Tasks

This section describes how to migrate the configuration to the true-up environment. This section contains the following sections:

- Prerequisites for Running Migration
- Migrate Configuration to True-Up Environment
- Post-Migration Tasks

7.6.4.1 Prerequisites for Running Migration

Before running migration, ensure the following prerequisites are met:

- Stop only the IDM source environment. To minimize downtime, you can keep the services running when the binaries are set up and only shut down before the migration.
- Ensure that your administrator passwords or schema passwords do not expire in the next 7 days.
- Ensure that `stagedir` is shared and mounted on same path on all hosts. This way when the `stagedir` is passed during the invocation of migration on each host, the same directory path is passed.

7.6.4.2 Migrate Configuration to True-Up Environment

Migrating the configuration from the introspected environment to the newly setup true-up environment uses the artifacts generated by the discovery tool. Before migrating, change to the following directory:

```
cd SHARED_LOCATION/idmUpgrade
```

Migrate the configuration to the true-up environment by running the following command on all IDM nodes:

```
perl idmMigrateOnPremise.pl -node=<node type> -stagedir=<stage dir>
```

Run the `idmMigrateOnPremise.pl` command on each node in the following order:

- OID

  ```
  perl idmMigrateOnPremise.pl -node=OID -stagedir=<location of staging directory>
  ```

  If the environment is scaled out, run the following commands on the OID scaled out node:

  ```
  perl idmMigrateOnPremise.pl -node=OID-SO -stagedir=<location of staging
  directory>
  ```

- OIM

  ```
  perl idmMigrateOnPremise.pl -node=OIM -stagedir=<location of staging directory>
  ```

  If the environment is scaled out, run the following commands on the OIM scaled out node:

  ```
  perl idmMigrateOnPremise.pl -node=OIM-SO -stagedir=<location of staging
  directory>
  ```

- OHS

  ```
  perl idmMigrateOnPremise.pl -node=OHS -stagedir=<location of staging directory>
  ```

  If the environment is scaled out, run the following commands on the OHS scaled out node:

  ```
  perl idmMigrateOnPremise.pl -node=OHS-SO -stagedir=<location of staging
  directory>
  ```

Confirm that the status message at the end of the run is successful on each node. If the script gives an error, check the error message and resolve the issue. Rerun `idmMigrateOnPremise.pl` and ensure it is successful.

7.6.4.3 Post-Migration Tasks

After running migration, you must perform the following task:

- Manually Register OID Instances

After migration, you can start/stop the IDM components on a given node using the IDM provisioning start/stop scripts as described in Start and Stop All IDM Components on a Host.

7.6.4.3.1 Manually Register OID Instances

After completing migration, you must manually register OID instances to enable the OID and OVD status to be shown in EM console.

- Run the following command:

  ```
  $OID_INST_HOME/bin/opmnctl registerinstance -adminHost ADMINSERVER_HOST -
  adminPort ADMINSERVER_PORT -adminUsername ADMIN_USER
  ```

  After running this command, you are prompted for the admin user password.

> **Note:**
>
> You must perform this on each of the OID instances involved in the IDM setup.

7.6.5 Verify True-Up Environment Is Up

To verify if your true-up environment is up and running, perform the following tests:

- **WLS Tests**

  1. Log in to the OIM Domain Admin Server console and perform the following steps:

a. Check the server status.
b. Check the cluster status.
c. Check the data sources.
d. Ensure that all the deployments are either in "Running" or "Installed" state.

2. Log in to the EM console.

- **OIM Tests**

1. Log in to the Oracle Identity Manager Administration Console, with `xelsysadm` and perform the following steps:
   a. Verify requests as follows:
      i. Create a Request, such as updating the phone number information for `xelsysadm`.
      ii. Go to your inbox and verify whether the request has come for approval.
      iii. Click the task, and click **Approve** in the **Actions** tab.
      iv. Click the refresh icon. The request comes back. Approve it again.
      v. Ensure that the request's details page shows the correct information.
      vi. Click users, and then search `xelsysadm`.
      vii. Ensure that the phone number for `xelsysadm` is modified.
   b. Verify new users as follows:
      i. Create a new user.
      ii. Log in using the newly created user.
      iii. Change the password for the user.
      iv. Log out and log in again with the same user using the new password.
2. Log in to the sysadmin console and perform the following steps:
   a. In the left pane, under Event Management, click **Reconciliation**.
   b. In the left pane, under System Management, click **Scheduler**.
   c. Search for "LDAP*" and proceed as follows:
      i. Run any full reconciliation job, for example, LDAP User Create and Update Full Reconciliation.
      ii. Run any incremental reconciliation job, for example, LDAP User Create and Update Reconciliation.

- **OAM Tests**
  – Log in to the OAM console.

7.6.6 Run preValidate Script

The following `preValidateOnPremise.pl` script must be executed serially on each IDM node, including the scaled out nodes:

```
perl preValidateOnPremise.pl <node type> REPOSITORY_LOCATION/
installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches STAGE_DIR/
upgradeOnPremise.properties
```

Where

- *REPOSITORY_LOCATION*: Fusion Applications Release 12 repository.
- STAGE_DIR: Location of stagedir.

Run the preValidateOnPremise command in the following order:

- OID

  ```
  perl preValidateOnPremise.pl OID REPOSITORY_LOCATION/installers,SHARED_LOCATION/
  11.12.x.0.0_post_repo_patches STAGE_DIR/upgradeOnPremise.properties
  ```

  If the environment is scaled out, run the following command on the OID scaled out node:

  ```
  perl preValidateOnPremise.pl OID-SO REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches STAGE_DIR/
  upgradeOnPremise.properties
  ```

- OIM

  ```
  perl preValidateOnPremise.pl OIM REPOSITORY_LOCATION/installers,SHARED_LOCATION/
  11.12.x.0.0_post_repo_patches STAGE_DIR/upgradeOnPremise.properties
  ```

  If the environment is scaled out, run the following command on the OIM scaled out node:

  ```
  perl preValidateOnPremise.pl OIM-SO REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches STAGE_DIR/
  upgradeOnPremise.properties
  ```

- OHS

  ```
  perl preValidateOnPremise.pl OHS REPOSITORY_LOCATION/installers,SHARED_LOCATION/
  11.12.x.0.0_post_repo_patches STAGE_DIR/upgradeOnPremise.properties
  ```

  If the environment is scaled out, run the following command on the OHS scaled out node:

  ```
  perl preValidateOnPremise.pl OHS-SO REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches STAGE_DIR/
  upgradeOnPremise.properties
  ```

Confirm that the status message at the end of the run is successful on each node. If the script gives an error, check the error message and resolve the issue. Rerun preValidate and ensure it is successful.

7.6.7 Manually Download OIM Email Template

After running the preValidate script on your type II environment, manually download the OIM email template as follows:

1. Log in to the OIM host.
2. Go to the idmUpgrade unzip location.
3. Execute exportOIMDataOnPremise.pl as follows:

   ```
   perl exportOIMDataOnPremise.pl STAGE_DIR/upgradeOnPremise.properties
   <SHARED_UPGRADE_LOCATION>/<podName>/emailTemplateDir/emailtemplate.xml
   ```

   Where

- `SHARED_UPGRADE_LOCATION`: It is located in `pod.properties`, and its default value is `/u01/sharedupgradelocation`.

4. Confirm that the status message at the end of the run is successful. If the script gives an error, check the error message and resolve the issue. Then, rerun `exportOIMDataOnPremise.pl` and ensure it is successful.

7.6.8 Stop All IDM Services

Stop all IDM services by running the following command on all IDM nodes:

```
perl stopIDMOnPremise.pl <node type> STAGE_DIR/upgradeOnPremise.properties
```

Where

- *STAGE_DIR*: Location of stagedir.

Run the `stopIDMOnPremise.pl` command in the following order:

- OHS

  If the environment is scaled out, run the following command on the OHS scaled out node:

  ```
  perl stopIDMOnPremise.pl OHS-SO STAGE_DIR/upgradeOnPremise.properties
  ```

  If the environment is not scaled out, run the following command on the OHS node:

  ```
  perl stopIDMOnPremise.pl OHS STAGE_DIR/upgradeOnPremise.properties
  ```

- OIM

  If the environment is scaled out, run the following command on the OIM scaled out node:

  ```
  perl stopIDMOnPremise.pl OIM-SO STAGE_DIR/upgradeOnPremise.properties
  ```

  If the environment is not scaled out, run the following command on the OIM node:

  ```
  perl stopIDMOnPremise.pl OIM STAGE_DIR/upgradeOnPremise.properties
  ```

- OID

  If the environment is scaled out, run the following command on the OID scaled out node:

  ```
  perl stopIDMOnPremise.pl OID-SO STAGE_DIR/upgradeOnPremise.properties
  ```

  If the environment is not scaled out, run the following command on the OID node:

  ```
  perl stopIDMOnPremise.pl OID STAGE_DIR/upgradeOnPremise.properties
  ```

7.6.9 Upgrade Binaries

Upgrade the binary files used by IDM components by running the following command on all IDM nodes:

```
perl idmUpgradeOnPremise.pl -node=<node type> REPOSITORY_LOCATION/
installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=STAGE_DIR/
upgradeOnPremise.properties -mode=binary
```

Where

- *REPOSITORY_LOCATION*: Fusion Applications Release 12 repository.
- *STAGE_DIR*: Location of stagedir.

Run the `idmUpgradeOnPremise.pl` command in the following order:

- OID

  ```
  perl idmUpgradeOnPremise.pl -node=OID REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=STAGE_DIR/
  upgradeOnPremise.properties -mode=binary
  ```

  If the environment is scaled out, run the following command on the OID scaled out node:

  ```
  perl idmUpgradeOnPremise.pl -node=OID-SO REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=STAGE_DIR/
  upgradeOnPremise.properties -mode=binary
  ```

- OIM

  ```
  perl idmUpgradeOnPremise.pl -node=OIM REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=STAGE_DIR/
  upgradeOnPremise.properties -mode=binary
  ```

  If the environment is scaled out, run the following command on the OIM scaled out node:

  ```
  perl idmUpgradeOnPremise.pl -node=OIM-SO REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=STAGE_DIR/
  upgradeOnPremise.properties -mode=binary
  ```

- OHS

  ```
  perl idmUpgradeOnPremise.pl -node=OHS REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=STAGE_DIR/
  upgradeOnPremise.properties -mode=binary
  ```

  If the environment is scaled out, run the following command on the OHS scaled out node:

  ```
  perl idmUpgradeOnPremise.pl -node=OHS-SO REPOSITORY_LOCATION/
  installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=STAGE_DIR/
  upgradeOnPremise.properties -mode=binary
  ```

7.6.10 Update IDM Configuration

Update the IDM configuration to Release 12 level by running the following `config` upgrade commands on all IDM nodes:

```
perl idmUpgradeOnPremise.pl -node=<node type> REPOSITORY_LOCATION/
installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=STAGE_DIR/
upgradeOnPremise.properties -mode=config
```

Where

- *REPOSITORY_LOCATION*: Fusion Applications Release 12 repository.
- *STAGE_DIR*: Location of stagedir.

Run the `idmUpgradeOnPremise.pl` command in the following order:

- OID

```
perl idmUpgradeOnPremise.pl -node=OID REPOSITORY_LOCATION/
installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=STAGE_DIR/
upgradeOnPremise.properties -mode=config
```

If the environment is scaled out, run the following command on the OID scaled out node:

```
perl idmUpgradeOnPremise.pl -node=OID-SO REPOSITORY_LOCATION/
installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=STAGE_DIR/
upgradeOnPremise.properties -mode=config
```

- OIM

```
perl idmUpgradeOnPremise.pl -node=OIM REPOSITORY_LOCATION/
installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=STAGE_DIR/
upgradeOnPremise.properties -mode=config
```

If the environment is scaled out, run the following command on the OIM scaled out node:

```
perl idmUpgradeOnPremise.pl -node=OIM-SO REPOSITORY_LOCATION/
installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=STAGE_DIR/
upgradeOnPremise.properties -mode=config
```

If you are on a Solaris platform, after running this command on OIM perform the steps as listed in Re-create IDM Schemas Manually (Solaris Only).

- OHS

```
perl idmUpgradeOnPremise.pl -node=OHS REPOSITORY_LOCATION/
installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=STAGE_DIR/
upgradeOnPremise.properties -mode=config
```

If the environment is scaled out, run the following command on the OHS scaled out node:

```
perl idmUpgradeOnPremise.pl -node=OHS-SO REPOSITORY_LOCATION/
installers,SHARED_LOCATION/11.12.x.0.0_post_repo_patches -props=STAGE_DIR/
upgradeOnPremise.properties -mode=config
```

7.6.11 Run postValidate Script

To confirm that the upgrade was successful, run the following post-upgrade validation command on all IDM nodes:

```
perl postvalidateOnPremise.pl <node type> STAGE_DIR/upgradeOnPremise.properties
```

Where

- *STAGE_DIR*: Location of stagedir.

Run the `idmUpgradeOnPremise.pl` command in the following order:

- OID

```
perl postvalidateOnPremise.pl OID STAGE_DIR/upgradeOnPremise.properties
```

If the environment is scaled out, run the following command on the OID scaled out node:

```
perl postvalidateOnPremise.pl OID-SO STAGE_DIR/upgradeOnPremise.properties
```

- OIM

```
perl postvalidateOnPremise.pl OIM STAGE_DIR/upgradeOnPremise.properties
```

If the environment is scaled out, run the following command on the OIM scaled out node:

```
perl postvalidateOnPremise.pl OIM-SO STAGE_DIR/upgradeOnPremise.properties
```

- OHS

```
perl postvalidateOnPremise.pl OHS STAGE_DIR/upgradeOnPremise.properties
```

If the environment is scaled out, run the following command on the OHS scaled out node:

```
perl postvalidateOnPremise.pl OHS-SO STAGE_DIR/upgradeOnPremise.properties
```

Confirm that the status message at the end of the run is successful on each node. If the script gives an error, check the error message and resolve the issue.

After upgrade, you can start/stop the IDM components on a given node using the IDM provisioning start/stop scripts as described in Start and Stop All IDM Components on a Host.

7.7 Reconnect Enterprise IDM Integrations

If your IDM for FA is integrated with Enterprise IDM and you disconnected integrations as listed in Disconnect Enterprise IDM Integrations, then you must reconnect them by following the steps listed in *Getting Started with Oracle Fusion Applications Bridge for Active Directory (Doc ID 2309139.1)* available on My Oracle Support.

7.8 Update Status to Success

After successfully upgrading Oracle Identity Management, update the task status to `success` on the IDM host as follows:

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype IDM -hostname host_name -
release 11.12.x.0.0 -phase DowntimePreFA -taskid UpgradeIDMPausePointPlugin  -
taskstatus success
```

7.9 Resume Upgrade Orchestrator to Upgrade Oracle Fusion Applications

Resume orchestration on each IDM host that is listed in the following properties in the pod.properties file, using the command in Run Upgrade Orchestrator During Downtime, Step 4:

- `HOSTNAME_IDMOID`
- `HOSTNAME_IDMOIM`
- `HOSTNAME_IDMOHS`

Upgrade Orchestrator runs the tasks in the following table to upgrade Oracle Fusion Applications.

Table 7-4 Tasks Run During Various Downtime Phases

Task Name	Phase Name	Task ID	Host Types
Run Upgrade Readiness (During Downtime) Checks	DowntimePreFA	DuringDowntimeChecks	Primordial, OHS, Midtier
Remove Conflicting Patches for Oracle Fusion Middleware Component Oracle Homes	DowntimePreFA	RemoveConflictingPatches	Primordial
Upgrade JDK	DowntimePreFA	UpgradeJDK	Primordial
Run RUP Lite for OVM in Offline Mode as Application User	DowntimePreFA	RupLiteOvmOffline	Primordial, OHS, Midtier, IDM
Run Oracle Fusion Applications RUP Installation Part 1 of 2	DowntimeDuringFA Phase	RunFirstRUPInstaller	Primordial

Once you have successfully resumed Upgrade Orchestrator to upgrade Oracle Fusion Applications, proceed to Pause Point 3 - Reload Orchestration.

7.10 IDM for FA Upgrade Properties Files

This section describes some properties files used in the IDM for FA Upgrade to Release 12 (11.12.x.0.0).

upgradeOnPremise.properties

The following tables provides a description of the upgradeOnPremise.properties:

> **Note:**
>
> The optional parameters are usually defaulted or introspected. You can change them if the property values differ in your environment.

Property Name	Mandatory	Default Value	Description
DB_OIM_SYS_PASSWORD	Yes	Blank	Password for the IDM sys DB
DB_IDSTORE_SYS_PASSWORD	Yes	Blank	Password for the OID sys DB
NODE_MANAGER_PWD	Yes	Blank	Password for the Node manager
OID_IDSTORE_ORCLADMIN_PASSWORD	Yes	Blank	Password for the OID admin user

Property Name	Mandatory	Default Value	Description
OVD_IDSTORE_ORCLADMIN_PASSWORD	Yes	Blank	OVD admin user password
OAM_ADMINUSER_PASSWORD	Yes	Blank	Password for the OAM Admin user
OIM_XELSYADM_PASSWORD	Yes	Blank	Password for the OIM user xelsysadm
IDM_DOMAIN_ADMIN_PASSWORD	Yes	Blank	Password for the WLS Domain administrator user
OAM_SW_USER_PWD	Yes	Blank	Password for the OAM Software User account
IDSTORE_USERSEARCHBASE	Yes	`cn=Users,dc=us,dc=oracle,dc=com`	User search base
IDSTORE_GROUPSEARCHBASE	Yes	`cn=Groups,dc=us,dc=oracle,dc=com`	Group search base
ID_STORE_SEARCH_BASE	Yes	`dc=us,dc=oracle,dc=com`	Search base for all
TOPOLOGY_XML_FILE_LOC	Yes	`/u01/IDMTOP/config/lcmconfig/topology/topology.xml`	Location of the topology.xml file
START_STOP_SCRIPT_WORKING_DIR	Yes	`/u01/IDMTOP/config/scripts`	Location of IDM Provisioning Start/Stop scripts
IDMLCM_HOME	Yes	`/u01/IDMTOP/idmlcm`	Location of IDMLCM home
IDMUTILS_HOME	Yes	`/u01/IDMTOP/products/app/Oracle_IDMUTILS1`	Location of Oracle IDMUTILS
OID_JAVA_HOME	Yes	`/u01/IDMTOP/products/dir/jdk6`	Location of OID MW JAVA HOME
OIM_JAVA_HOME	Yes	`/u01/IDMTOP/products/app/jdk6`	Location of OIM MW JAVA HOME
OHS_JAVA_HOME	Yes	`/u01/IDMTOP/products/ohs/jdk6`	Location of OHS MW JAVA HOME
NODE_MANAGER_USER=admin	No	admin	Node manager username
OID_USER=cn=orcladmin	No	orcladmin	OID admin username
OVD_USER=cn=orcladmin	No	orcladmin	OVD admin username
IDSTORE_OAMADMINUSER=oamAdminUser	No	oamAdminUser	OAM Admin user used to login to oamconsole
IDM_DOMAIN_ADMIN=weblogic_idm	No	weblogic_idm	IDM weblogic domain administrator username

Property Name	Mandatory	Default Value	Description
IDSTORE_OAMSOFTWAREUSER=oamSoftwareUser	No	oamSoftwareUser	OamSoftwareUser present in OAM configuration
FA_POLICYSTORE_NAME=cn=FAPolicies	No	cn=FAPolicies	FA Policy store name
AGENT_ID=Webgate_IDM	No	Webgate_IDM	Webgate Agent ID
APP_DOMAIN=IAMSuite	No	IAMSuite	Application Domain Name
HOST_IDENTIFIER=IAMSuiteAgent	No	IAMSuiteAgent	Host identifier related to application domain
ACCESS_CLIENT_PASSPHRASE_USER=user	No	user	Access client passphrase user
ACCESS_CLIENT_PASSPHRASE_PWD=	No	If not provided, the password is introspected	Access client passphrase password
NAP_GLOBAL_PASSPHRASE_USER=user	No	user	NAP global passphrase user
OPSS_DB_PASSWORD=	No	If not provided, it is defaulted to the OAM schema password	New password for OPSS DB schema
OIF_11GR2_SINGNING_KEY_PWD=	No	If not provided, it is defaulted to the OAM schema password	New password required by OIF keystore for signing
IS_OVD_SPLIT_CONFIGURE=false	No	If configured, set it to true	Flag to identify if OVD Split Profile is configured or not
SHADOW_ENTRIES_USER_CONTAINER_DN=cn=shadowentries	No	cn=shadowentries	Container in Oracle Internet Directory when OVD split profile is configured

7.11 IDM Upgrade and Migration Log Files Location

The following table shows the location of the IDM Upgrade and migration log files:

> **Note:**
>
> These values may change based on the customization you perform to the `LOG_DIR` property in the upgrade and migration properties file.

Table 7-5 Log Files Location

Log	Location
Type I Upgrade	`/u01/logs`

Table 7-5 (Cont.) Log Files Location

Log	Location
Type II Migration	`stagedir/logs`
Type II Upgrade	`stagedir/logs`

8
Run Post-Upgrade Tasks

This section describes the tasks that must be performed after completing the steps in Upgrade to Oracle Fusion Applications Release 12. The following topics are discussed:

8.1 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*.

8.2 Review the Post RUP Installer Report

To check for any errors or warnings that require attention, review the Post RUP Installer report as it provides an overview of the tasks that Upgrade Orchestrator ran when it called RUP Installer. This report is generated in HTML and XML files and includes links to log files.

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 12, the Post RUP Installer report files can be found in the following location:

APPLICATIONS_CONFIG`/lcm/logs/11.12.x.0.0/RUP:`

`PostRUPInstallerReport_`*`timestamp`*`.html`
`PostRUPInstallerReport_`*`timestamp`*`.log`
`PostRUPInstallerReport_`*`timestamp`*`.xml`

For information about resolving errors, see Monitor and Troubleshoot the Upgrade .

8.3 Review the Orchestration Report

To check for any errors or warnings that require attention and to confirm whether the upgrade completed successfully, review the Oracle Fusion Applications Orchestration Report. If there were previous failures during the upgrade, this report would have been generated each time there was a failure. The report name is `FAOrchestrationReport_`*`release_hosttype_hostname_timestamp`*`.html`.

The Orchestration 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 Oracle Fusion Applications Orchestration Report.

8.4 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 the following directory:

APPLICATIONS_CONFIG`/lcm/admin/11.12.x.0.0/fapatch/JAZN/`*`stripe`*`/report/report.txt`

The *stripe* is: `appsdiag`, `crm`, `hcm`, `obi`, `soa-infra`, `b2bui`, `fscm`, `IDCCS`, or `OracleBPMComposerRolesApp`

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, evaluate and manually patch the role by using Oracle Authorization Policy Manager (APM).

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 for each stripe is under:

  APPLICATIONS_CONFIG/lcm/admin/11.12.x.0.0/fapatch/JAZN/*stripe*/stage/baseline

- Location of patch files for each stripe is under:

  APPLICATIONS_CONFIG/lcm/admin/11.12.x.0.0/fapatch/JAZN/*stripe*/stage/current

8.5 Disable Oracle Java Virtual Machine Support

The process for disabling Oracle Java Virtual Machine (OJVM) support has already been partially completed during pre-upgrade. In particular, patch 23341410 has already been downloaded and unzipped into a stage directory.

For the following steps, whichever stage directory was used is represented by *STAGE_DIR*:

1. Execute the following command:

   ```
   cd $STAGE_DIR/bin
   ```

2. Execute the following command:

   ```
   sh ojvmctrl.sh -mode disable -appbase APPLICATIONS_BASE -stage
   ```

8.6 Reload Custom Templates in BI Publisher

If BI Publisher reports have been customized, reload custom templates for BI Publisher reports on Oracle-delivered BI Publisher reports by following the steps in "Retaining customized templates while upgrading or applying patches (Doc ID 1909819.1)" from My Oracle Support. If there is a plan to create payments with a format created in Release 8 or earlier and attached with a predefined BI Publisher template name, refer to "Custom formats created by attaching seeded BI Publisher template in Release 8 or earlier will not generate the correct payment file in Release 10 (Doc ID 1910233.1)".

8.7 Perform Steps in Technical Known Issues

Follow any post-upgrade steps mentioned in the Post-Upgrade Known Issues section of the *Technical Known Issues* found on My Oracle Support.

8.8 Allocate Memory for HCM Workforce Reputation Management

This section is applicable only if there is a plan to use the Human Capital Management (HCM) Workforce Reputation Management product packaged with the Workforce Deployment, or Workforce Development product offerings. To allocate memory for HCM Workforce Reputation Management, perform the following steps:

1. The physical machine hosting the HCM Workforce Reputation Management (`WorkforceReputationServer_1`) managed server must have a minimum of 24 GB of memory. 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 following line:

     ```
     fusion.HCMDomain.WorkforceReputationCluster.default.minmaxmemory.main=-Xms512m -Xmx2048
     ```

     with the following line:

     ```
     fusion.HCMDomain.WorkforceReputationCluster.default.minmaxmemory.main=-Xms4096m -Xmx8192m
     ```
   - Save the `fusionapps_start_params.properties` file.
2. Restart the HCM Workforce Reputation Management (`WorkforceReputationServer_1`) managed server either from the WebLogic console or Enterprise Management for the HCM domain. For more information, see Start and Stop an Oracle Fusion Applications Environment in the *Oracle Fusion Applications Administrator's Guide*.

8.9 Apply Oracle Fusion Applications Patches

If any Oracle Fusion Applications patches were downloaded in Download and Unzip Mandatory Post-Release 12 Patches, apply these patches now. For more information, see the Apply Technical Patch Bundles: P4FA, Apply Functional Patch Bundle, Apply One-Off Patches, or Apply Identity Management (IDM) Patches in the *Oracle Fusion Applications Patching Guide*.

8.10 Confirm Inbound Refinery (IBR) is Registered

This step relates to environments that contain local domain deployment in the domain topology. To determine there is a need to perform this step, review the following file:

```
$UCM_DOMAIN_PATH/CommonDomain/ucm/cs/data/providers/providers.hda
```

- If this file contains the string, `"IbrProvider"`, then IBR is registered and this step can be skipped.

- If this file does not contain `"IbrProvider"`, perform the following steps:

1. Ensure that all WLS servers of the CommonDomain are running.
2. Run the following command. Note that `$UCM_DOMAIN_PATH` is the domain directory on the local domain node where the UCM server is running:

   ```
   $UCM_DOMAIN_PATH/CommonDomain/ucm/cs/bin/IdcCommand -c server -f $ADMIN_NODE/
   CommonDomain/provisioning/ibr/add_ibr_provider.hda -u sysadmin
   ```

3. Confirm that `"IbrProvider"` now exists in `$UCM_DOMAIN_PATH/CommonDomain/ucm/cs/data/providers/providers.hda`.
4. Bounce all servers in the CommonDomain.

8.11 Apply the Resource Manager Plan (Oracle VM Only)

On Oracle VM environments only, apply the Resource Manager Plan (`FUSIONAPPS_PLAN`) using the SQL script provided in Resource Manager Plan - SQL Script. Run this script as the privileged database user (SYSTEM/SYS).

8.12 Ensure Update Bundles Were Applied

Ensure that the latest update bundles were applied on the current environment:

- Oracle Fusion Middleware Update Bundles (P4FA) for Fusion Applications.
- Oracle Fusion Applications Update Bundles. See the Oracle Fusion Applications Update Bundle Readme (Doc ID 1603154.1) on My Oracle Support.

For information about how to install update bundles, review the update bundle `readme` file. Contact Oracle Support to obtain more information about update bundles.

8.13 Update Credential Store Password

When performing a direct upgrade and if Release 11 and Release 12 are in the upgrade path, the `FUSION_APPS_HCM_IIP_APPID` credential is seeded with different passwords causing a password mismatch between OID and the credential store.

To update the password in the credential store, perform the following steps:

1. Log in to Enterprise Manager (EM) for any Fusion Applications (FA) domain. For example, HcmDomain with read/write user permissions.
2. Follow the path **Farm_HCMDomain**, then **WebLogic Domain**, and then **HCMDomain**.
3. On the right pane open the **WebLogic Domain** menu, then go to **Security**, and then **Credentials**.
4. In the Credential Store Provider search for the `oracle.apps.security` menu.
5. Select `FUSION_APPS_HCM_IIP_APPID-KEY` from the credential list, and click **Edit**.
6. Ensure the User Name is as follows:

   ```
   'cn=FUSION_APPS_HCM_IIP_APPID,cn=AppIDUsers,cn=Users,dc=us,dc=oracle,dc=com'
   ```

7. Update the password in the credential store to a known one, for example, *`password`*.

8. Use Oracle Directory Services Manager (ODSM) to query the `FUSION_APPS_HCM_IIP_APPID` user.
9. Reset the password for the `APPID` to the same password you entered in Step 7.
10. Bounce the FA FMW tier (all domains).

8.14 Rerun the fmwDS.py Script

When performing a direct upgrade to Release 12 and the `fusion_aq` prefix is missing in the `JRFWSAsyncJmsModuleAQDOO-jms.xml` file, you must rerun the `fmwDS.py` script.

To rerun the `fmwDS.py` script, perform the following steps:

1. Validate if the `fusion_aq` prefix is present in the `JRFWSAsyncJmsModuleAQDOO-jms.xml` file (if the file exists) by using vi editor as shown in the following example path:

   ```
   /u01/<APPLTOP>/instance/domains/admin-apps.oracleoutsourcing.com/<SCM domain hostname>/config/jms/JRFWSAsyncJmsModuleAQDOO-jms.xml
   ```

   The correct `remote-jndi-name` should contain the `fusion_aq` prefix as shown in the following examples:

   ```
   <remote-jndi-name>Queues/fusion_aq.SCM_DOO_AsyncWS_Request</remote-jndi-name>

   <remote-jndi-name>Queues/fusion_aq.SCM_DOO_AsyncWS_Response</remote-jndi-name>
   ```

   If the `fusion_aq` prefix is present, no further actions are needed.

   If the `fusion_aq` prefix is not present, proceed to the following steps.
2. If the `<SCM domain hostname>` is online, shut it down before proceeding to the next step.
3. Navigate to the `wlst.sh` location as follows:

   ```
   cd /u01/<APPLTOP>/fusionapps/oracle_common/common/bin/
   ```
4. Rerun the `fmwDS.py` script. The script takes the following 3 parameters as inputs:
   - Domain Name: `<SCM domain hostname>`
   - Domain Path
   - Override Flag: "Y"

   For example:

   ```
   ./wlst.sh /u01/<APPLTOP>/fusionapps/atgpf/atgpf/bin/fmwDS.py <SCM domain hostname> /u01/APPLTOP/instance/domains/admin-apps.oracleoutsourcing.com/<SCM domain hostname> Y
   ```
5. Ensure the `fusion_aq` prefix is present by reviewing the `JRFWSAsyncJmsModuleAQDOO-jms.xml` file again.
6. Start the `<SCM domain hostname>` servers.

8.15 Correct ODI Agent Connections

In non-scaled out environments where the loadbalancer is not setup, you must update the ODI agents port to the OHS port.

To correct the ODI agent connections, perform the following steps:

1. Sign in to the ODI console and select **Master Repository**.
2. From the topology navigator, select one of the following applicable physical agents:
   - FusionCrmOdiAgent
   - FusionHcmOdiAgent
   - FusionIcOdiAgent
   - FusionScmOdiAgent
3. Right-click the agent and click **Edit**.
4. Update the host name and port number in the agent configuration with the OHS host and port for the respective domain, and then click **Save**.

8.16 Update the BISoapConnection Attribute 'WSDLContext' for CRM Domain

In post release 12 upgrade, the '`WSDLContext`' attribute value for `BISoapConnection` in the CRM Domain is incorrect.

You must update the '`WSDLContext`' attribute by performing the following steps:

1. Log in to the CRM Domain Enterprise manager Console as follows:

   ```
   http(s)://hostname:<CRMDomainPort>/em
   ```

2. Reach the CRMDomain node within Weblogic Domain.
3. Right-click on CRMDomain and open System MBean Browser.
4. Under the Application Defined MBeans node, find the following:

   ```
   oracle.adf.share.connections
   ```

5. Open this node and subsequently open the Sales Server node.
6. Navigate to the SalesApp node, then to ADFConnections, and then to BISoapConnection.
7. Click MarketingServerExternal and see the information in the right hand pane.
8. Change the value for WSDLContext attribute to analytics-ws.
9. Click **Apply** on the top right of the page to save the changes.
10. Restart the SalesServer in the CRMDomain.

8.17 Set Up AD Sync

Perform this step *only* if you used OVD to proxy AD in split profile and you performed the steps in Prepare for Upgrade. Otherwise, skip this step.

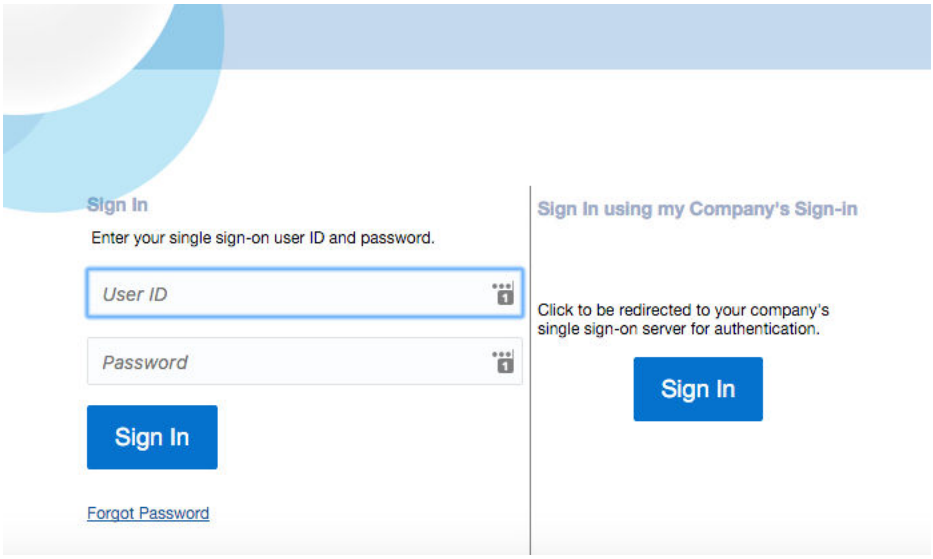
Set up AD sync post-upgrade to ensure that new users added to AD will be replicated into the bundled OID. You can set this up by using the AD-Bridge solution provided by Oracle.

8.18 Verify If Resource Is Protected

> **Note:**
>
> Perform this post-upgrade task only if you enabled federation and performed the steps as listed in Enable Federation for AD OVD Split-Profile. Otherwise, skip this task.

To verify if the `IAMSuiteAgent:/welcome_webcenter.html` resource is protected, perform the following steps:

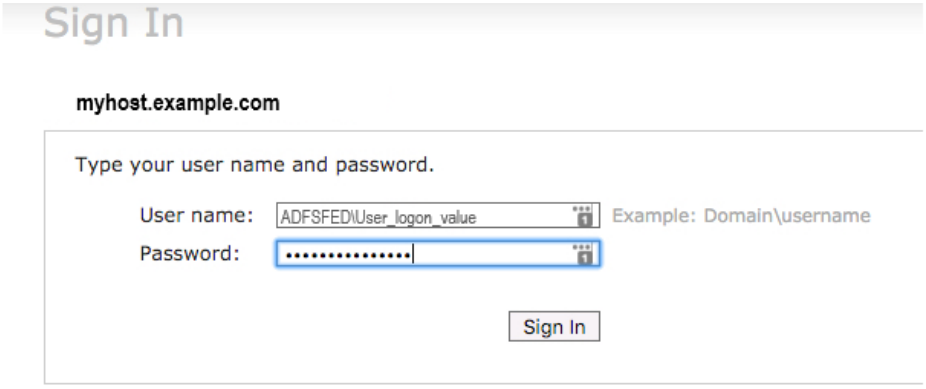
1. Go to `https://sso_lbr server: PORT URL/welcome_webcenter.html`.
   - If you configured your Single Sign-on (SSO) with federation as described in Configure OIF with an Identity Provider, Step 4, then the login page shows two login options as shown in the following figure. One login option is a local FA and the other one is an IdP login.



     a. Click **Sign In** in the "Sing In using my Company's Sign-in" section.

        You are redirected to the IdP login page.

     b. Log in using the Domain\Username and your password.
   - If you did not configure your SSO with federation, then the login page shows only the IdP login option.



– Log in using your Domain/username and your password.

2. Perform SSO and Single Logout (SLO).

8.19 Change the Lock File Location on OHS Server (Optional)

This is an optional post-upgrade step. By default, Oracle HTTP Server (OHS) places its lock file under the /tmp directory on Unix platforms. As a best practice, for on premise OVM environments, change the lock file location as follows:

- For APP OHS: `/dev/shm/ohs_ohs1_http_lock`
- For OSN OHS: `/dev/shm/osn_ohs1_http_lock`
- For bare metal environments: use the default lock file location

8.20 Remove the Contents of `patch_stage` Directory (Optional)

This is an optional post-upgrade step. To increase free disk space, remove the contents of the *`APPLICATIONS_BASE`*`/../patch_stage` directory.

8.21 Upgrade Oracle Fusion Applications and Oracle Identity Management Databases to 12c RDBMS

After upgrading to Release 12, the Oracle Fusion Applications and Oracle Identity Management Databases can be upgrade to RDBMS 12*c* as it is supported for Release 12.

9
Monitor and Troubleshoot the Upgrade

This section provides information to troubleshoot upgrade issues. The following topics are discussed:

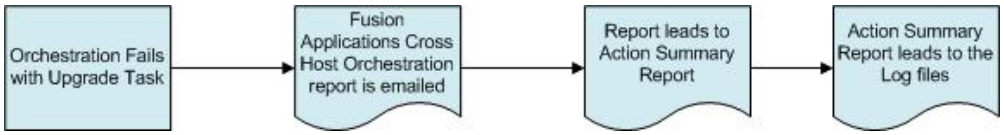
9.1 General Troubleshooting for Upgrade Orchestrator Failure

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 Orchestration Report as an attachment. The report name is `FAOrchestrationReport_release_hosttype_hostname_timestamp.html`. This report specifies the location to 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/11.12.x.0.0/orchestration/*host_name*-rel12_*hosttype_timestamp*.log.

The following figure shows the high level flow for troubleshooting Upgrade Orchestrator failures:

Figure 9-1 Troubleshooting Flow



Previous reports are archived whenever a new report is generated, as described in Unable to Find the Orchestration Report After Failure. For more information about the report, see Oracle Fusion Applications Orchestration Report.

Note that if an orchestration session exits due to an error, its status is "Failed". If an orchestration session exits as a result of the `exitOrchestration` command, its status is "Terminated".

The Classloader Analysis Tool (CAT) is a Web-based class analysis tool that simplifies filtering classloader configuration and helps in the analysis pf classloading issues, such as detecting conflicts, debugging application classpaths and class conflicts, and proposes solutions to help resolve them. Starting with 11*g* Release 10 (11.1.10), CAT is deployed to every WebLogic domain during the upgrade. For more information about the Classloader Analysis Tool, see the *Oracle Fusion Middleware Developing Applications for Oracle Weblogic Server Guide*.

9.2 Log Locations

In addition to the orchestration log file, *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*host_name*-rel12_*hosttype_timestamp*.log, the following types of log files are available:

- Upgrade Orchestrator Log File Directories
- RUP Installer Log File Directories

9.2.1 Upgrade Orchestrator Log File Directories

The following table contains a list of log directories for Upgrade Orchestrator activities. Note that the directory name, `11.12.x.0.0`, is used to represent the appropriate version of Release 12 being upgraded to. For IDM and OHS log files, the location can be configured using the `LOG_LOCATION` property, in the `IDM.properties` and `OHS.properties` files. For more information, see Update Orchestrator Properties Files.

Table 9-1 Upgrade Tasks and Related Log Files

Task Display Name and ID	Log File Location
Stopping Index Schedules and Deactivating Index Optimization (StopIndexSchedules)	• *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log
Stopping All Servers (StopAllServers)	Orchestration log files: • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_midtier_*timestamp*.log Control log file: • *APPLICATIONS_CONFIG*/lcm/logs/startstop/STOP_*date_time_hostname*.log
Setting CrashRecoveryEnbled Property to False (DisableCrashRecoveryEnabled)	• *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_midtier_*timestamp*.log
Stopping OPMN Control Processes (StopOPMNProcesses)	Orchestration log files: • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_midtier_*timestamp*.log • /u01/logs/OHS/11.12.x.0.0/orchestration/*hostname*-rel12_ohs_*timestamp*.log OPMN log file: • *APPLICATIONS_CONFIG/DOMAIN_CONFIG* Example: BIInstance/diagnostics/logs/OPMN/opmn/
Stopping Node Managers (StopNodeManager)	• *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_midtier_*timestamp*.log
Running Upgrade Readiness (During Downtime) Checks (DuringDowntimeChecks)	• *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/healthchecker/primordial_*hostname*-DuringDowntimeUpgradeReadinessHealthChecks_*timestamp*.log • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/healthchecker/midtier_*hostname*-DuringDowntimeUpgradeReadinessHealthChecks_*timestamp*.log • /u01/logs/OHS/logs/healthchecker/OHS_*hostname*-DuringDowntimeUpgradeReadinessHealthChecks_*timestamp*.log

Table 9-1 (Cont.) Upgrade Tasks and Related Log Files

Task Display Name and ID	Log File Location
Removing Conflicting Patches for Oracle Fusion Middleware Component Oracle Homes (RemoveConflictingPatches)	• *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel11_primordial_*timestamp*.log
Installing Oracle Fusion Applications LCM Tools for Oracle VM (InstallFaSaasLcmTools)	• *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log
Preparing for Oracle Fusion Applications LCM Tools for Oracle VM Upgrade (PrepareLCMToolsForOVMUpgrade)	• *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log
Applying Oracle Fusion Applications LCM Tools for Oracle VM Patches (ApplyLCMToolsForOVMPatches)	• *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log
Running RUP Lite for OVM in Offline Mode as Application User (RupLiteOvmOffline)	• APPLICATIONS_CONFIG/lcm/rupliteovm/output/logs/11.12.x.0.0/*hostname*/rupliteoffline.log
Running RUP Lite for OVM in Pre-Root Mode	• APPLICATIONS_CONFIG/lcm/rupliteovm/output/logs/11.12.x.0.0/*hostname*/ruplitepre-root.log
Running Oracle Fusion Applications RUP Installation Part 1 of 2 (RunFirstRUPInstaller)	Orchestration log file: • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel11_primordial_*timestamp*.log Oracle Fusion Applications Patch Manager log file: • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/RUP/fapatch_*timestamp*.log
Running RUP Lite for Domain Configuration (RunRUPLiteForDomainsConfig)	Orchestration log file • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_midtier_*timestamp*.log RUPLite for Domain Config log file: • *APPLICATIONS_CONFIG*/lcm/admin/11.12.x.0.0/fapatch/ruplitedomain/output/logs
Starting Node Managers (StartNodeManager)	Orchestration log file: • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_midtier_*timestamp*.log Oracle Fusion Applications Control log file: • *APPLICATIONS_CONFIG*/lcm/logs/startstop_saas/STOP_*timestamp*_*hostname*.log

Table 9-1 (Cont.) Upgrade Tasks and Related Log Files

Task Display Name and ID	Log File Location
Starting OPMN Control Processes (StartOPMNProcesses)	Orchestration log files: • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_midtier_*timestamp*.log • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_ohs_*timestamp*.log
Running Oracle Fusion Applications RUP Installation Part 2 of 2 (RunSecondRUPInstaller)	Orchestration log file: • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log Oracle Fusion Applications Patch Manager log file: • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/RUP/fapatch_*timestamp*.log
Invoking an Instance of UpdateSOAMDS SOA Composite (UpdateMDSSOAComposite)	• *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log
Preparing for Oracle Fusion Applications WebTier Upgrade (CopyWebtierUpgradeToCentralLoc)	• *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log
Stopping Oracle Fusion Applications - APPOHS (StopOPMNProcesses)	Orchestration log files: • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_midtier_*timestamp*.log • /u01/logs/OHS/11.12.x.0.0/orchestration/*hostname*-rel12_ohs_*timestamp*.log OPMN logs: • *APPLICATIONS_CONFIG/DOMAIN_CONFIG* Example: BIInstance>/diagnostics/logs/OPMN/opmn/
Removing Conflicting Patches for Oracle Fusion Applications WebTier Oracle Homes (RemoveConflictingPatches)	• /u01/logs/OHS/11.12.x.0.0/orchestration/*hostname*-rel12_ohs_*timestamp*.log
Upgrading Oracle Fusion Applications OHS binaries (UpgradeOHSBinary)	Orchestration log files: • /u01/logs/OHS/11.12.x.0.0/orchestration/*hostname*-rel112_ohs_*timestamp*.log WebGate log file: • /u01/webgate/*hostname*/webgate_installer_REL9/output/logs/*hostname*/rupliteohsupgradeohsbinary_*timestamp*.log

Table 9-1 (Cont.) Upgrade Tasks and Related Log Files

Task Display Name and ID	Log File Location
Upgrading Oracle Fusion Applications OHS Configuration (UpgradeOHSConfig)	Orchestration log files: • `/u01/logs/OHS/11.12.x.0.0/orchestration/hostname-rel12_ohs_timestamp.log` RUP Lite log file: • `/u01/webgate/hostname/webgate_installer_REL12/output/logs/hostname/backupupgradeohsconfig/rupliteohsupgradeohsconfig_timestamp.log`
Running RUP Lite for BI (RunRUPLiteForBI)	• `APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/orchestration/hostname-rel12_midtier_timestamp.log`
Running RUP Lite for OVM in Online Mode as Application User (RupLiteOvmOnline)	• `APPLICATIONS_CONFIG/lcm/rupliteovm/output/logs/11.12.x.0.0/hostname/rupliteonline.log`
Setting CrashRecoveryEnabled Property to True (EnableCrashRecoveryEnabled)	• `APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/orchestration/hostname-rel12_primordial_timestamp.log` • `APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/orchestration/hostname-rel12_midtier_timestamp.log`
Running Post Upgrade Health Checks (PostUpgradeChecks)	• `APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/healthchecker/primordial_hostname-PostUpgradeHealthChecks_timestamp.log` • `/u01/logs/OHS/logs/healthchecker/OHS_hostname-PostUpgradeHealthChecks_timestamp.log` • `APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/healthchecker/midtier_hostname-PostUpgradeChecks_timestamp.log` • `APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/healthchecker/primordial_hostname-GeneralSystem_timestamp.log` • `APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/healthchecker/midtier_hostname-GeneralSystem_timestamp.log`
Running Data Quality Checks (DataQualityChecks)	• `PRIMORDIAL_hostname-DataQualityChecks_timestamp.log`
Running Post Upgrade Cleanup Tasks (PostUpgradeCleanup)	• `APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/orchestration/hostname-rel12_primordial_timestamp.log`
Installing binaries for Incremental Provisioning (InstallIpBinary)	• `APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/orchestration/hostname-rel12_primordial_timestamp.log`
Generating silent response files for Incremental Provisioning (GenerateSilentIpResponseFiles	• `APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/orchestration/hostname-rel12_primordial_timestamp.log`

Table 9-1 (Cont.) Upgrade Tasks and Related Log Files

Task Display Name and ID	Log File Location
Running Incremental Provisioning Manually (RunIncrementalProvisioning Manually)	Orchestration log file: • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log Incremental Provisioning log file: • *APPLICATIONS_CONFIG*/provisioning/logs/provisioning/*HOSTNAME*/ Provision Plan file: • *APPLICATIONS_CONFIG*/provisioning/plan
Upgrading All Installed Languages (LanguagePackInstall)	• *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log
Stopping All Servers (StopServersAfterLP)	• *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_midtier_*timestamp*.log
Starting All Servers (StartSeversAfterLP)	• *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_primordial_*timestamp*.log • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/orchestration/*hostname*-rel12_midtier_*timestamp*.log
Running Post Language Pack Health Checks (PostLangPackChecks) - This task calls both general system and post LP upgrade checks	• *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/healthchecker/primordial_*hostname*-GeneralSystemHealthChecks_*timestamp*.log • *APPLICATIONS_CONFIG*/lcm/logs/11.12.x.0.0/healthchecker/primordial_*hostname*-PostLanguagePackHealthChecks_*timestamp*.log

9.2.2 RUP Installer Log File Directories

The following table contains a list of log directories for RUP Installer activities:

Table 9-2 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/11.12.x.0.0/RUP	Top level directory for RUP Installer logs. Only the messages that indicate that a configuration assistant started and the result of its processing, such as success or error, are written to this log file.
APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/RUP/ARCHIVE/*timestamp*	Top level log directory where log files are moved when retrying the installation session.

Table 9-2 (Cont.) Log Directories for RUP Installer Activities

Log directory name	Description
APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/RUP/configlogs	Top level log directory for configuration assistants. A log file exists for each configuration assistant. All messages that are generated during the configuration assistant processing are written to this log file.
APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/RUP/PatchManager_DBPatch	Database upload configuration assistant logs after failure or completion. For more information, see Troubleshoot Loading Database Components.
APPLICATIONS_BASE/instance/BIInstance/diagnostics/logs	Oracle Business Intelligence logs.
APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/RUP/StartStop	StartStop utility logs. 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/11.12.x.0.0/RUP/soalogs	SOA artifacts configuration assistant logs. 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 SOA Composite Log Files.
APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/RUP/PatchManager_DownloadedPatches	Applying Downloaded Patches configuration assistant logs.

9.3 Monitor Upgrade Orchestration Progress

It is possible to track the progress of the upgrade by monitoring the console output that shows processes running on the primordial host and also open another session that tails the logs for the other servers. It is also possible to monitor the progress of the upgrade using the following methods:

- Use the getStatus Command to Monitor the Upgrade
- Use the report Command to Monitor the Upgrade
- Receive Email Notifications for Upgrade Task Failures

9.3.1 Use the getStatus Command to Monitor the Upgrade

To get the upgrade status for that host or for other hosts, run the `getStatus` command on any host as follows:

```
Retrieve the status of all tasks in a phase
./orchestration.sh getStatus -pod fcsm -hosttype PRIMORDIAL -hostname host_name -
release 11.12.x.0.0 -phase predowntime
```

```
Retrieve all tasks with a specific status
./orchestration.sh getStatus -pod fscm -hosttype PRIMORDIAL -hostname host_name -
release 11.12.x.0.0 -taskstatus success

Retrieve all tasks with a specific status
./orchestration.sh getStatus -pod fscm -hosttype PRIMORDIAL -hostname host_name -
release 11.12.x.0.0 -taskid HostTypeValidatePlugin
```

Table 10-3 displays a complete list of options for the `orchestration.sh getStatus` command.

9.3.2 Use the report Command to Monitor the Upgrade

The report command generates a report, in both HTML and XML formats, that provides information about the percentage of the upgrade that is complete. It can also inform of any processes that may be hanging. The command follows:

```
(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh report -pod comma_separated_list_of_POD_NAMES -release
release_version
```

9.3.3 Receive Email Notifications for Upgrade Task Failures

If any upgrade tasks fail, the Fusion Applications Orchestration Report is generated and mailed as an attachment to the user specified in the `EMAIL_TO_RECIPIENT` and `EMAIL_CC_RECIPIENT` properties in the `pod.properties` file. For more information, see Oracle Fusion Applications Orchestration Report. For information about troubleshooting failures, refer to the appropriate section in Monitor and Troubleshoot the Upgrade to resolve the issue. After a failure, restart Orchestrator on the host where it failed, using the same commands used in Run Upgrade Orchestrator During Downtime.

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** configuration assistant in RUP Installer fails, an email notification is received 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 listed in Database Worker Fails While Loading Database Components.

9.4 Terminate Upgrade Orchestration

Orchestration can be terminated on all hosts under scenarios that require the issue of an exit command across the entire environment. It may be needed 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, for example.

This section describes the commands used to manage the termination of orchestration on all hosts in the following topics:

- Terminate an Orchestration Session
- Clear the Exit Status on All Hosts

- Get the ExitOrchestration Status

9.4.1 Terminate an Orchestration Session

The following 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:

```
cd /ORCH_LOCATION/bin
./orchestration.sh exitOrchestration –pod POD_NAME –hosttype host_type
```

The `hosttype` argument must match the host from which this command is issued. Upgrade Orchestrator sends a notification after all hosts exit from orchestration. After this notification is received, run the command to clear the exit status on all hosts, as described in Clear the Exit Status on All Hosts. If this notification is not received on a timely basis, the status of the request can be found by running the command described in Get the ExitOrchestration Status.

From the time `exitOrchestration` is issued, until `clearExitOrchestration` is issued, only the `getExitOrchestrationStatus` command can be issued on the `pod`. Additionally, `exitOrchestration` can be issued from any host but is applicable for all the hosts in an environment.

9.4.2 Clear the Exit Status on All Hosts

After the notification that confirms all hosts exited from orchestration is received, run the following command to clear the exit status on any individual host for the entire pod:

```
cd /ORCH_LOCATION/bin
./orchestration.sh clearExitOrchestration -pod POD_NAME –hosttype host_type
```

After this command runs, users can continue with the upgrade or take other appropriate actions on the pod.

9.4.3 Get the ExitOrchestration Status

While the `exitOrchestration` command is running, run the `getExitOrchestrationStatus` command to retrieve the status of the `exitOrchestration` command as follows:

```
cd /ORCH_LOCATION/bin
./orchestration.sh getExitOrchestrationStatus –pod POD_NAME
```

9.5 Cancel the Upgrade and Restore From Backup

To cancel the upgrade and to restore the system, first terminate orchestration by following the steps in 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. Remove checkpoint locations.

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`

If these configured directories are shared among multiple instances, then orchestration creates *`POD_NAME`* sub directories. As part of the above cleanup, delete the `POD` specific directories and their contents.

Run the following commands to remove any checkpoint location and its contents:

```
rm -rf ORCHESTRATION_CHECKPOINT_LOCATION/POD_NAME/*
rm -rf ORCHESTRATION_CHECKPOINT_ARCHIVE_LOCATION/ARCHIVE/POD_NAME/*
```

2. Update the *`APPLICATIONS_CONFIG`*`/instance/nodemanager/*/nodemanager.process.lck` file from read only access to read and write access. Starting servers fail if the nodemanager.process.lck file is not updated.
3. Run the following command:

   ```
   perl updateNMProperties.pl -appBase APPLICATIONS_BASE  -postUpgrade [-verbose]
   ```

   The `updateNMProperties.pl` script is located in the *`REPOSITORY_LOCATION`*`/installers/farup/Disk1/upgrade/bin` directory.
4. Follow the steps in the Restore Data Under the Root Node of the OPSS Security Store section, if applicable.
5. Remove or rename IDM upgrade checkpoint folders when a `POD` is restored to backup. If a checkpoint file is present, orchestration skips the steps that are updated in the checkpoint file. If there is not a need to delete the checkpoint files, re-name the checkpoint files with a .bak extension, or move them to a backup folder.

   From the OIM and AUTHOHS nodes, remove the contents of `/u01/logs/checkpoint`. Note that OID and OIM share the same `/u01` file system, so there is no need to delete `/u01/logs/checkpoint` on the OID node. The checkpoint files are named `checkpoint_11.12.x.0.0_`*`nodename_hostname`*`.txt`.

9.6 Troubleshoot Upgrade Orchestrator Failures

The following specific troubleshooting scenarios are described in this section:

- Unable to Upload Orchestration Checkpoint Location
- Upgrade Orchestrator Hangs
- Unable to Find the Orchestration 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 Orchestration Failure
- Upgrade Orchestrator Does Not Use a Value in the Properties File
- Stale NFS File Handle Error

9.6.1 Unable to Upload Orchestration Checkpoint Location

Problem

When orchestration is relaunched for any reason, there could be an error uploading 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/
11.12.x.0.0/orchestration/bin/../checkpoint.
Corrective Action: Remove any existing files from older Orchestration run in /
fsnadmin/upgrade/fusionChangeOps/11.12.x.0.0/orchestration/bin/../checkpoint
before you proceed.
```

Solution

Perform the required corrective action suggested in the error message and then resume orchestration to proceed with the upgrade.

9.6.2 Upgrade Orchestrator Hangs

Problem

Orchestration hangs during the `preDowntime` or `downtimeFA` phase, or there is a need to exit Upgrade Orchestrator in the middle of an upgrade for any valid reason. If Upgrade Orchestrator hangs, it sends an email with a subject of "ALERT: *`POD_NAME`* : Orchestration on *`host_type host_name`* could potentially be hung." The email includes the cause of the hang and the log file location.

Solution

If orchestration results in any hanging tasks on any host, do not use ctrl-C or ctrl-Z to exit. Follow the steps in Terminate Upgrade Orchestration. It is possible to run these commands from another console, on any host in the pod, to gracefully exit orchestration. The `exitOrchestration` command terminates the upgrade on all hosts. Therefore, after resolving the issue that caused the hanging task, resume orchestration on all hosts where orchestration was previously running.

9.6.3 Unable to Find the Orchestration Report After Failure

Problem

After Upgrade Orchestrator fails, the console reports the following example information:

```
Fusion Applications Orchestration Report:
/u01/orchestration/orchreports/
FAOrchestrationReport_release_hosttype_hostname_timestamp.html
```

This html file does not exist in the `/u01/orchestration/orchreports` directory.

Solution

As the upgrade progresses, the Orchestration report is archived after the failure or completion of each task. Find the output in the following directory, based on the example:

`/u01/orchestration/orchreports/ARCHIVE/release/timestamp/FAOrchestrationReport_release_hosttype_hostname_timestamp.html`

9.6.4 Orchestration Fails to Generate Report With an Out Of Memory Error

Problem

Upgrade Orchestrator fails while generating the Orchestration 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
```

9.6.5 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_NAME/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.

9.6.6 Phase in Error Status, All Tasks Were Successful

Problem

The `updateStatus` command was run to manually set the status of a failed `task_id` on the primordial host to "success" during the `DowntimePostFA` phase, for example. After resuming orchestration on the IDM host, it fails with the following error:

```
Wait for peer phase: PRIMORDIAL:DowntimePostFA on host.mycompany.com
Found peer phase: PRIMORDIAL:DowntimePostFA on host.mycompany.com Error.
```

The results of `getStatus` on the pod shows that all tasks were successful but the `DowntimePostFA` 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.

9.6.7 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. Then resume Upgrade Orchestrator.

Upgrade Orchestrator supports only the following status transitions:

- Error to Success
- Running to Error
- ManualStep to Success
- Success to Error

9.6.8 Emails Are Not Being Sent Upon Orchestration Failure

Problem

The emails that Upgrade Orchestrator sends upon failure are not being received.

Solution

Perform the following steps to check if the mail server is configured properly:

1. Run the following command:

   "echo hello | /usr/sbin/sendmail *email_address*"

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 11-1.

9.6.9 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 the properties file was updated after launching Upgrade Orchestrator, follow the steps to safely exit orchestration in Upgrade Orchestrator Hangs and then relaunch orchestration. Upgrade Orchestrator reads property file values only before launching.

9.6.10 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, search for mount point in Upgrade Orchestrator Properties Files.

9.6.11 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.AuditStoreDataManager
searchFilterPresets
```

Solution

This error can be ignored.

9.6.12 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/.nfs00000000015595b30000004b': Device or resource busy

Oracle Fusion Applications Release Upgrade Orchestration failed.
```

Solution

Remove the file that is causing the error and restart Upgrade Orchestrator.

9.6.13 Unable to Initialize the Checkpoint System

Problem

During orchestration, a process can fail when the checkpoint system cannot be initialized, and the following error message is reported:

```
Failed to load prevayler under path_for_snapshot: Chunk header corrupted in the log file.
```

Solution

Perform the following steps to resolve this issue:

1. Review the log file to ensure there is no "out of disk space" exception.
2. If there is no "out of disk space" exception, restart orchestration on the host where the failure occurred. If there is an "out of disk space" exception, ensure there is enough disk space and then restart orchestration.

9.6.14 BackupOPSS Plug-In Fails

Problem

Orchestration fails when running the `BackupOPSS` plug-in, which backs up the OPSS Security Store, with the following error:

```
ORCH-DOWNTIME-00001 : Plugin Failed with error.
Please enter bind password:
ldap_search: No such object
```

This error occurs because the OPSS Security Store assumes that `jpsroot` is `FAPolicies`.

Solution

If the `jpsroot` is not `FAPolicies`, the workaround is to back up the OPSS Security Store manually. To back up all data under the root node of the OPSS Security Store and to back up the bootstrap wallet, perform the following steps:

Ensure the backups are performed in directories from which they can be restored. Use any directory to back up the data, as long the location from where to restore the backup is known.

1. Using Fusion Applications Control, perform the following steps to identify the root node in the Oracle Internet Directory that hosts the OPSS Security store:
   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 the case of an upgrade failure, restore this entire node.

2. Perform the following `ldifwrite` and `bulkload` operations 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:

   a. Set the following environment variables:

   ```
   (Unix)
   setenv ORACLE_HOME  OID_ORACLE_HOME
   setenv ORACLE_INSTANCE  OID_INSTANCE_HOME
   ```

   For example:

   ```
   (Unix)
   setenv ORACLE_HOME /u01/oid/oid_home
   setenv ORACLE_INSTANCE /u01/oid/oid_inst
   ```

   b. Create the backup in the *SHARED_UPGRADE_LOCATION/POD_NAME/release/* directory as follows:

   In the system where the Oracle Internet Directory is located, produce an LDIF file by running `ldifwrite` as illustrated in the following command. The Operational Data Store (ODS) password is required.

   ```
   OID_HOME/ldap/bin/ldifwrite connect="srcOidDbConnectStr"
   basedn="cn=FAPolicies", "c=us" ldiffile="srcOid.ldif"
   ```

   For 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.

   c. Perform the following steps if there is a need to restore the backup:

      i. Ensure Oracle Internet Directory is up and running.

      ii. Perform a `bulkdelete` on Oracle Internet Directory nodes.

      iii. 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.

      iv. Load data into the Oracle Internet Directory by running `bulkload` as shown in the following command:

      ```
      OID_HOME/ldap/bin/bulkload connect="dstOidDbConnectStr" load=true
      file="fullPath2SrcOidLdif"
      ```

3. Back up the `cwallet.sso file` in the *DOMAIN_HOME*/`config/fmwconfig/bootstrap` directory for **each WLS domain** in an Oracle Fusion Applications installation. Take backups of each `cwallet.sso` file for each domain and when restoring, be careful to

restore the correct file. For example, `cwallet.sso` is backed up from the Common Domain, then restore it in the Common Domain upon failure. If `cwallet.sso` is backed up from the BI domain, restore it to the BI Domain upon failure.

4. Resume orchestration to proceed with the upgrade.

9.6.15 Database Credential Store Retrofit Utility or CSF Cache Utility Fails

Problem

The Database Credential Store Retrofit Utility or CSF Cache Utility steps fail. Sometimes, these steps fail because of a case mismatch in the value of the db unique name when compared between the value you get from the table (`V$DATABASE`) and the one listed in the `oratab` file on the db host.

Solution

To resolve this issue, perform the following steps:

1. Check the result of the following SQL:

   ```
   SELECT DB_UNIQUE_NAME FROM V$DATABASE
   ```

2. If the result value is all lower case, ignore the next step.
3. If the value is all upper case or mixed case, replicate the case in the `/etc/oratab` file exactly as seen in `DB_UNIQUE_NAME FROM V$DATABASE`.
4. After the upgrade, revert the changes.

9.7 Troubleshoot RUP Installer Failures

This section provides information about the following RUP Installer failures:

- RUP Installer Fails
- Automatic Retry for Failed Configuration Assistants
- Pre-copy Phase of RUP Installer Fails
- RUP Installer Fails Due To Thread Calls
- Recover From an Installer Session That Was Shut Down
- Applying Pre-PSA Middleware Patches Fails for fusionbhd Component (Solaris Only)
- Applying Online BI Metadata Updates Reports a JPS Exception
- Generating OHS Reference Configuration File Configuration Assistant Fails
- Applying Admin Server Online Setting and Configuration Changes Fails
- RUP Installer 2 Fails While Starting Servers

9.7.1 RUP Installer Fails

RUP Installer runs numerous configuration assistants and is the primary utility called by Upgrade Orchestrator. In the case of a failure while RUP Installer is running, refer to information in General Troubleshooting for Upgrade Orchestrator Failure applies. In

addition to the Oracle Fusion Applications Orchestration Report and the log location, the RUP Installer Report location is also included as part of the notification that is sent. For more information, see Review the Post RUP Installer Report. For information about specific configuration assistants, see RUP Installer Configuration Assistants.

9.7.2 Automatic Retry for Failed Configuration Assistants

Most configuration assistants are configured to automatically retry after a failure. The default number of retries is three times and the default wait time between retries is two minutes. After ten minutes, no further retries are attempted. When reviewing log files after a failure, the number of retry attempts is indicated by "Autoretrying attempt "{0}" of "{1}".

9.7.3 Pre-copy Phase of RUP Installer Fails

Problem

The pre-copy phase of RUP installer fails, causing the installer to terminate.

Solution

To resolve this failure during the first RUP Installer, perform the following steps:

1. Open the `checkpoint.xml` file located in the *`central_inventory_location`*`/checkpoint/farup1/`*`version`*`/` directory.
2. Edit the following line in the checkpoint file:

   ```
   <module name="install" type="install" status="Success">
   ```

   Update the value for status as follows:

   ```
   <module name="install" type="install" status="Config">
   ```

To resolve this failure during the second RUP Installer, perform the following steps:

1. Open the `checkpoint.xml` file located in the *`central_inventory_location`*`/checkpoint/fusionapps/`*`version`*`/` directory.
2. Edit the following line in the checkpoint file:

   ```
   <module name="install" type="install" status="Success">
   ```

   Update the value for status as follows:

   ```
   <module name="install" type="install" status="Config">
   ```

9.7.4 RUP Installer 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 RUP Installer by resuming Upgrade Orchestrator.

9.7.5 Recover 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 the backup of *APPLICATIONS_BASE* and start from the beginning of the upgrade.

9.7.6 Applying Pre-PSA Middleware Patches Fails for fusionbhd Component (Solaris Only)

Problem

In Solaris platforms, the 1st RUP installer configuration assistant "Apply Pre-PSA Middleware Patches" fails with the following `java.library.path` setting error `opatch disablecas` operation for the `fusionbhd` component:

```
[2017-07-22T15:03:59.188+00:00] [log] [NOTIFICATION] []
[ApplyPrePSAMiddlewarePatches2017-07-22_02-57-35PM.log] [tid: 1] Job  validation
successful, setting the req env to run the job...
[2017-07-22T15:03:59.188+00:00] [log] [NOTIFICATION] [PAPUTL020]
[ApplyPrePSAMiddlewarePatches2017-07-22_02-57-35PM.log] [tid: 1] Executing  the
command [<APPLTOP>/fusionbhd/OPatch/opatch disablecas  -oh <APPTOP>/fusionbhd -jre
<APPLTOP>/fusionapps/jdk]
[2017-07-22T15:03:59.188+00:00] [log] [NOTIFICATION] []
[ApplyPrePSAMiddlewarePatches2017-07-22_02-57-35PM.log] [tid: 1] Oracle Home  is:
<APPLTOP>/fusionbhd
The java.library.path system variable is missing or invalid. Please set
java.library.path with a correct value and retry the operation.
```

Solution

To resolve this issue, perform the following steps:

1. Backup `<APPLTOP>/fusionbhd/oui/oraparam.ini`.
2. Append `-d64` to the `JRE_MEMORY_OPTIONS` in `<APPLTOP>/fusionbhd/oui/oraparam.ini` as shown in the following example:

   ```
   JRE_MEMORY_OPTIONS=" -d64 -mx512m -XX:MaxPermSize=256m"
   ```

3. Rerun Orchestration.

9.7.7 Applying Online BI Metadata Updates Reports a JPS Exception

Problem

The **Applying Online BI Metadata and Configuration Updates** configuration assistant reports the following JPS exception:

```
oracle.security.jps.JpsException: JPS-01016: A password credential is expected;
instead found null for alias AuditDbPrincipalMap and key AuditDbPrincipalKey at
location
/u01/APPLTOP/instance/domains/bi.oracleoutsourcing.com/BIDomain/config/fmwconfig/
bootstrap.
```

Solution

This exception has no functional impact on the upgrade and can be ignored.

9.7.8 Generating OHS Reference Configuration File Configuration Assistant Fails

Problem

The RUP configuration assistant "Generating OHS Reference Configuration File" fails initially while processing the context root metadata files from FMW. For example, the files under `/APPTOP/fusionapps/applications/lcm/common/fmwohs`.

Solution

To resolve this issue, perform the following steps:

1. In the `/APPTOP/oraInventory/checkpoint/farup/<RELEASE_VERSION>/checkpoint.xml` checkpoint file, find the following:

```
<aggregate name="Generating OHS Reference Configuration File" status="fail"
 progress="97">
           <property name="OHS27"
value="/scratch/mwport/REL8FA/APPTOP/fusionapps/applications/lcm/common/fmwohs

/soa.modwl.conf.xml"/>
          ..............
          ..............
          <property name="OHS12"

value="/scratch/mwport/REL8FA/APPTOP/fusionapps/applications/com/deploy/scmExt

 ernalUriAdf.xml"/>
</aggregate>
```

   And then, replace it with the following:

```
<aggregate name="Generating OHS Reference Configuration File" status="success"/>
```

2. Rerun orchestration.

9.7.9 Applying Admin Server Online Setting and Configuration Changes Fails

Problem

The RUP Installer configuration assistant "Applying Admin Server Online Setting and Configuration Changes" fails with the following error message:

```
[2017-09-01T07:06:17.166+00:00] [apps] [ERROR] []
[oracle.apps.ad.rupconfig.Applying_Admin_Server_Online_Setting_and_Configuration_Chan
ges] [tid: 32] [ecid: 0000LswBvjR7y0I_IpP5if1PeG7o000006,0] CFGEX-00024 : Config
plugin "Updating JPS Config Timeout Settings" failed. No further plugins will be run.
```

Solution

This error message is expected when upgrading from release 8 or 9 directly to release 12. It does not cause any functional impact and you can skip this failed task and continue with upgrade.

To resolve the issue, perform the following steps:

1. Make a copy of the check point xml file:

   ```
   cp checkpoint.xml checkpoint.xml.orig
   ```

2. In the `/APPTOP/oraInventory/checkpoint/farup/<RELEASE_VERSION>/checkpoint.xml` checkpoint file, find the following:

   ```
   <property name="Updating JPS Config Timeout Settings" value="Failed"/>
   ```

   And then, replace it with the following:

   ```
   <property name="Updating JPS Config Timeout Settings" value="Success"/>
   ```

3. Save the `checkpoint.xml` file and resume the upgrade.

9.7.10 RUP Installer 2 Fails While Starting Servers

Problem

In Release 8 to Release 12 upgrades, RUP Installer 2 fails while starting all servers with the following error:

```
ERROR: CFGLOG-00104 : "Starting All Servers" configuration failed.
ERROR: CFGLOG-00175 : Startup of server
"BIInstance~coreapplication_obisch1~OracleBISchedulerComponent~coreapplication_obisch
1" in domain "BIDomain" "failed".
ERROR: CFGLOG-00175 : Startup of server
"BIInstance~coreapplication_obis1~OracleBIServerComponent~coreapplication_obis1" in
domain "BIDomain" "failed".
ERROR: CFGLOG-00175 : Startup of server
"BIInstance~coreapplication_obiccs1~OracleBIClusterControllerComponent~BIClusterContr
oller" in domain "BIDomain" "failed".
ERROR:
oracle.as.install.fapatchconfig.exception.PatchsetConfigException:CFGEX-00069 :
Startup failed for following domain:server pairs"
[BIDomain:BIInstance~coreapplication_obisch1~OracleBISchedulerComponent~coreapplicati
on_obisch1,
BIDomain:BIInstance~coreapplication_obis1~OracleBIServerComponent~coreapplication_obi
s1,BIDomain:BIInstance~coreapplication_obiccs1~OracleBIClusterControllerComponent~BIC
lusterController]".
```

Solution

To resolve this issue, perform the following steps from the BI host:

1. Execute the following BI ruplite:

   ```
   java -jar $BIOH/biapps/tools/lib/biruplite.jar  $BODOMAIN_HOME $BIOH false
   ```

   For example:

```
/slot/ems16838/appmgr/APPTOP/fusionapps/jdk/bin/java -jar
/slot/ems16838/appmgr/APPTOP/fusionapps/bi/biapps/tools/lib/biruplite.jar
/slot/ems16522/appmgr/APPTOP/instance/domains/slcah751.us.mycompany.com/BIDomain
/slot/ems16838/appmgr/APPTOP/fusionapps/bi false
```

2. Add the [opss-DBDS] section to `$BIInstance/bifoundation/OracleBIApplication/coreapplication/setup/odbc.ini`. Refer to the `BIShared` file at `BIShared/Essbase/essbaseserver1/bin/.odbc.ini`.
3. Stop `BIcomponent` and the OPMN instance as follows:

   ```
   $BIInstance/bin/opmnctl stopall
   ```

4. Restart only the OPMN instance as follows:

   ```
   $BIInstance/bin/opmnctl start
   ```

5. Rerun RUP Orchestration from the Primordial host.

9.8 Troubleshoot Node Manager and OPMN failures

9.8.1 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. The 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. For more information, see Start Node Manager in the *Oracle Fusion Applications Administrator's Guide*.

9.8.2 Exception During Stopping OPMN Processes

Problem

Upgrade Orchestrator fails to stop OPMN processes with an 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 orchestration.

9.8.3 Troubleshoot 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 resolving 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 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 the Web Tier (OHS) installed with the Oracle Fusion Applications middle tier is run, it is possible to start it using the following steps. If the Web Tier is run on a separate machine, it may be possible 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 GOP is 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 Directories Structure Overview.

The BI, Web Tier, and GOP (when applicable) processes managed by OPMN are started by the installer in the **Starting All Servers** configuration assistant.

4. Fix any other environment issues before resuming the upgrade. If the 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 there are unresolved environment issues.
5. After starting the services, resume orchestration to proceed to the **Starting All Servers** configuration assistant. If the starting of servers times out, see Troubleshoot Server Start and Stop Failures.

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.`

9.8.4 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 1

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, 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 timestamp 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/11.12.x.0.0/RUP/configlogs

APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/RUP/ARCHIVE/*timestamp*/configlogs

The last time stamp entry is the execution timestamp.

Problem 2

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 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.>`

9.8.5 The StopOPMNProcesses Plug-in Fails on the OHS Node

Problem

The following error occurs on the OHS node:

```
[Plugin failed]: StopOPMNProcesses
[Phase DowntimePostFA]: failed

ORCH-DOWNTIME-OPMN-00004 : Stopping OPMN Control Process failed. Review log file
```

Solution

This error can occur when OHS is on the same node as the primordial host and *APPLICATIONS_CONFIG* is not *APPLICATIONS_BASE*/instance. For example, this error occurs if *APPLICATIONS_BASE* =/APPTOP and *APPLICATIONS_CONFIG* =/instance.

To resolve the issue, perform the following steps:

1. Create a link from *APPLICATIONS_BASE*/instance to *APPLICATIONS_CONFIG* as follows:

   `ln -s APPLICATIONS_CONFIG APPLICATIONS_BASE/instance`
2. Resume orchestration.
3. Delete the link after orchestration completes successfully.

9.9 Troubleshoot RUP Lite for OHS Failures

This section describes the following RUP Lite for OHS failures:

- RUP Lite for OHS Fails With Missing JDK exception

9.9.1 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 Orchestration.

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 Orchestration.

9.9.2 RUP Lite for OHS Fails With ReassociateCommonDomain Plug-in

Problem

During the upgrade, 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.

9.9.3 RUP Lite for OHS Fails With Security Mode Errors

Problem

RUP Lite for OHS reports a server side error occurs with the following error message:

```
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

To resolve this issue, 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.

Check the Oracle Fusion Applications OHS to ensure that SSO still works after the change. If it does not, upgrade Webgate manually for the Oracle Fusion Applications OHS.

9.10 Troubleshoot IDM Upgrade Failures

This section describes the following troubleshooting issues:

9.10.1 Communication Exception on Primordial Console While Waiting for IDMOHS

Problem

While the primordial host is waiting for `IDMOHS:IDMUpgradeDone`, there are communication exceptions on the PRIMORDIAL console.

Solution

These errors can be ignored and orchestration can be resumed.

9.10.2 OAM Configuration Step Fails Due to Special Characters in Password

Problem

If the OAM administrator password contains special characters, such as '#' or '&', the OAM Configuration step fails. To work around this issue, manually validate that the

OAM Administration Server host/port and username/password are correct. After manually validating this information, proceed with the manual upgrade.

Solution

To validate, perform the following steps:

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 username 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. For example:

   ```
   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 orchestration can be resumed.

9.10.3 OAM Configuration Update Fails for OVD Removal

This troubleshooting step is only applicable if the OAM configuration fails while you are performing the steps to remove OVD from your environment as listed in Update OAM Configuration.

Problem

OAM configuration update fails for OID authenticator.

Solution

To resolve this issue, run following command using WLST:

```
cd  $OAM_ORACLE_HOME/common/bin
setenv DOMAIN_HOME /u01/app/idm/admin/IDMDomain/aserver/IDMDomain$DOMAIN_HOME/bin/
setDomainEnv.sh
./wlst.sh
connect('weblogic_idm','$WLS_ADMIN_PASSWORD','t3://myhost.example.com:7001')
editUserIdentityStore(name="OIMIDStore", ldapUrl="ldap://idstore.example.com:
```

```
3060", ldapProvider="OID", userSearchBase="cn=Users,dc=us,dc=oracle,dc=com",
groupSearchBase="cn=Groups, dc=us,dc=oracle,dc=com)
```

9.10.4 Location of GRC Policies in the OAM Applications Domain

The location of the Governance, Risk, and Compliance (GRC) policies varies, depending on the upgrade path to Release 12. GRC polices are located in the *grc* OAM application domain if the 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 the environment was originally provisioned with version 11.1.3 and upgraded to version 11.1.4 and beyond, the GRC policies are located in the *fs* OAM application domain.

9.10.5 Restore Data Under the Root Node of the OPSS Security Store

Problem

Due to a failure during the upgrade, it is necessary to restore all of the data under the root node of the OPSS Security Store.

Solution

To restore all of the data under the root node of the OPSS Security Store, perform the following steps:

1. Ensure Oracle Internet Directory is up and running.
2. Perform a `bulkdelete` on Oracle Internet Directory nodes.
3. 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.
4. 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"
   ```

9.10.6 Applying One-Off Patch Fails

Problem

Applying Release12 One-Off patches on an Release 12 setup fail.

Workaround

To workaround this issue, create a symbolic link pointing to `/u01/IDMTOP` immediately after the upgrade. For example, if the real top is in `/abc/idmtop`, perform the following steps:

```
mkdir /u01
ln -s /abc/idmtop /u01/IDMTOP
```

9.10.7 Webgate Is Not configured on the OHS SO Node

If Webgate is not configured on the OHS SO Node, perform the following steps:

1. Log in to the OHS SO Node.
2. Append environment variable `LD_LIBRARY_PATH` with the Web Tier library path `APPLICATIONS_BASE/webtier_mwhome/webtier/lib` as follows:

   ```
   WEBHOST2> export LD_LIBRARY_PATH=APPLICATIONS_BASE/<webtier_mwhome>/
   <webtier_directory_name>/lib:$LD_LIBRARY_PATH
   ```

   For example:

   ```
   WEBHOST2> export LD_LIBRARY_PATH=/u01/app/idm/products/ohs/ohs/
   lib:$LD_LIBRARY_PATH
   ```

3. Execute `deployWebgateInstance.sh` as follows:

   a. Execute the following command:

   ```
   cd <WEBTIER_MW_HOME>/webgate/webgate/ohs/tools/deployWebGate
   ./deployWebGateInstance.sh -w <WEBTIER_INSTANCE_HOME>/config/OHS/ohs2/ -oh
   <WEBTIER_MW_HOME>/webgate
   ```

   For example:

   ```
   ./deployWebGateInstance.sh -w
   /u02/local/idm/config/instances/ohs2/config/OHS/ohs2/ -oh
   /u01/app/idm/products/ohs/webgate
   ```

   b. Execute the following command:

   ```
   cd <WEBTIER_MW_HOME>/webgate/webgate/ohs/tools/setup/InstallTools
   ./EditHttpConf -w <WEBTIER_INSTANCE_HOME>/config/OHS/ohs2/ -oh
   <WBETIER_ME_HOME>/webgate -o webgate.conf
   ```

   For example:

   ```
   ./EditHttpConf -w /u02/local/idm/config/instances/ohs2/config/OHS/ohs2/ -oh
   /u01/app/idm/products/ohs/webgate -o webgate.conf
   ```

   c. Copy the following from `WEBHOST1` to `WEBHOST2`:

   - From `<WEBTIER_INSTANCE_HOME>/config/OHS/ohs1/webgate/config`, copy the following to `<WEBTIER_INSTANCE_HOME>/config/OHS/ohs2/webgate/config` on `WEBHOST2`:

     ```
     "ObAccessClient.xml","cwallet.sso","password.xml"
     ```

   - From `<WEBTIER_INSTANCE_HOME>/config/OHS/ohs1/webgate/config/simple`, copy the following to `<WEBTIER_INSTANCE_HOME>/config/OHS/ohs2/webgate/config/simple` on `WEBHOST2`:

     ```
     "aaa_key.pem","aaa_cert.pem"
     ```

4. Restart Oracle HTTP Server as follows:

   ```
   WEBHOST2> cd <WEBTIER_INSTANCE_HOME>/bin
   WEBHOST2> ./opmnctl stopall
   WEBHOST2> ./opmnctl startall
   ```

5. Ensure that the URLs are accessible as before, by temporarily stopping Oracle HTTP server on the Node 1 and making accessible the URLs.

9.10.8 Corrupted JAR Found

Problem

The following corrupted JAR error message is found in the migration and pre-downtime logs:

```
51fea9603f49 ,lastModified:2010-01-10T17:46:52.000-0800
,ioe:java.util.zip.ZipException: Could not find End Of Central Directory
<ERROR> Error message was found in log file on line ::2905:: -->WARNING:
corrupted jar found.
file:/u01/IDMTOP/products/app/iam/oam/server/lib/jmx/oam-dummy-config.xml,
md5sum:2c3ede41786705c57cf151fea9603f49
,lastModified:2010-01-10T17:46:52.000-0800 ,ioe:java.util.zip.ZipException:
Could not find End Of Central Directory
<ERROR> rror message was found in log file on line ::2991:: -->WARNING:
corrupted jar found.
file:/u01/IDMTOP/products/app/iam/oam/server/lib/jmx/oam-dummy-config.xml,
md5sum:2c3ede41786705c57cf151fea9603f49
,lastModified:2010-01-10T17:46:52.000-0800 ,ioe:java.util.zip.ZipException:
Could not find End Of Central DirectoryExit Value from individual subroutine
check is 1
```

Solution

Ignore the error message.

9.10.9 Migration or Upgrade Fails with Permission Issues

Problem

Migration or upgrade fails with permission issues such as unable to access or unable to write.

Solution

To resolve this issue, check the failed file's user and group privileges and permissions of the `stagedir` and `idmUpgrade` folders. The user and group permissions should be same as the user who is running the upgrade. In addition, all of the folders need to be writable.

9.10.10 OIF URL Not Accessible Post Migration

Problem

The OIF URL is not accessible post migration.

Solution

To resolve this issue, perform the following steps:

1. Bring down all servers.
2. Clean up the `tmp` folders of all the servers in both shared config (`/u01/IDMTOP/config`) and local config (`/u02/local/IDMTOP/config`).
3. Restart the servers and check the OIF URL.

9.10.11 Download Email Template from OIM Fails

Problem

Download email template from OIM fails in Run Upgrade Orchestrator During Downtime.

Solution

This is an expected failure. The Download email template step is executed again as part of the IDM upgrade in Manually Download OIM Email Template.

9.10.12 SOA Server Fails to Start on Scaled Out Machine During Migration

Problem

The SOA managed server fails to start on the scaled out machine with the following exception in the SOA logs under `/u01/IDMTOP/config/scripts/logs`:

```
Starting server wls_soa2 ...Access to domain 'IDMDomain' for user 'admin' denied
No stack trace available.
```

Solution

To resolve this issue, perform the following steps:

1. Execute the `nmEnroll` WSLT command as follows:

   ```
   nmEnroll('/u02/local/IDMTOP/config/domains/IDMDomain',
   '/u01/IDMTOP/config/nodemanager/<IDMSOHOSTNAME>');
   ```

   Where

   - `<IDMSOHOSTNAME>`: The secondary/scaled out machine host name.

   For more information about the execution of the `nmEnroll` command, see Oracle WebLogic Server 12c: Configuring and Using Node Manager.

2. After the successful execution of the `nmEnroll` command, rerun migration on the SOA scaled out node.

9.10.13 OIM Binary Upgrade Fails in Type II Upgrade

Problem

OIM binary upgrade fails with no "`IDMTOP/products/app/utils/orainst.loc`" error.

One possible cause is that you may be using the `upgradeOnPremise.properties` under the `idmUpgrade` folder for upgrade rather than the one under `stagedir`. For type II upgrades, `upgradeOnPremise.properties` is auto-generated by the discovery tool during discovery execution by seeding necessary values for upgrade.

Solution

To resolve this issue, rerun upgrade using the `upgradeOnPremise.properties` under `stagedir`.

9.10.14 Migration Fails To Stop the Processes and Restart in Type II Upgrade

Problem

Migration exits with an error to stop the processes and restart.

Solution

Either the source servers or components are not stopped or some stale processes related to source environment exist. To resolve this issue, perform the following steps:

1. Check the migration logs for details on those processes, and then stop them.
2. Restart migration.

9.11 Troubleshoot 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 Middleware Patchsets Fails Due to DISPLAY
- Applying Post-PSA Middleware Patches Hangs
- Applying Database Client Patches Fails
- ORA-01658: unable to create INITIAL extent for segment in tablespace
- Troubleshoot Upgrading Middleware Schema

9.11.1 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/11.12.x.0.0/RUP/
ApplyPrePSAMiddlewarePatchestimestamp.log

APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/RUP/
ApplyPostPSAMiddlewarePatchestimestamp.log
```

For Language Pack failures, review the following log files:

- Failures during Install mode and Standalone LP installation:
  `APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/LanguagePack/language/FAPatchManager_ApplyMWLangPackPatchestimestamp.log`
- Failures during LP upgrade through orchestration (configuration mode):

```
APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/LanguagePack/MergedLPs/
FAPatchManager_ApplyMWLangPackPatchestimestamp.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.

9.11.2 Applying Middleware Patchsets Fails Due to DISPLAY

Problem

The **Applying Middleware Patchsets** configuration assistant fails with an error as shown in the following example:

```
[as] [ERROR] [] [oracle.as.install.engine.modules.presentation] [tid: 15]
[ecid: 0000JsNJml6AxGGpIww0yf1HRacu000006,0] sun/awt/X11GraphicsEnvironment[[
.
java.lang.NoClassDefFoundError: sun/awt/X11GraphicsEnvironment
        at java.lang.Class.forName0(Native Method)
```

Solution

Unset the DISPLAY variable or set it to the correct value. To unset it, run "`unset/unsetenv DISPLAY`" on all hosts. Then resume Upgrade Orchestrator.

9.11.3 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. Resolve this issue by following the steps in Troubleshoot Loading Database Components. Run the commands from *ATGPF_ORACLE_HOME* instead of *FA_ORACLE_HOME*.

9.11.4 Applying Database Client Patches Fails

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.

To resolve this issue, perform the following steps:

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` as shown in the following example:

   ```
   <!-- <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>
   ```

9.11.5 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.

9.11.6 Troubleshoot Upgrading Middleware Schema

This section contains the following topics:

- Log Files for Upgrading Middleware Schema
- Upgrading SES Component Fails When TDE Data Vault is Enabled

9.11.6.1 Log Files for 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/psa`*`timestamp`*`.log`

9.11.6.2 Upgrading SES Component Fails When TDE Data Vault is Enabled

Problem

The **Upgrading Middleware Schema** configuration assistant fails while upgrading SES component when TDE Data Vault is enabled. The following error is reported:

```
[RCU] [TRACE] [] [upgrade.RCU.jdbcEngine] [tid: 10] [ecid:
0000K8DIf5l9xWR5IZL6if1ISVu^000000,0] Driver: oracle.jdbc.driver.OracleDriver
[2013-10-31T06:54:31.536+00:00] [RCU] [TRACE] [] [upgrade.RCU.jdbcEngine]
[tid: 10] [ecid: 0000K8DIf5l9xWR5IZL6if1ISVu^000000,0] jdbcUrl =
jdbc:*****:thin:sys as
sysdba/*****@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=TCP)(HOST=fusion

db.*****outsourcing.com)(PORT=1616))(ADDRESS=(PROTOCOL=TCP)(HOST=fusiondb2.***
*outsourcing.com)(PORT=1616))(CONNECT_DATA=(SERVICE_NAME=fusiondb)))
```

Solution

To resolve this issue, perform the following steps:

1. Connect as searchsys.
2. DROP INDEX "SEARCHSYS"."EQ$DOC_PATH_IDX" force.
3. Execute `eq_adm.use_instance(1)`.
4. Execute `eq_ddl.create_index()`.
5. Resume orchestration.

9.12 Troubleshoot 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, it may be needed to review one or more of the log files in the following locations:

- *`APPLICATIONS_CONFIG`*`/lcm/logs/11.12.x.0.0/RUP/PatchManager_DBPatch/`
  - `FAPatchManager_apply_`*`timestamp`*`.log`
  - `adpatch_apply_`*`timestamp`*`.log`
  - `adpatch_apply_`*`timestamp_workernum`*`.log`
- *`ATGPF_HOME`*`/admin/FUSION/log`

- If the language is upgraded through orchestration, then the config mode LP logs for **Loading DB Componenets** are present in *APPLICATIONS_CONFIG*`/lcm/logs/11.12.x.0.0/RUP/PatchManager_NLS_DBPatch`.

The following troubleshooting issues are described in this section:

9.12.1 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

Find the cause of the failure by running the script manually as the `sysdba` user, using SQL*Plus or SQL*Developer. After resolving the issue, resume orchestration.

9.12.2 Database Worker Fails While Loading Database Components

Problem

An email notification stating that one or more database workers failed during the **Loading Database Components** configuration assistant is received.

Solution

This email notification is only received 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 Troubleshoot Patching Sessions for Database Content in the *Oracle Fusion Applications Patching Guide*. After resolving 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 orchestration is run with the `-DlogLevel` option set to `FINEST`.

There might be corner cases when an alert email indicating failed workers although the workers are still running might be received. In such cases, ignore the email alert after ensuring the workers are running with no failures.

9.12.3 Database Failure While Loading Database Components

Problem

The database goes down while RUP Installer is running the **Loading Database Components** configuration assistant. If simply bringing the database up and then resuming orchestration, the following error might be received:

```
Failed to connect to the database as fusion with error:
No more data to read from socket
```

Solution

To recover from this error, perform the following steps:

1. Force the database patching session to fail as follows:

   `(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh forcefail`

2. Start AD Controller as follows:

   `(UNIX) FA_ORACLE_HOME/lcm/ad/bin/adctrl.sh`

   For more information, see Start AD Controller in the *Oracle Fusion Applications Patching Guide*.

3. Perform the following 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 the operating system, check for processes that are running `fapmgr`, `javaworker`, `adpatch`, `adadmin`, `sqlplus`, and `adworker`. If any exist, terminate them from the operating system.
   f. Select **Tell worker to restart a failed job** and enter **All** for all workers.
4. Resume orchestration.

9.12.4 AutoPatch Validation Fails

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 as follows:

   `(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh 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 as shown in the following example:

   `(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh 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`

9.12.5 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 Restart a Failed Worker in the *Oracle Fusion Applications Patching Guide*.

9.12.6 Loading pje_txn_fix_issues_bug18504814.sql Fails

Problem

The upgrade script, `pje_txn_fix_issues_bug18504814.sql`, fails with the following error:

```
ORA-00001: unique constraint (FUSION.PJE_ISSUE_TYPES_TL_U1) violated.
```

Solution

Skip the AD worker that failed while running the `pje_txn_fix_issues_bug18504814.sql` file.

9.12.7 Loading DB Components Fails for CRMCOMMON MOW Tables

Problem

Upgrade fails with the following error due to **Loading Database Components** failure for Work Management (MOW) tables:

```
[2016-11-22T10:23:05.464+00:00] [xdf] [ERROR] [XDF-10567] [oracle.xdf]
[tid: 1] [ecid: 0000LY7^LAfBX7M5ING7yf1OClRT000001,0] Could not modify the column to
NOT NULL.
[2016-11-22T10:23:05.464+00:00] [xdf] [NOTIFICATION] [XDF-00005] [oracle.xdf]
[tid: 1] [ecid: 0000LY7^LAfBX7M5ING7yf1OClRT000001,0] Alter DDL: ALTER TABLE
"FUSION"."MOW_RULE_SET_DETAILS" MODIFY ("MAX_SCORE" NUMBER(9,0))
```

Solution

Ignore the error. Skip and restart the failed adworker.

9.13 Troubleshoot Deployment of Applications Policies

This section contains the following information about troubleshooting issues that may occur during the **Deploying Application Policies** configuration assistant:

- Log Files for Deploying Application Policies
- Analysis of Applications Policies Fails
- Deploying Applications Policies Fails
- Deploying Applications Policies Fails With Duplicate Permissions Warning
- Deploying Applications Policies Reports Warning "Failed to Validate XML Content"
- Warning during Migrate Security Store
- IDM Server Fails During Deployment of Applications Policies

9.13.1 Log Files for Deploying Application Policies

Log files for this configuration assistant may be found in this location:

APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/RUP/configlogs/
fapatch_Deploying_Applications_Policies_(jazn-data.xml)_*timestamp*.log

APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/LanguagePack/language/configlogs/
fapatch_Deploying_Applications_Policies_(jazn-data.xml)_*timestamp*.log

9.13.2 Analysis of Applications Policies Fails

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/11.12.0.0.0/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
- fapatch_B2BJaznAnalysis_*timestamp*.log

After resolving the JAZN analysis error, retry the analysis for the failed stripe to confirm the issue is resolved.

9.13.3 Deploying Applications Policies Fails

Problem

A failure occurs during the **Deploying Application Policies** configuration assistant.

Solution

When a failure occurs during **Deploying Application Policies**, restore only the stripe or system policy that has failed, from the 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 resolving the issue, resume orchestration. For more information, see the Migrating with the Script migrateSecurityStore section in the *Oracle Fusion Middleware Applications Security Guide*.

9.13.4 Deploying Applications Policies Fails With Duplicate Permissions Warning

Problem

The **Deploying Application Policies** configuration assistant fails with the following warning:

```
oracle.security.jps.internal.policystore.ldap.PermissionManagerImplsearchPermissionEn
try

WARNING: Duplicate permissions
```

Solution

Contact Oracle Support to request assistance in resolving this issue.

9.13.5 Deploying Applications Policies Reports Warning "Failed to Validate XML Content"

Problem

The following warning occurs during the **Deploying Application Policies** configuration assistant:

```
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

Ignore this message as there is no functional impact of this warning and the deployment is successful.

9.13.6 Warning During Migrate Security Store

Problem

The following warning occurs during the **Deploying Application Policies** configuration assistant:

```
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:933)
        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

Ignore this message as there is no functional impact of this warning and the deployment is successful.

9.13.7 IDM Server Fails During Deployment of Applications Policies

Problem

The IDM Server goes down during the **Deploying Application Policies** configuration assistant and the deployment fails.

Solution

Upgrade Orchestrator does not allow a retry after this type of failure. Instead, exit orchestration and restore from the IDM backup. Then, resume orchestration.

9.14 Troubleshoot Server Start and Stop Failures

This section includes the following troubleshooting topics:

9.14.1 Starting All Servers Fails Due to Timeout 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 takes all servers to actually start during the **Starting All Servers** configuration assistant. Although the 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 the environment requires more time than the installer allows.

If this configuration assistant fails, perform the following 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/11.12.x.0.0/RUP/StartStop/fastartstop_`*timestamp*`.log`, indicates which server started and failed to start. For example:

```
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/11.12.x.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 determining and resolving the cause of the failure, restart Upgrade Orchestrator.

9.14.2 Starting All Servers Fails due to BIServer Failure

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

To work around this issue, perform the following steps:

1. Resume orchestration, which shuts down and starts bi_server1.
2. Monitor the fastartstop log files and the state of bi_server1(BIDomain).
3. When bi_server1 restarts, as indicated by a RUNNING status, start the component coreapplication_obiccs1 or all the components of type OracleBIClusterControllerComponent using opmnctl as shown in the following example:

   ```
   */BIInstance/bin/opmnctl startproc ias-component=coreapplication_obiccs1
   ```

9.14.3 Startup Fails 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.conf, for example:
   - For Apps OHS: `"/dev/shm/ohs_ohs1_http_lock"`
   - For OSN OHS: `"/dev/shm/osn_ohs1_http_lock"`
2. Confirm whether the directory that contains the lock file exists.
3. Assuming this directory does not exist, create the directory.

9.14.4 Online Preverification Fails With EditTimedOutException

Problem

The following error is reported during Online Preverification:

```
weblogic.management.mbeanservers.edit.EditTimedOutException
```

Solution

It may be necessary to manually release the edit session. For more information, see Resolve an EditTimedOutException Error in the *Oracle Fusion Applications Patching Guide*.

9.14.5 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 the 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`.

9.14.6 WLS SocketTimeoutException During Server Startup

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.

9.14.7 The SOA-infra Application is in a Warning State

Problem

After the upgrade, the following error displays after logging in to the WLS Console of CommonDomain. and navigate to Deployments:

```
soa-infra application is in WARNING state.
```

Solution

Ignore this error as there is no functional impact for SOA users due to this error.

9.14.8 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.

9.14.9 Failure to Start or Stop a Custom Domain

Problem

The custom domains are not stopped or started by FAStartStop and there errors are reported.

Solution

`FAStartStop` does not recognize custom domains. Custom domains must be started and stopped manually, as required, before resuming orchestration.

9.15 Troubleshoot 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)
- Deploy SOA Composites Manually
- Invoke an Instance of SOA Composite
- Merge SOA Composite JDeveloper Customizations During SOA Preverification

The following documents provide additional information related to subjects discussed in this section:

- For more information about working with SOA composites, see Customizing the SOA Composite Application in the *Oracle Fusion Applications Extensibility Guide for Developers*.
- For more information about customizing SOA composites, see Customizing and Extending SOA Components in the *Oracle Fusion Applications Extensibility Guide for Developers*.

9.15.1 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/11.12.x.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`

9.15.2 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 orchestration is resumed.

The following are examples of error messages related to SOA Composite failures:

```
COMMONLOG-00049: 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.

COMMONLOG-00050: 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.

COMMONLOG-00051: 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.
```

The following is an example of report exceptions:

```
COMMONEX-00026: 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.
```

Solution

When patching existing SOA composites, RUP Installer automatically recovers any partially deployed SOA composites after failure when Upgrade Orchestrator is restarted. 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 is 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 restarting orchestration.

9.15.3 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"
```

It has been confirmed that the `wsm-pm` application is running on this domain.

Solution

To resolve this issue, 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.

9.15.4 Deploy SOA Composites Manually

If a customized SOA composite deployment fails during the upgrade, manually deploy this composite using WLST commands.

To apply a SOA composite manually after a deployment failure, perform the following steps:

The following 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`. 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 the patched revision is deployed with the merged JDeveloper customizations. Using the `sca_*.jar` file from Step 1, follow the JDeveloper customization merge instructions that are described in Merge 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 as shown in the following example:

```
sca_patchComposite('SOA-Infra URL', user, password,
'/FA_ORACLE_HOME/crm/deploy//sca_FinAprev2.0.jar', mergeLogFile='/tmp/merge-
log.txt')
```

9.15.5 Invoke an Instance of SOA Composite

Run the `UpdateSOAMDS` SOA composite on every domain if any flexfield changes were made by following the steps described in Synchronizing Customized Flexfields in the MDS Repository for SOA in the *Oracle Fusion Applications Extensibility Guide for Developers*.

9.15.6 Merge SOA Composite JDeveloper Customizations During SOA Preverification

If JDeveloper customizations were performed to a SOA composite and the composite was deployed to the SOA runtime, RUP Installer reports an error during **SOA Preverification**, which asks to take the newer version of the composite that is in the release. Then, merge the 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 the upgrade. 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".
3. Import the composite `sca_*.jar` file from *FA_ORACLE_HOME*/*stripe*/`deploy` into the project, for example revision 11.12.x.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, 11.12.x.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_rev11.12.x.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.

9.16 Troubleshoot RUP Lite for OVM Failures

This section contains the following topics:

- Troubleshooting RUP Lite for OVM Plug-in Failures
- Troubleshooting Hanging in Offline or Online Mode

9.16.1 Troubleshoot RUP Lite for OVM Plug-in Failures

Review the `APPLICATIONS_CONFIG/lcm/rupliteovm/output/logs/ruplite.log` file to confirm there are no errors. Alternatively, check rehydration framework logs under `/assemblybuilder/logs`or `/var/log` for any errors.

Review the following troubleshooting information for specific plug-ins:

- **ValidateEnvironment**: This plug-in runs during every mode of RUP Lite for OVM. If this plug-in fails, RUP Lite for OVM stops. Resolve any errors reported in the log file and then run RUP Lite for OVM again.
- **SetupCredentials:** This plug-in runs during every mode of RUP Lite for OVM. 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. Resolve any errors reported in the log file and then run RUP Lite for OVM again.

This plug-in prompts for all secure properties that are required by offline RUP Lite plug-ins. It stores these properties in a wallet file, which are encrypted using a key provided by the user. If a wallet already exists, the user provided key must be valid for the existing wallet. If the wallet does not exist, a new wallet is created using the provided key. If a secure property already exists in the wallet, then it is not prompted for again.

This plug-in prompts only for secure properties that are needed by other plug-ins that will execute. If a plug-in does not execute on the current node or is disabled, then its properties are not be requested. If no plug-ins that will execute require secure properties, the wallet creation or access is skipped and the user is not be prompted for the wallet key.

- **RequireRoot**: This plug-in sets the require root flag to true so that RUP Lite for OVM checks that root user is used for the pre-root mode. If this plug-in fails, RUP Lite for OVM stops.
- **AutoCorrectEtcHosts**: This plug-in updates the `/etc/hosts` file on each non-IDM node to include entries for the VMs logical host and internal logical host (if applicable), for all VMs that were deployed as part of the current upgrade.
- **RemoveRunAsRoot**: This plug-in removes the `run_as_root` file from *`ovabdir/`*`deployfw/bin/` file path and is rerunnable. Verify this plug-in was successful by confirming that the run_as_root file no longer exists under the *`ovabdir/`*`deployfw/bin directory`. The *`ovabdir`* is `/u01/ovmext` for IDM nodes and for all non-IDM nodes it is `/u01/APPLTOP/ovabext`.
- **ModifyOutputOwner**: This plug-in modifies RUP Lite files to be owned by the application user instead of root. To verify that this plug-in was successful, check the owner of the `/u01/APPLTOP/instance/lcm/ruplitovm/output` directory. The owner should be an apps user and not the root user.
- **GenerateOptimizedQueryPlans**: This plug-in is re-runnable. 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.
- **DeployECSF**: This plug-in is re-runnable. If the environment was originally provisioned before Release 5, verify that this plug-in was successful by confirming that the help object, schedule and group being deployed are reported in the log file. Alternatively, use Fusion Applications Control to connect to the Administration Server that hosts the search application and confirm that the Help instance artifacts are deployed.
- **IDMDecouplingCleanupEtcHosts**: This plug-in only applies to upgrades where IDM decoupling is enabled. The plug-in will remove the following entries from `/etc/hosts` on non-IDM hosts:
  - pstore.oracleoutsourcing.com
  - oim-admin.oracleoutsourcing.com
  - oim.oracleoutsourcing.com

- oim-server.oracleoutsourcing.com
- ids-db*.oracleoutsourcing.com

9.16.2 Troubleshoot Hanging in Offline or Online Mode

Problem

RUP Lite for OVM runs for a long time during domain configuration.

Solution

To resolve this issue, perform the following steps:

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.

If none of the above steps solve the problem, contact Oracle Support with detailed log information.

9.17 Troubleshoot Incremental Provisioning Issues

This section contains troubleshooting information for Incremental Provisioning (IP). The following topic is discussed:

- OPSS-DBDS Datasource Not Targeted to Supply Chain Management Clusters

9.17.1 OPSS-DBDS Datasource Not Targeted to Supply Chain Management Clusters

Problem

Some Oracle Fusion Supply Chain Management (SCM) clusters are missing from the OPSS data source. The server logs show the following error:

```
oracle.security.jps.service.credstore.CredStoreException: JPS-01055: Could not
create credential store instance. Reason
oracle.security.jps.service.policystore.PolicyStoreException: JPS-10702: The
datasource jdbc/OPSSDBDS is not found.[[
```

Solution

To fix this issue, perform the following steps:

1. Log in to the SCM Domain Admin WebLogic Console as an administrator:

   ```
   http://host:7801/console
   ```

2. Go to **Domain Configurations**, and select **Data Sources** under the **Services** section.
3. Select **opss-DBDS** from the list, and then select the **Targets** tab.
4. Ensure that the ”All servers in the cluster” option is checked for the following SCM clusters. If not, select **Lock** to edit and check both boxes:
   - OrchestrationInfrastructureCluster
   - ConfiguratorCluster
   - SupplyOrchestrationCluster
   - PlanningCluster
   - ManufacturingCluster
5. Repeat Step 4 for the following data sources (if they exist):
   - opss-DBDS-rac1
   - opss-DBDS-rac2
6. Click **Activate Changes** for the changes to take effect.

This solution will take effect and there is no need to bounce the servers or environment.

9.18 Troubleshoot Solaris Issues

This section contains troubleshooting information for Solaris. The following topic is discussed:

- Health Checker IdstoreConnectivityCheck Error

9.18.1 Health Checker IdstoreConnectivityCheck Error

Problem

Post upgrade, the Health Checker (HC) IdstoreConnectivityCheck fails with the following error:

```
[2017-01-24T07:20:17.739+00:00] [IdstoreConnectivityCheck] [ERROR] []
[IdstoreConnectivityCheck] [tid: 92] [ecid:
0000LbFM8W07y0I_IpP5if1OXjyg000009,0] HC-COMMON-00001 : Unable to perform the
check:[[
oracle.security.jps.service.idstore.IdentityStoreException: JPS-01520: Cannot
initialize identity store, cause: oracle.security.idm.ConfigurationException:
Failed to connect to directory. Check configuration information..
oracle.security.idm.ConfigurationException: Failed to connect to directory.
Check configuration information.
 Review log files for additional details to take an appropriate corrective
action ]]
```

Solution

To resolve this failure, perform the following steps:

1. Connect to the OID DB using the ODS schema user as follows:

   ```
   $ORACLE_HOME/bin/sqlplus ods/<ods_password>@<oid_db_connect_string>
   ```

2. Execute the `oidstats.sql` available under the `OID_ORACLE_HOME/ldap/admin` directory as follows:

   ```
   /u01/products/dir/oid/ldap/admin/oidstats.sql
   ```

3. Rerun orchestration.

9.19 Troubleshoot Other Potential Issues During the Upgrade

This section contains the following troubleshooting scenarios:

9.19.1 Troubleshoot setenv PERLIB5 Version Compatibility

Problem

While downloading patches, as described in the Download and Unzip Release 12 Language Packs, the environment variables are set to run the `adCreateMosPlan.pl` script. After issuing 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.

9.19.2 Health Checker FileOwnerAndPermissionsCheck Error

Problem

Health Checker (HC) FileOwnerAndPermissionsCheck might report the following error:

```
[Error]: Plugin 'FileOwnerAndPermissionsCheck': HC-PERM-0003: Failed to verify the
permission of files/folders in /u01/APPLTOP/fusionapps/odi/.cas/CLI/inventory using
find command. Review log files for additional details to take an appropriate
corrective action (verifying File Ownership and Permissions)
```

Solution

Ignore the error and proceed.

Note that the `/u01/APPLTOP/fusionapps/odi/.cas/CLI/inventory` error is only an example. If any similar error related to "`.cas`" is reported, ignore the error and proceed.

9.19.3 Patch Sessions and Processes Check Fails

Problem

When running Health Checker, the `PatchSessionsAndProcessesCheck` check fails with the following error:

```
HC-PATCHSP-00001: Patch sessions or processes found in your environment:HC-
PATCHSP-00017 : Check #7: Running patch processes found in this environment.
```

For any details needed for the running processes, review the log files .

Solution

This issue can occur even when no active session is found. To resolve this issue, perform the following steps:

1. Open the Health Checker log file to search for the running process that was reported. The running process typically contains strings such as `adpatch`, `adadmin`, `adworker`, `adctrl`, `oracle.apps.ad.worker.AdJavaWorker`, or `oracle.apps.ad.fapmgr.FAPManager`.
2. To see if there are active sessions, run the following command:

   ```
   ./fapmgr.sh report -patchprogress
   ```

3. If `./fapmgr.sh` returns no rows from the previous step, find the origin of the session(s) identified in Step 1. Then, decide whether this session needs to be terminated or allowed to finish before rerunning Health Checker.
4. Terminate or allow the process(es) to finish and then rerun Health Checker.

   If Health Checker detects that an active session was terminated or has completed, running Health Checker again succeeds.

9.19.4 General System Health Checks Error

Problem

General System Health Checks (mid tier hosts) completes successfully. However, it is showing the following java exception on the output:

```
oracle.jbo.client.CADatabaseConnectionProvider.loadConnectionProperties(CAData
baseConnectionProvider.java:154) at oracle.jbo.client.Configuration.
initializeFromConnectionName(Configuration.java:1225) at oracle.jbo.client.
Configuration.getConfiguration(Configuration.java:649) at oracle.jbo.common.
ampool.PoolMgr.loadConfiguration(PoolMgr.java:759) at oracle.jbo.common.
ampool.PoolMgr.findPool(PoolMgr.java:589) at oracle.jbo.client.Configuration.
createRootApplicationModuleHandle(Configuration.java:1589) at oracle.jbo.client.
Configuration.createRootApplicationModuleHandle(Configuration.java:1559)
at oracle.apps.topologyManager.model.applicationModule.TopologyManagerAMUtil.
getApplicationModuleInfo(TopologyManagerAMUtil.java:122) at oracle.apps.
topologyManager.model.applicationModule.TopologyManagerAMImpl.getApplicationModuleInf
o(TopologyManagerAMImpl.java:73) at
oracle.topologyManager.client.deployedInfo.DeployedInfoProvider.getDeployedDomainsByE
nvironment(DeployedInfoProvider.java:880) at oracle.check.common.util.
TMUtils.getDeployedDomains(Unknown Source)at oracle.check.common.util.
MWUtils.getDomainDetailsFromTM(Unknown Source) at oracle.check.common.util.
MWUtils.getDomainDetails(Unknown Source) at oracle.check.apps.
OPMNManagedProcessesStatusCheck.verifyManagedProcessesAreUp(Unknown Source)
at oracle.check.apps.OPMNManagedProcessesStatusCheck.execute(Unknown
Source)at oracle.check.common.AbstractCheckPlugin.plugin_execute(Unknown
Source)at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:
43)
        at java.lang.reflect.Method.invoke(Method.java:606)
        at oracle.healthcheckplug.core.PluginProxy.invoke(Unknown Source)
        at com.sun.proxy.$Proxy5.plugin_execute(Unknown Source)
        at oracle.healthcheckplug.core.PluginCallable.call(Unknown Source)
        at oracle.healthcheckplug.core.PluginCallable.call(Unknown Source)
        at java.util.concurrent.FutureTask.run(FutureTask.java:262)
        at java.util.concurrent.ThreadPoolExecutor.runWorker
(ThreadPoolExecutor.java:1145)
        at java.util.concurrent.ThreadPoolExecutor$Worker.run
(ThreadPoolExecutor.java:615)
        at java.lang.Thread.run(Thread.java:745)

Plugin succeeded: Verifying OPMN managed processes are up
```

Solution

Ignore the warning and proceed.

9.19.5 Post Language Health Checks Fail

Problem

The `PostLangPackChecks` plug-in fails for all Health Checks.

Solution

If the `SKIP_UPGRADE_FOR_LANGUAGE` property was enabled with one or more language codes, the Post Language Pack Health Checks are expected to fail for the skipped languages. These failures can be ignored because Post Language Patch Health Checks are run manually after the languages are upgraded manually.

9.19.6 Troubleshoot RUP Lite for RDBMS

Problem

The following error is reported when running RUP Lite for RDBMS:

```
[SEVERE] Fatal Error, Traceback (most recent call last):

File "/SHARED_LOCATION/work_dir/DB_2014-05-27_10-22-31/db_server_bundle/ruplite/
main.py", line 280, in _executeplugin
 result = _runpluginmodule(plugin_module)

File "/SHARED_LOCATION/work_dir/DB_2014-05-27_10-22-31/db_server_bundle/ruplite/
main.py", line 191, in _runpluginmodule
    errinfo = eval("plugin_module.plugin_execute()")
  File "<string>", line 1, in <module>

File "/SHARED_LOCATION/work_dir/DB_2014-05-27_10-22-31/db_server_bundle/db/plugin/
PostActions.py", line 95, in plugin_execute
    raise Exception('Failed to perform post DB restart actions.')
Exception: Failed to perform post DB restart actions.

[main] [SEVERE] Failed execution of plugin: db.plugin.PostActions

 [main] [SEVERE] Fatal error, exiting
 [main] [SEVERE] Summary of plugins:
 [main] [SEVERE]  Succeeded: db.plugin.ValidateEnv
 [main] [SEVERE]  Skipped: db.plugin.PreActions
 [main] [SEVERE]  Skipped: db.plugin.ApplyDBPatches
 [main] [SEVERE]  Failed with fatal:
db.plugin.PostActions, Exception: Failed to perform post DB restart actions.
[main] [SEVERE] RUPLite Installer for DB Stopped
```

Solution

RUP Lite for RDBMS failed while connecting to the database, which indicates an invalid value in the *work_dir*/DB_*timestamp*/db_server_bundle/metadata/env.properties file. If there is an extra "/" character for the ORACLE_HOME property, in this file, remove it. This ORACLE_HOME value must exactly match the database *ORACLE_HOME* and it should not have an additional "/" at the end.

Note that running RUP Lite for RDBMS in "validate" or "setdbparameter" mode runs successfully even if there as an additional "/" in the ORACLE_HOME property.

9.19.7 Troubleshoot 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. Review the related log files in the following location:

APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/RUP/
FAPatchManager_bootstrap_*timestamp*.log

9.19.8 Troubleshoot 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 Propagating Domain Configuration Assistant Was Successful
- WARs or EARs Are Not Accessible From The Primordial Host

9.19.8.1 Propagating Domain Configuration Assistant Takes Too Long to Complete

Problem

The **Propagating Domain** configuration assistant 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. Monitor the progress of this configuration assistant by reviewing log files in this location:

APPLICATIONS_CONFIG/lcm/admin/*version*/fapatch//ruplitedomain/output/logs

9.19.8.2 Confirm the Propagating Domain 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
```

9.19.8.3 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 the upgrade is running. The following is an example of the error caused by this condition:

```
<< read domain from
APPTOP/instance/domains/server.company.com/SCMDomain
<< write template to
APPLICATIONS_CONFIG/lcm/admin/11.12.x.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/11.12.x.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, undeploy or uninstall the WAR or EAR, which is `datalens.war` in this example. Then, resume orchestration. After the upgrade has completed successfully, install or deploy the WAR or EAR.

9.19.9 Upgrade Failures on Non-Oracle VM Configuration Using OVM Templates

Problem

The upgrade fails when Oracle Fusion Applications is running on a non-Oracle VM configuration and is using an Oracle VM template.

Solution

This configuration is not supported. To resolve this, check if a directory named `/assemblybuilder` exists in the environment. If this directory is present and this is not an Oracle VM environment, rename the directory to any other name. Then, resume orchestration.

9.19.10 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.

9.19.11 Extending Certificate Validation Fails on non-Oracle VM Environment

Problem

The **Extending Certificate Validation** fails with exception reporting if there is Incentive Compensation, Enterprise Contracts, and Oracle Fusion Accounting Hub offerings on the environment:

APPLICATIONS_CONFIG/domains/*CommonDomain_host*/CommonDomain /config/fmwconfig/owc_discussions.jks (No such file or directory).

Solution

If the missing file cannot be found in *APPLICATIONS_CONFIG*/domains/*CommonDomain_host*/CommonDomain/config/fmwconfig, perform the following steps:

1. Copy default_keystore.jks to owc_discussions.jks in *APPLICATIONS_CONFIG*/domains/*CommonDomain_ host*/CommonDomain/config/fmwconfig.
2. Resume orchestration.

9.19.12 Multiple Warnings in Data Security Grants Logs

Problem

After the Release 8 upgrade step called "Deploying Data Security Grants", the fapatch_Deploying_Data_Security_Grants_timestamp.log file contains entries as shown in the following example:

```
Number of records processsed : 8372
Number of records updated (grantee_key or compile_flag) : 3934
Number of records where GUIDs matched and no reconciliation done : 4366
Number of records in database missing necessary meta data : 2
Number of records in database that could not be reconciled with LDAP : 70
```

These messages may start with either "WARNING" or "SEVERE". The severe errors may be associated with exceptions as shown in the following examples:

```
SEVERE: Policy Store Exception raised in
getApplicationPolicyoracle.security.jps.service.policystore.
PolicyObjectNotFoundException: JPS-04028: Application with name
"cn=ADRGroups,cn=Groups" does not exist.

SEVERE: RuntimeException raised. Incorrect entry found in db for application role
PJT_PROJECT_WORK_PLAN_MANAGEMENT_DUTY.
May require reconciliation with target LDAP Processing row with grant_guid:
F9C89E5D04C2322629EBE642337695FC. ROLE_NAME is
PJT_PROJECT_WORK_PLAN_MANAGEMENT_DUTY ROLE_NAME_SPACE is
cn=ADRGroups,cn=Groups. PJT_PROJECT_WORK_PLAN_MANAGEMENT_DUTY GUID in
database is 61065B6FEA8E3824B74476B1A315FDE4 Runtime Exception is
oracle.jbo.JboException: JBO-29114 ADFContext is not setup to process
messages for this exception. Use the exception stack trace and error code to
investigate the root cause of this exception. Root cause error code is
JBO-29000. Error message parameters are
{0=oracle.security.jps.service.policystore.PolicyObjectNotFoundException,
1=JPS-04028: Application with name "cn=ADRGroups,cn=Groups" does not exist.}
```

Solution

These warnings and errors have no impact on functionality and can be ignored.

9.19.13 Ignorable Errors During Applying Online BI Metadata and Configuration Updates

Problem

Errors related to missing approles may be reported during the **Applying Online BI Metadata and Configuration Updates** configuration assistant. These errors are reported in `bi_webcat_patch.log`, and can be ignored, as they have no impact on the upgrade.

Solution

If Upgrade Orchestrator stops due to this error, resume the upgrade.

9.19.14 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>
```

Note that if this error follow any of above errors, then can be safely ignored.

```
ORA-01927: cannot REVOKE privileges you did not grant
```

9.19.15 Troubleshoot LCM Seed Utility

Problem

The LCM Seed Utility creates LCM_* schemas and grants access to them. While executing those grants, the RCU Scripts might fail because the schemas are not available, and the database connection or TNS listener is failing. The following errors occurs in the RCU logs:

```
SQL> old 1: GRANT CREATE SESSION TO &&1 new new 1: GRANT CREATE SESSION TO
LCM_EXP_ADMINGRANT CREATE SESSION TO LCM_EXP_ADMINERROR at line 1: RA-01917: user or
role 'LCM_EXP_ADMIN' does not exist
```

Solution

The LCM Seed Utility needs to be re-run after correcting the issues related to the database.

9.19.16 Troubleshoot Unexpected Processes Error in upgradeidmbinaries While Checking for Running Processes on Solaris Platforms

Problem

The `upgradeidmbinaries` plug-in fails in running process check on Solaris platforms. The following is an example error:

```
[2016-11-25T14:54:44.631+00:00] [orchestration] [NOTIFICATION] []
[oracle.orchestration] [tid: 36] Checking for server process:
/u01/products/dir
[2016-11-25T14:54:44.659+00:00] [orchestration] [NOTIFICATION] []
[oracle.orchestration] [tid: 36] ERROR: Some unexpected processes or servers
running, stop them manually and start the upgrade again.
```

Solution

Use an absolute path for the *PERL_LOCATION* property in `IDM.properties` instead of using a symlink path such as `/u01` as shown in the following example:

```
PERL_LOCATION=/scratch/mwport/IDM_SETUP/products/dir/oid/perl
```

The following is an example of an incorrect Perl path:

```
PERL_LOCATION=/u01/products/dir/oid/perl
```

9.20 Troubleshoot Tagging of JAZN Policies

The following is the log files location for Tagging JAZN Policies:

```
APPLICATIONS_CONFIG/lcm/logs/11.12.x.0.0/RUP/configlogs/
fapatch_Tagging_JAZN_Policies_timestamp.log
```

Problem

The “Tagging JAZN Policies” CA fails with the following error:

`Failed to tag JAZN policy for stripe: stripename`

Solution

Contact Oracle Support to request assistance in resolving the issue.

10

Additional Information About Upgrade Orchestrator

This section provides additional information about Upgrade Orchestrator. It includes the following topics:

- Upgrade Orchestrator Features
- Additional Information About Upgrade Orchestrator Commands
- Utilities Run by Upgrade Orchestrator

10.1 Upgrade Orchestrator Features

Upgrade Orchestrator provides the following features:

- Upgrade Phases
- Pause Points
- Oracle Fusion Applications Orchestration Report
- Language Upgrade

10.1.1 Upgrade Phases

Upgrade Orchestrator is run 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. The frequency of email alerts can be modified by the EMAIL_LEVEL property. For more information, see Table 11-1.

10.1.2 Pause Points

Upgrade Orchestrator pauses when it reaches a task that must be performed outside of orchestration. 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
- Start external servers

Default pause points cannot be edited or removed. For more information, see Pause Point Steps.

10.1.3 Oracle Fusion Applications Orchestration Report

The Oracle Fusion Applications Orchestration report is generated for each pod and its location is defined in the mandatory *ORCH_REPORT_LOCATION* property in the `pod.properties` file. When running the report, it is possible to 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 users who are specified in the `EMAIL_TO_RECIPIENT` and `EMAIL_CC_RECIPIENT` properties, if the `EMAIL_LEVEL` property is set to do so. The report name is `FAOrchestrationReport_`*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. The Fusion Applications Orchestration report also displays the following information:

- **Upgrade from Release**: The starting release on the pod, which could be release 11.1.8.0.0 or 11.1.9.n.n.
- **Upgrade to Release**: The ending release, which in this case is "FA version 11.12.x.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.

10.1.4 Language Upgrade

If any languages in addition to US English were previously installed, Upgrade Orchestrator performs the upgrade of each installed language.

Orchestration allows skipping one or more installed language pack upgrades by using a property called `SKIP_UPGRADE_FOR_LANGUAGE` in the PRIMORDIAL.properties file. If the option of skipping any languages is chosen, upgrade them manually after the completion of Upgrade Orchestration. For more information, see Perform Optional Language Installations in the *Oracle Fusion Applications Installation Guide*.

10.2 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

10.2.1 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 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 Options for the Orchestration getStatus Command and Monitor Upgrade Orchestration Progress.
- Use `exitOrchestration` to terminate orchestration gracefully on all hosts on a specific pod. For more information, see Terminate Upgrade Orchestration.
- Use `clearExitOrchestration` to clear the exit status on all hosts. For more information, see Terminate Upgrade Orchestration.
- Use `getExitOrchestrationStatus` to retrieve the status of the `exitOrchestration` command. For more information, see Get the ExitOrchestration Status.
- 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 The validatesetup Argument.

10.2.2 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 10-1 Options for the orchestration.sh Command

Name	Mandatory	Description
-pod	Yes	The value of *POD_NAME* refers to the directory created in Step 3 of 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 Host Types.
-release	No	The release version, for example, 11.12.x.0.0.
-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 the `-DlogLevel` option is set to FINEST.
-v	No	Displays the product version and exits.
-h	No	Displays help information and exits.

10.2.3 Options for the Orchestration updateStatus Command

The following table provides a description of the available options when using the orchestration `updatestatus` command to update the status of orchestration tasks:

Table 10-2 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 version, for example, 11.12.x.0.0. If this option is not used, all releases defined in the manifest file are executed

Table 10-2 (Cont.) Options for orchestration.sh updateStatus Command

Name	Mandatory	Description

-phase	Yes	The phase name. Valid values are as follows:
		`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

10.2.4 Options for the Orchestration getStatus Command

The following table provides a description of the available options when using the orchestration `getstatus` command to find the status of an orchestration session:

Table 10-3 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 number, for example, 11.12.x.0.0. If this option is not used, all releases defined in the manifest file are queried

-phase	No	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

Table 10-3 (Cont.) Options for orchestration.sh getStatus Command

Name	Mandatory	Description
-v	No	Displays the product version and exits
-h	No	Displays help information and exits

10.2.5 The validatesetup Argument

If the `orchestration.sh` command is run 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 run implicitly when any of the orchestration commands run.

10.3 Utilities Run by Upgrade Orchestrator

This section describes the utilities that are run by Upgrade Orchestrator. This section is informational 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

10.3.1 RUP Installer

During the installation phase, RUP Installer copies all files for Release 12 (11.12.x.0.0) 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 to perform the remaining tasks required to update and deploy artifacts to Oracle Fusion Applications. Depending on the starting release of upgrade to Release 12 (11.12.x.0.0), not all configuration assistants may run.

10.3.1.1 RUP Installer Configuration Assistants

All mandatory configuration assistants must complete successfully before proceeding to the next configuration assistant. An `autoretry` feature is introduced in Release 10 that provides the ability for certain configuration assistants to automatically retry after a failure. The following are three types of configuration assistants with respect to `autoretry`:

- Those that never `autoretry`
- Those that always `autoretry`
- Those that `autoretry`, depending on how long it runs before failing. This is the default.

The following table provides a list of configuration assistants that the first installer runs. If available, links are provided to relevant troubleshooting sections.

Table 10-4 Configuration Assistants Run by Oracle Fusion Applications Release 12 (11.12.x.0.0) RUP Installer Part 1 of 2

Name	Mandatory	Description
Configure Patch Manager	Yes	Configures Oracle Fusion Applications Patch Manager
Update Patch Manager and Dependent Components	Yes	Applies Patch Manager Patches
Reconfigure Patch Manager	Yes	Reconfigures Oracle Fusion Applications Patch Manager
Bootstrap Patch Manager	Yes	Updates the data model for Oracle Fusion Applications Patch Manager by running the `fapmgr bootstrap` command
Create LCM Administration Schemas	Yes	Creates LCM Administration schemas
Upgrade LCM Administration Schemas	Yes	Upgrades LCM Administration schemas to give them the required grants
Create Middleware Schemas	Yes	Creates Oracle Fusion Middleware schemas

Table 10-4 (Cont.) Configuration Assistants Run by Oracle Fusion Applications Release 12 (11.12.x.0.0) RUP Installer Part 1 of 2

Name	Mandatory	Description
Apply Middleware Patch Sets	Yes	Applies Oracle Fusion Middleware patch sets, which can include upgrades, schema changes and installers. For more information, see Middleware Installers Invoked by the Apply Middleware Patch Sets Configuration Assistant
Apply Pre-PSA Middleware Patches	Yes	Applies Pre-PSA Middleware Patches For more information, see Patches Not Supported by the Apply Pre-PSA and Post-PSA Middleware Patches Configuration Assistants
Verify Middleware PSA Schema Credentials	Yes	Verifies users and logins for schemas
Upgrade Middleware Schemas	Yes	Runs Oracle Fusion Middleware patch set assistants (PSA)
Apply Post-PSA Middleware Patches	Yes	Applies Post-PSA Middleware Patches. For more information, see Patches Not Supported by the Apply Pre-PSA and Post-PSA Middleware Patches Configuration Assistants
Create Grants and Synonyms on Middleware Database Objects	Yes	Creates `FMW_RUNTIME` schema
Upgrade OPSS	Yes	Upgrades the Policy Store
Apply Offline Setting and Topology Manager Changes	Yes	Updates Taxonomy Management tables with the information on the offerings that were selected
Apply Offline BI Metadata and Configuration Updates	Yes	Performs the deployment of the updated applications policies for Oracle Business Intelligence

Table 10-4 (Cont.) Configuration Assistants Run by Oracle Fusion Applications Release 12 (11.12.x.0.0) RUP Installer Part 1 of 2

Name	Mandatory	Description
Apply ESSAPP Code Source Grant Changes	Yes	Adds code source grants to support auditing
Relocate Managed Servers	Yes	Relocates managed servers
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
Upgrade Offline OSN Configuration	Yes	• Generates the input properties file • Upgrades OSN offline
Configure EDQ	Yes	Configures a new managed server for Enterprise Data Quality (EDQ) in the CommonDomain with scaled out servers in the appropriate environments. This configuration also occurs in CRM or Procurement domains if they are provisioned in the environment
Apply Domain Configuration	Yes	• Configures System Resources • Configures IBR • Configures new ODI Server • Applies File Actions • Configures JDBC Persistent Store for SOA JMS and TLog • Resets Server Credential Store Password • Reconfigures EDQ Server Properties • Consolidates JDK Certs • Applies WLS JDK Updates • Updates Fusion Applications Start Parameters • Updates Domain Component Versions
Propagate Domain Configuration	Yes	Unzips RUP Lite for Domain Configuration into *APPLICATIONS_CONFIG*/lcm/admin/*version*/fapatch/ruplitedomain. Updates properties in the RUP Lite env.properties file and prepares RUP Lite so RUP Lite can be run for 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, 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.

Table 10-5 Configuration Assistants Run by Oracle Fusion Applications Release 12 (11.12.x.0.0) RUP Installer Part 2 of 2

Name	Mandatory	Description
Configure Patch Manager	Yes	Configures Oracle Fusion Applications Patch Manager
Bootstrap Patch Manager	Yes	Updates the data model for Oracle Fusion Applications Patch Manager by running the fapmgr `bootstrap` command
Install Downloaded Fusion Application Patches	Yes	Applies Fusion Applications Patch Bundles (FAPB) in install only mode during upgrade flow
Install Downloaded Fusion Applications Upgrade Patches	Yes	Installs downloaded Oracle Fusion Applications upgrade patches, as described in the Download and Unzip Mandatory Post-Release 12 Patches section
Copy FAPB Merged Metadata	Yes	Copies Merged metadata from FAPB location to `ORACLE_HOME` as shown in the following example: • `RUP: "<FAPB_LOCATION>/RUP" location to "/APPTOP/fusionapps/applications/admin/patchsettop/<version>/en"` • `LP: "<FAPB_LOCATION>/LanguagePack" location to "/APPTOP/fusionapps/applications/admin/patchsettop/<version>/<langCode>"`
Prepare Merged Metadata	Yes	Copies the patch metadata from the `ORACLE_HOME` to the Instance directory. For LP upgrade flows, It modifies the merged patch driver file to refer to active language if required.
Offline Preverification Pre Database Content Upload	Yes	Performs the following validation checks while all servers are shut down: • Policy Store • Number of database workers • Database Content Upload • Application Policies (`system-jazn-data.xml`) • Business Intelligence Publisher (BIP) • Oracle Data Integrator (ODI)
Generate Data Security Policy Customization Report Pre DB upload	Yes	Generates a report on the data security policies with customizations before the DB content is uploaded
Grant Privileges to Application Schemas	Yes	Grants system privileges to database users and creates base object privileges

Table 10-5 (Cont.) Configuration Assistants Run by Oracle Fusion Applications Release 12 (11.12.x.0.0) RUP Installer Part 2 of 2

Name	Mandatory	Description
Run Fusion Applications Patchset Assistants	Yes	This CA is designed to be the generic place where all PSAs from FA can be invoked. Currently, only the GRC PSA is being run from here.
Prepare Checkfile Information for Loading Database Components	Yes	Prepares checkfile information for loading database components
Remove Retired SOA Composites	No	Remove retired SOA composites that are no longer used
Consolidate Servers	Yes	Consolidates servers by reassigning resources from the source cluster to the target cluster
Delete Application Deployments	Yes	Unregisters and deletes the obsolete applications including those applications that were never deployed
Delete Managed Server Clusters	Yes	Deletes obsolete serves
Load Database Components	Yes	Uploads the database content packaged in 11*g* Release 12 (11.12.x.0.0) to the database, such as database objects, seed data, and package headers and bodies
Migrate OID User Preferences and OIM Customizations	Yes	Runs 2 FA supplied utility scripts to migrate the OID user preferences and the OIM customizations to the FA database
Install Language Packs	No	This CA is only run if the upgraded environments have language pack already installed
Install Downloaded Fusion Application Language Patches	Yes	Applies Fusion Applications Patch Bundles (FAPB) NLS patches in install only mode during the upgrade flow. This CA is applicable only if there are active languages available in the environment at the time of the upgrade

Table 10-5 (Cont.) Configuration Assistants Run by Oracle Fusion Applications Release 12 (11.12.x.0.0) RUP Installer Part 2 of 2

Name	Mandatory	Description
Copy FAPB Merged Metadata for Languages	Yes	Copies merged metadata from FAPB location to `ORACLE_HOME` as shown in the following example: `<FAPB_LOCATION>/LanguagePack` location to `/APPTOP/fusionapps/applications/admin/patchsettop/<version>/<langCode>`. This CA is applicable only if there are active languages available in the environment at the time of the upgrade
Install Downloaded Fusion Application Language Upgrade Patches	Yes	Installs downloaded Oracle Fusion Applications upgrade NLS patches in install only mode, as described in Download and Unzip Mandatory Post-Release 12 Patches. This CA is applicable only if there are active languages available in the environment at the time of the upgrade
Create Language Pack Merged Metadata	Yes	It is invoked only when there are active languages on the pod indicated by the flag "`ACTIVE_LANG_EXISTS`". It should get invoked if the merged LP manifest file `mw_patchset_manifest.xml` and merged LP DB patch do not exist at the expected location. When executed it should perform the following operations: • Merging MW Manifest Files • Merging Database Patch Files This CA is applicable only if there are active languages available in the environment at the time of the upgrade
Prepare Merged Metadata for Languages	Yes	It is invoked only when there are active languages on the pod indicated by the flag "`ACTIVE_LANG_EXISTS`". When executed, it performs the following operations: • Copies the merged metadata from Oracle home to Instance directory • Modifies the DB patch driver file for LP flow if required This CA is applicable only if there are active languages available in the environment at the time of the upgrade
Synchronize Multilingual Tables for Upgrades	Yes	Replicates the US seed data for each active language that is getting upgraded. It is invoked only when there are active languages on the pod indicated by the flag "`ACTIVE_LANG_EXISTS`." This CA is applicable only if there are active languages available in the environment at the time of the upgrade
Apply Middleware Language Upgrade Patches	Yes	Applies ATGPF database patches in config only mode. It is invoked only when there are active languages on the pod indicated by the flag "`ACTIVE_LANG_EXISTS`." This CA is applicable only if there are active languages available in the environment at the time of the upgrade
Load Database Components for Languages	Yes	Translates the US messages to the corresponding language messages in the database. This CA is applicable only if there are active languages available in the environment at the time of the upgrade

Table 10-5 (Cont.) Configuration Assistants Run by Oracle Fusion Applications Release 12 (11.12.x.0.0) RUP Installer Part 2 of 2

Name	Mandatory	Description
Deploy BI Publisher Language Artifacts	Yes	Deploys BI Publisher language artifacts using catalog manager
Update Language Release Information	Yes	Updates the language release version information in the AD_Languages table. This CA is applicable only if there are active languages available in the environment at the time of the upgrade
Deploy JAZN Policies	Yes	Deploys updated applications policies, based on your selections during the Policy Store Analysis configuration assistant
Tag JAZN Policies	Yes	Locks down all the oracle seeded policies by means of tagging and prevent the policies from being changed
Export Roles from the Identity Store	Yes	Migrates the roles from the ID store to the policy store in the offline part. The online part is finished in the "Migrate Roles to Policy Store" CA
Deploy BI Publisher Artifacts	Yes	Using Catalog Manager, deploys BI Publisher artifacts
Import Oracle Data Integrator Repositories	Yes	• Imports ODI topology • Imports ODI model folders • Imports ODI models • Imports ODI projects • Drops ODI error tables
Generate Data Security Policy Customization Report Post DB upload	Yes	Generates a report on the data security policies with customizations after the DB content is uploaded
Create Grants/ Synonyms on Application Database Objects	Yes	Creates synonyms between database objects and grants object privileges to database users
Offline Preverification Post Database Content Upload	Yes	• Validate host and port for new managed servers • Validate LDAP Data (LDIF)

Table 10-5 (Cont.) Configuration Assistants Run by Oracle Fusion Applications Release 12 (11.12.x.0.0) RUP Installer Part 2 of 2

Name	Mandatory	Description
Configure New Managed Servers	Yes	Configures managed servers for new applications to be associated with the first non-admin host by default
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
Deploy New Applications	Yes	Deploys new applications using domain extension templates
Create AQ Queues	Yes	Creates AQ queues
Populate Topology Manager Backfeed Data	Yes	Registers Middleware specific applications to the Topology Manager, including OSN, EDQ, and SOA applications
Generate SOA Configuration Plan	Yes	Generates the configuration plan to be used for deploying SOA composites
Register Forgot Password Page	Yes	Registers the HCM domain forgot password page to the OAM resource target
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`
Apply Offline Setting Changes	Yes	Applies Oracle Fusion Applications environment configuration setting changes while all servers are shut down: • Reassign System Resource Targets • Update BPEL EJB Timeout • Update JTA Timeout • Update Provisioned Configuration Files • Update Authenticator Settings • Update Authenticator Timeout Settings • Update Application Policy Stripe Version • Edit Server Start Arguments • Updat UCM DR Configuration • Update Domain Component Versions • Apply Offline Setting Changes • Update FND Preferences

Table 10-5 (Cont.) Configuration Assistants Run by Oracle Fusion Applications Release 12 (11.12.x.0.0) RUP Installer Part 2 of 2

Name	Mandatory	Description
Quiesce SOA Servers Offline	Yes	Places all SOA servers in a quiescent mode, which effectively queues any incoming requests not related to the administration of the upgrade until the quiescent mode is exited
Verify Node Manager and OPMN Status	Yes	Verifies the following processes: • Node Managers • BI OPMN Processes • GOP OPMN Processes • Web Tier OPMN Processes • OSN Web Tier OPMN Processes Do not exit out of RUP Installer during this configuration assistant.
Start All Admin Servers	Yes	Starts all Administration Servers
Delete MDS Documents	Yes	Deletes SOA MDS artifacts
Configure OPSS Keystore Service	Yes	Configures the OPSS Keystore Service
Deploy LDIF User Data	Yes	Uploads the LDIF user data for the language that is being configured
Create Fusion APPIDs	Yes	Creates Fusion APPID users and groups in the LDAP server and credentials for those users in the credential store
Apply Admin Server Online Setting and Configuration Changes	Yes	• Updates diagnostic settings • Updates JPS Config Timeout settings • Removes deprecated code source grants • Updates audit log location settings • Redeploys `NONJ2EEMANAGEMENT.EAR` • Configures JMS persistence store resiliency
Start Minimal Servers for Configuration Updates	Yes	Starts minimal managed servers required to run the necessary configuration assistants successfully
Apply UCM Configuration	Yes	Configures UCM to store content in the database instead of the file system

Table 10-5 (Cont.) Configuration Assistants Run by Oracle Fusion Applications Release 12 (11.12.x.0.0) RUP Installer Part 2 of 2

Name	Mandatory	Description
Apply WebCenter Configuration Changes	Yes	• Replaces `WebCenter-UCM` Connection with `FusionAppsContentRepository` Connection • Updates Connection References • Applies Skyros changes • Registers Custom Resource Action Handler For WebCenter Profile Service
Configure VirusScan	Yes	• Configure ApplCore Virus scan for UCM • Remove CRM VS jars from FS apps (FSM)
Configure Trust Asserter	Yes	Configures trust asserter to be used for remote task flow Keystore Service
Update LPA Policies	NA	Not applicable to on premise
Import OWSM Repository	No	Imports OWSM repository to Fusion Applications database
Configure KSS for OWSM	Yes	Configures Keystore Service for OWSM
Delete Credentials	No	Deletes existing credentials
Migrate Roles to Policy Store	Yes	Continues the role migration from the ID store to the policy store in the online part. The offline part is finished in the "Export Roles from the Identity Store" CA
Re-Associate Security Store to Database	Yes	Re-associates the security store from an LDAP based security store to a database based security store
Upgrade Admin Server Online OSN Configuration	Yes	Upgrades those OSN related configurations that require only the admin servers to be online
Start All Servers	Yes	Starts all servers in all domains, including the BI servers. Also performs the `opmnctl` start for Oracle HTTP Server (OHS) and `BIInstance`

Table 10-5 (Cont.) Configuration Assistants Run by Oracle Fusion Applications Release 12 (11.12.x.0.0) RUP Installer Part 2 of 2

Name	Mandatory	Description
Online Preverification	Yes	Validates the following artifacts:. • 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
Deploy Data Security Grants	Yes	Reconciles Data Security changes
Generate OHS Reference Configuration File	Yes	Generates OHS configuration files for installed product families in the directory, *`APPLICATIONS_CONFIG`*`/lcm/admin/`*`version`*`/fapatch/OHS/patched_moduleconf`
Apply OWSM Configuration	No	Upgrades Oracle Web Services Manager (Oracle WSM) policies after backing up the policies: • Back up OWSM Repository and Templates • Apply Global Policies for OWSM • Enabling Conditional Global Policy Attachments (GPA)
Deploy SPE Inline Service Artifacts	No	Deploys SPE Inline Service Artifacts
Upgrade Online OSN Configuration	Yes	Upgrades the online OSN configuration
Upgrade ADF Metadata	No	Upgrades ADF related metadata
Apply OAM Configuration	No	Applies changes to the Oracle Access Manager (OAM) configuration.

Table 10-5 (Cont.) Configuration Assistants Run by Oracle Fusion Applications Release 12 (11.12.x.0.0) RUP Installer Part 2 of 2

Name	Mandatory	Description
Deploy Flexfields	No	Deploys flexfields to the domain that hosts the `FndSetup` application
Apply Online BI Metadata and Configuration Updates	Yes	Upgrades the online BI configuration
Upgrade Custom Metadata	No	Upgrades custom metadata
Import Group Space Templates	No	Imports changes present in group space template artifacts
SOA Preverification	Yes	Performs the following steps. If there are customizations, merge them during this 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 • Middleware 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: • Image Routing (IPM): Checks if the IPM server is up
Migrate Groups to Roles in BPM Task Instances	No	Invokes the `GroupToRoleMigrateTask.py` script on all SOA database schemas
Migrate Groups to Roles in BPM Rules	No	Invokes the `GroupToRoleMigrateRule.py` script on all SOA domains
Apply SES Configuration Changes	No	Updates additional configuration updates to Oracle Secure Enterprise Search (SES) running on the Common Domain: • Applies SES doc type configuration changes • Applies SES security update VO • Applies SES security update index • Runs SES upgrade scripts

Table 10-5 (Cont.) Configuration Assistants Run by Oracle Fusion Applications Release 12 (11.12.x.0.0) RUP Installer Part 2 of 2

Name	Mandatory	Description
Remove UCM SES Objects	No	Removes the following objects on the SES search administration server: • Index Schedule with the name "WebCenter UCM Schedule" • Data source with the name "WebCenter UCM" • Data source with the name "WebCenter UCM" from the data source group with the name "Collaboration"
Apply BPM Template Changes	No	Applies BPM template changes to the MDS repository
Deploy B2B Metadata	No	Deploys B2B Metadata
Deploy SOA Shared Repository	Yes	Deploys SOA shared repository artifacts to the SOA servers available in the environment
Deploy Middleware SOA Composites	No	Deploys middleware SOA composites to every domain
Deploy Flexfield Independent SOA Composites	No	Deploys SOA composites that do not depend on flexfields
Deploy Flexfield Dependent SOA Composites	No	Deploys SOA composites that depend on flexfields
Activate SOA Language	No	It is deployed only if the Language Pack (LP) is already installed
Deploy Offering Dependent SOA Composites	No	Deploys SOA composites based on the new offering dependency
Deploy Public Event Catalog	Yes	Deploys Public Event Catalog to all SOA domains

Table 10-5 (Cont.) Configuration Assistants Run by Oracle Fusion Applications Release 12 (11.12.x.0.0) RUP Installer Part 2 of 2

Name	Mandatory	Description
Regenerate Customer Defined SOA Composites	No	NA
Register SOA Resource Bundles	Yes	Deploys SOA Resource Bundles to the corresponding SOA servers
Undeploy SOA Composites	No	Undeploys obsolete SOA composties and deletes their jars from disk
Undeploy Middleware SOA Composites	Yes	Undeploys Middleware SOA composites
Apply Image Routing (IPM) Artifacts	Yes	Applies Image Routing (IPM) artifacts
Import Image Routing (IPM) Artifacts	No	Deploys IPM artifacts to the IPM server
Apply Online Setting and Metadata Changes	No	• Update Server Parameters • Delete Portlet Metadata • Update Thread Count for EDN • Update UMS Auto Delete Metadata • Update BPEL Auto Recovery Parameters
Generate RUP Lite for OHS	Yes	Generates the zip file that contains all files needed by RUP Lite for OHS to upgrade OHS
Post Configuration	No	Deletes wallets

10.3.1.1.1 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

10.3.1.1.2 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: Patch the Database Server. For more information, see Apply Exadata Patches for Release 12.
- Oracle Identity Management Server: Patch the IDM server by following the steps in Upgrade the Oracle Identity Management Domain to Release 12 (11.12.x.0.0).

10.3.1.1.3 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.
- `UpdateSOAMDS` SOA Composite: Verifies the taxonomy, checks if the Administration Server is up, and if the SOA platform is ready.
- SOA Shared Repository: Verifies the taxonomy, checks if the Administration Server is up, and checks for SOA_SERVER and SOA_PLATFORM readiness.
- 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 Merge SOA Composite JDeveloper Customizations During SOA Preverification.
- Image Routing (IPM): Checks if the IPM server is up.

10.3.2 Health Checker Utility

Upgrade Orchestrator runs the Health Checker utility to run system checks during and after the upgrade to ensure that the environment meets recommended standards. Health Checker is run during pre-down time, as described in Run the 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. 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.

The following topics describe the usage of Health Checker:

- Health Checker Manifests
- Health Checker Plug-ins
- Override Health Checks

10.3.2.1 Health Checker Manifests

When running Health Checker manually, a manifest file is specified, as described in the following table. 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 the 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 10-6 Health Checker Manifest Files

Manifest File	Host Requirements	Typical Usage of the Manifest
GeneralSystemHealthChecks.xml	Primordial, OHS, Midtier	Run this manifest during pre-down time and Upgrade Orchestrator runs this manifest during and after the upgrade. See General System Health Checks.
PreDowntimeUpgradeReadinessHealthChecks.xml	Primordial, OHS, Midtier	Run this manifest before the upgrade downtime. See Pre-Downtime Upgrade Tasks .
DuringDowntimeUpgradeReadinessHealthChecks.xml	Primordial, OHS, Midtier	Upgrade Orchestrator runs this manifest during downtime and before the upgrade starts. See Pre-Upgrade Tasks Performed by Health Checker During Downtime.
VitalSignsChecks.xml	Primordial	Upgrade Orchestrator runs this manifest during the upgrade. See Vital Signs Check.
PostUpgradeHealthChecks.xml	Primordial, OHS, Midtier	Upgrade Orchestrator runs this manifest after the upgrade. See Post-Upgrade Tasks Performed by Health Checker.
LanguagePackReadinessHealthChecks.xml	Primordial	Run this manifest before installing a language pack. See Language Pack Readiness Health Checks.
PostLanguagePackHealthChecks.xml	Primordial	Run this manifest after installing a language pack. See Post Language Pack Health Checks.
PatchingReadinessHealthChecks.xml	Primordial	Run this manifest before applying a patch. See Patching Readiness Health Checks.
PostPatchingHealthChecks.xml	Primordial	Run this manifest after applying a patch. See Post Patching Health Checks.
DataQualityChecks.xml	Primordial	Run this manifest to check the quality of data, such as Flex data. Note that these checks might require significant processing time. See Data Quality Check.

10.3.2.2 Health Checker Plug-ins

Health Checker calls plug-ins to perform its tasks. This section describes which plug-ins run during the following phases of patching and upgrade processes:

- General System Health Checks
- Pre-Downtime Upgrade Tasks
- Pre-Upgrade Tasks Performed by Health Checker During Downtime
- 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

- Data Quality Check
- Vital Signs Check

Plug-ins are listed in the order that they are run by Health Checker, within each manifest.

10.3.2.2.1 General System Health Checks

The following checks occur when Health Checker runs the `GeneralSystemHealthChecks.xml` manifest:

- Validate LDAP Connectivity

  Verifies the connectivity to the identity store and policy store LDAP using identity store credentials.

- Database Connectivity

  Checks if the database instance is up. For RAC databases, checks if all nodes are up.

- ODI Repository Check

  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`.

- JAZN Version Check

  Verifies that the JAZN version in `system-jazn-data.xml` is the same as the version in the policy store.

- Identity Store Connectivity

  Verifies that the `idstore.ldap.provider` in `jps-config-jse.xml` can be used to connect to the identity store.

- IP Port Range Check

  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.

- ODI Setup Check

  Confirms the correct connection URLs exist in the ODI Repository.

- Verify Node Managers are Accessible

  Verifies that node managers for all hosts are running and are accessible.

- Verify Server Status

  Confirm that all relevant Administration Servers and Managed Servers have a RUNNING status.

- OAM Server Status Check

  Verifies OAM server status.

- OPMN Managed Processes Up

  Verifies the OPMN managed processes are up and running.

- OPMN Additional Processes Up Check

  Verifies that the status of the OPMN process is up.

- OHS OPMN Check

  Checks if the OHS process is up on the OHS host using OPMN.

- Validate Required AppId

  Verifies that all required APPIDs exist in the Identity Store.

- File Owner Permissions Check

  Validates file and folder ownership and permissions for the file system.

- FSMount Check

  Verifies Required file system mount points.

- Database Schema Validate Version

  Verifies FMW and FA Schema Versions.

- WSM-PM Check

  Verifies that the WSM-PM application is running on all SOA domains.

10.3.2.2.2 Pre-Downtime Upgrade Tasks

The following checks occur when running Health Checker during Pre-Downtime, using the `PreDowntimeUpgradeReadinessHealthChecks.xml` manifest:

- Disk Space Check

  Checks for free and usable disk space on the primordial and non-primordial Oracle Fusion Applications hosts.

- Locked Objects Check

  Verifies that there are no locked objects in the `FUSION_ODI` and `SES` schemas.

- Total Memory Check

  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. Note that the formula used in the Total Memory Check considers only the memory requirements for managed servers, administration servers, and BI clusters. The actual total memory requirements will exceed this calculation. For more information, see Verify Memory Requirements.

- SOA Platform is Ready

  Verifies whether the SOA platform is ready for each domain that is impacted by the contents of the upgrade.

- Web Logic Edit Check

  Verifies that no WLS edit sessions or unactivated changes exist.

- New Managed Servers Port Availability

  Verifies the availability of ports for managed servers that were added.

- Tablespace Autoextent Check

  Verifies the tablespace is autoextensible.

- File Owner Permissions Check

Verifies the permissions and owners of the file.

- Invalid Index Check

  Checks for unusable indexes in the Fusion Schema of the Oracle Fusion Applications database.

- Invalid Objects Check

  Checks for and reports any invalid objects.

- Fusion Read Only Schema Validation

  Validates database connectivity for Fusion read only schemas.

- Fusion Schema Validation

  Validates database connectivity to all Fusion schemas.

- MDS Schema Validation

  Checks database connectivity for MDS schemas.

- Middleware Schema Connectivity

  Checks database connectivity for all schemas except for `FUSION_MDS` schemas.

10.3.2.2.3 Pre-Upgrade Tasks Performed by Health Checker During Downtime

The following checks occur when Health Checker runs the `DuringDowntimeUpgradeReadinessHealthChecks.xml` manifest:

- Patch Sessions and Processes Check

  Verifies that no AD Administration, AutoPatch or Patch Manager processes are running.

- Active OPatch Processes Check

  Checks active OPatch processes.

- Database Instance Connectivity

  Checks if the database instance is up. For RAC databases, checks if all nodes are up.

- MDS Schema Validation

  Checks database connectivity for MDS schemas.

- Middleware Schema Validation

  Checks database connectivity to Fusion Middleware schemas, with exception of the MDS schemas.

- Fusion Read Only Schema Validation

  Validates database connectivity for Fusion read only schemas.

- Identity Store Connectivity

  Verifies that the `idstore.ldap.provider` in `jps-config-jse.xml` can be used to connect to the identity store.

- Verify Node Managers are down

  Verifies Node Managers are shut down.

- Server Status Down

Confirms that all relevant Administration Servers and Managed Servers are down.

- Validate LDAP Connectivity

  Verifies the connectivity to the identity store and policy store LDAP using identity store credentials.

- JAZN Version Check

  Verifies that the JAZN version in `system-jazn-data.xml` is the same as the version in the policy store.

- Free Memory Check

  Verifies free memory and swap space.

- OPMN Managed Processes Status

  Verifies OPMN managed processes are shut down.

- OPMN Managed Process Down

  Verifies again that OPMN processes are down.

- OdiActiveSessionCheck

  Verifies no active or locked ODI sessions exist.

10.3.2.2.4 Post-Upgrade Tasks Performed by Health Checker

The following checks occur when Health Checker runs the `PostUpgradeHealthChecks.xml` manifest:

- Language Pack Validation

  Checks if a language pack has been upgraded to the current release or needs to be upgraded to the current release.

- Patch Sessions and Processes Check

  Checks whether any AD Administration, AutoPatch or Patch Manager processes are running.

- Active OPatch Processes Check

  Verifies no active OPatch process is running.

- Locked Objects Check

  Verifies that there are no locked objects in the `FUSION_ODI` and `SES` schemas.

- WLS Edit Sessions and Unactivated Changes

  Verifies that no WLS edit sessions or unactivated changes exist.

- SOA Platform Check

  Verifies whether the SOA platform is ready for each domain that is impacted by the contents of the upgrade.

- Fusion Read Only Schema Validation

  Validates database connectivity for Fusion read only schemas.

- Fusion Schema Validation

  Validates database connectivity to all Fusion schemas.

- MDS Schema Validation

Checks database connectivity for MDS schemas.

- Middleware Schema Connectivity

  Checks database connectivity for all schemas except for `FUSION_MDS` schemas.

10.3.2.2.5 Language Pack Readiness Health Checks

The following checks occur when Health Checker runs the `LanguagePackReadinessHealthChecks.xml` manifest. This manifest is typically run before installing a language pack.

- Patch Sessions and Processes Check

  Verifies that no AD Administration, AutoPatch or Patch Manager processes are running

- Active OPatch Processes Check

  Checks active OPatch Processes

For more information, see Perform Optional Language Installations in the *Oracle Fusion Applications Installation Guide*

10.3.2.2.6 Post Language Pack Health Checks

The `PostLanguagePackHealthChecks.xml` manifest is typically run after installing a language pack. The following check occurs when Health Checker runs this manifest:

- Language Pack Validation

  Verifies that the SOA platform is ready for each domain that is impacted by the contents of the language pack.

For more information, see Perform Optional Language Installations in the *Oracle Fusion Applications Installation Guide*.

10.3.2.2.7 Patching Readiness Health Checks

The `PatchingReadinessHealthChecks.xml` manifest is typically before applying a patch. The following checks occur when Health Checker runs this manifest:

- JAZN Version Check

  Verifies the JAZN version in Oracle home matches with the policy store.

- Patch Sessions and Processes Check

  Verifies that no AD Administration, AutoPatch or Patch Manager processes are running.

- Active OPatch Processes Check

  Verifies Active OPatch Processes

- Locked Objects Check

  Verifies there are no locked objects in the `FUSION_ODI` or `SES` schema.

- Web Logic Conflict Check

  Verifies that no WLS edit sessions or unactivated changes exist.

- Database Connectivity Check

Verifies database instance connectivity.

- Invalid Index Check

  Checks for unusable indexes in the Fusion Schema of the Oracle Fusion Applications database.

- Invalid Objects Check

  Checks for and reports any invalid objects.

For more information, see Step 5 of Apply All Patches Related to a Functional Patch Bundle in the *Oracle Fusion Applications Patching Guide*.

10.3.2.2.8 Post Patching Health Checks

The `PostPatchingHealthChecks.xml` manifest is typically run after applying a patch. The following checks occur when Health Checker runs the manifest:

- JAZN Version Check

  Verifies that the JAZN version in `system-jazn-data.xml` is the same as the version in the policy store.

- Patch Sessions and Processes Check

  Verifies that no AD Administration, AutoPatch, or Patch Manager processes are running.

- Active OPatch Processes Check

  Checks active OPatch processes.

- Locked Objects Check

  Verifies that there are no locked objects in the `FUSION_ODI` or `SES` schema.

- Web Logic Conflict Check

  Verifies that no WLS edit sessions or unactivated changes exist.

10.3.2.2.9 Data Quality Check

The following check occurs when Health Checker runs the `DataQualityChecks.xml` manifest:

- FlexDataCheck

  Validates Flex Data Integrity

10.3.2.2.10 Vital Signs Check

The following checks occur when Health Checker runs the `VitalSignsChecks.xml` manifest:

- Middleware Schema Connectivity

  Checks database connectivity for all schemas except for `FUSION_MDS` schemas.

- Fusion Read Only Schema Validation

  Validates database connectivity for Fusion read only schemas.

- Database Instance Connectivity

Checks if the database instance is up. For RAC databases, checks if all nodes are up.

- Fusion Schema Validation

  Validates database connectivity to all Fusion schemas.

- MDS Schema Validation

  Checks database connectivity for MDS schemas.

- Identity Store Connectivity

  Verifies that the `idstore.ldap.provider` in `jps-config-jse.xml` can be used to connect to the identity store.

- Validate LDAP Connectivity

  Verifies the connectivity to the identity store and policy store LDAP using identity store credentials.

- Verify Server Status

  Verifies that all Administration and Managed Servers are up.

10.3.2.3 Override Health Checks

The Health Checker utility offers a method to manage which health checks run on the Oracle Fusion Applications environment. For example, a health check that is related to a known issue in an environment may need to be excluded. The configuration parameters for Health Checker are stored in the *`REPOSITORY_LOCATION`*`/installers/farup/Disk1/upgrade/config/healthchecks.xml` file. This file cannot be edited. If there is a need to override any configuration parameters or exclude certain plug-ins from running, it is possible to 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.

The Health Checker override files are staged under `SHARED_UPGRADE_LOCATION/healthchecker/common` as follows:

```
all_overrides.xml

FA_pods_overrides.xml.template
```

Where `SHARED_UPGRADE_LOCATION` is a property defined in the pod.properties file.

The following topics are discussed in this section:

- Health Checker Overrides Across the Fleet
- Health Checker Overrides Customization
- Exclude a Plug-in in FA_pods_overrides.xml
- Exclude a Plug-in in FA_pods_overrides.xml for a Single Pod
- Exclude a Plug-in in FA_pods_overrides.xml for Multiple Pods
- Customization: Re-enable a Plug-in that is Disabled in all_overrides.xml
- Exclude a Plug-in with More Granularity

10.3.2.3.1 Health Checker Overrides Across the Fleet

The `all_overrides.xml` file will define plug-in exclusions. These exclusions are applicable across the fleet. Checks disabled out of the box, and checks disabled due to emergency patch will be combined in this file. This file cannot be edited.

10.3.2.3.2 Health Checker Overrides Customization

The file `FA_pods_overrides.xml` can be used to define custom/pod-specific check exclusions. If there is a need to exclude a specific plugin, or to re-enable one of the excluded plugins, use this file as it will have higher precedence than `all_overrides.xml`.

If the `FA_pods_overrides.xml` file is already there, continue using it. If you do not have the file, then make a copy of `FA_pods_overrides.xml.template`, and rename it to `FA_pods_overrides.xml` as follows, all in one command line:

```
cp SHARED_UPGRADE_LOCATION/healthchecker/common/FA_pods_overrides.xml.template
SHARED_UPGRADE_LOCATION/healthchecker/common/FA_pods_overrides.xml
```

10.3.2.3.3 Exclude a Plug-in in FA_pods_overrides.xml

To disable a plug-in, first find its plug-in ID, which can be found on the manifest file in Health Checker Manifests. The following example shows where the plug-in ID is defined in a Health Checker manifest file:

```
<plugin id="DiskSpaceCheckPlugin"
  description="Verifying Free Disk Space"
  invoke="$HC_LOCATION/config/diskfree_checks.xml"
  plugin.class="oracle.check.diskfree.plugin.DiskSpaceCheckPlugin"
```

To override the plug-in in the `FA_pods_overrides.xml` file using the plug-in ID, perform the following steps:

Note that to-be-excluded plug-ins must be listed under the "exclude" category in `FA_pods_overrides.xml`.

1. Open and edit the `FA_pods_overrides.xml` file.
2. Add the following values:

   If the `<checks category="exclude">` tag already exists in the `FA_pods_overrides.xml` file, only the second line, which defines the specific check to be excluded, needs to be added to the file.

   ```
   <checks category="exclude">
    <check name="DiskSpaceCheckPlugin"/>
   </checks>
   ```

   This exclusion applies to all pods as it does *not* contain the `pod_name` attribute.

10.3.2.3.4 Exclude a Plug-in in FA_pods_overrides.xml for a Single Pod

To exclude `FusionSchemaValidation` for a pod named *abc*, perform the following steps:

1. Open and edit the `FA_pods_overrides.xml` file.
2. Add the following values specifying the `pod_name` attribute:

If the `<checks category="exclude">` tag already exists in the `FA_pods_overrides.xml` file, only the second line, which defines the specific check to be excluded, needs to be added to the file.

```
<checks category="exclude">
 <check name="FusionSchemaValidation" pod_name="abc"/>
</checks>
```

10.3.2.3.5 Exclude a Plug-in in FA_pods_overrides.xml for Multiple Pods

To exclude the `FusionSchemaValidation` plugin for pods *abc*, *xxx*, and *zzz*, perform the following steps:

1. Open and edit the `FA_pods_overrides.xml` file.
2. Add the following values specifying the `pod_name` attribute:

   If the `<checks category="exclude">` tag already exists in the `FA_pods_overrides.xml` file, only the second line, which defines the specific check to be excluded, needs to be added to the file.

   ```
   <checks category="exclude">
    <check name="FusionSchemaValidation" pod_name="abc,xxx,zzz"/>
   </checks>
   ```

   Pod names must be comma-separated without spaces.

10.3.2.3.6 Customization: Re-enable a Plug-in that is Disabled in all_overrides.xml

The following example shows an exclusion in the `all_overrides.xml` file:

```
<checks category="exclude">
 <check name="TablespaceCheckPlugin"/>
</checks>
```

To re-enable the `TablespaceCheckPlugin` for all pods, perform the following steps:

1. Open and edit the `FA_pods_overrides.xml` file.
2. Add the “disable” and set to "true" as follows:

   ```
   <checks category="exclude">
    <check name="TablespaceCheckPlugin" disabled="true"/>
   </checks>
   ```

   In this case, `disabled="true"` means that exclusion of a given check is disabled. The check will be performed by Health Checker.

10.3.2.3.7 Exclude a Plug-in with More Granularity

It is possible to exclude a plug-in for a specific host, a specific version of the Oracle Fusion Cloud Application, or a combination of both.

The following example shows how to exclude only the `DiskSpaceCheckPlugin` from running on the OHS host and for the Oracle Fusion Cloud Application version 11.12.0.0.0:

```
<checks category="exclude">
 <!-- Exclude diskspace check on the OHS host -->
 <check name="DiskSpaceCheckPlugin" host="OHS"/>
 <!-- Exclude diskspace check if installed version in APPLTOP is 11.12.0.0.0 -->
 <check name="DiskSpaceCheckPlugin" fa_version="11.12.0.0.0"/>
```

```
 <!-- Exclude diskspace check on OHS host if installed FA version is 11.12.0.0.0 -->
 <check name="DiskSpaceCheckPlugin" host="OHS" fa_version="11.12.0.0.0"/>
</checks>
```

For the value of the host attribute, use one of the following options:

- PRIMORDIAL
- MIDTIER
- OHS

10.3.3 RUP Lite for OVM Utility

The **RUP Lite for OVM** utility addresses the differences between a newly provisioned Oracle Virtual Machine (VM) environment on the latest release and an Oracle VM environment provisioned in a previous release. Run RUP Lite for OVM only if Oracle Fusion Applications is running 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 is an example location for running RUP Lite for OVM in offline mode:

```
/u01/APPLTOP/instance/lcm/rupliteovm/output/11.12.x.0.0/mycompany.com/
rupliteoffline.log
```

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. The following table describes the plug-ins that are included in RUP Lite for OVM in pre-root mode.

Table 10-7 Pre-Root Plug-ins for RUP Lite for OVM

Plug-in Name	Mandatory	Description
RequireRoot	Yes	Sets the require root flag to true so that RUP Lite for OVM checks that the root user is used for the pre-root mode.
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.
AutoCorrectEtcHosts	Yes	Executes for both primary and standby PODs and calls the EtcHosts utility, which in turn corrects the `/etc/hosts` file on each node by comparing it to a "holy grail" properties file supplied by SDI. This plugin does not use checkpointing since it relies on the EtcHosts utility to determine whether to execute or not.
InstallStartStopInitd	Yes	Installs `'idmstartstop'` under `/etc/init.d` for all the IDM hosts, whereas for all the other hosts, it installs `'fastartstop'` under `/etc/init.d`.

Table 10-7 (Cont.) Pre-Root Plug-ins for RUP Lite for OVM

Plug-in Name	Mandatory	Description
ModifyOutputOwner	Yes	Modifies RUP Lite for OVM files to be owned by the application user instead of root. It is targeted primarily for output files that are created as root-owned files during RUP Lite for OVM execution.

The following table describes the plug-ins that are included in RUP Lite for OVM in offline mode.

Table 10-8 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.
GenerateOptimizedQueryPlans	Yes	Generates optimized query plans for Oracle MDS queries.
CreatePodscratchDirs	No (On-Premise) Yes (SaaS Only)	Reuses the metadata file that has the list of directories to be created from rehydration. This metadata file is packaged and placed under `ovm/metadata/deployprops`. Once the metadata is parsed the directories are created sequentially if not already present. This plug-in should also be executed on the stand-by pod.

The following table describes the plug-ins that are included in RUP Lite for OVM in online mode.

Table 10-9 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.
SetupCredentials	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.

Table 10-9 (Cont.) Online Plug-ins for RUP Lite for OVM

Plug-in Name	Mandatory	Description
DeployECSF	Yes	Deploys ECSF artifacts that are not yet deployed, such as search objects, search categories, and index schedules.

Table 10-10 Post-Root Plug-ins for RUP Lite for OVM

Plug-in Name	Mandatory	Description
RequireRoot	N/A	N/A
ValidateEnvironment	Yes	Checks if the node is a valid Oracle VM node. This plug-in always runs and does not have any properties.
SetupCredentials	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.
ModifyOutputOwner	Yes	Modifies RUP Lite for OVM files to be owned by the application user instead of root. It is targeted primarily for output files that are created as root-owned files during RUP Lite for OVM execution.

10.3.4 RUP Lite for OHS Utility

The **RUP Lite for OHS** utility manages the steps required to update WebGate, WebTier, 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.
- Apply OPatches from the repository to WebGate, WebTier, and *ORACLE_COMMON*.
- Apply manually downloaded OPatches to WebGate, WebTier, and *ORACLE_COMMON*.
- Update the OHS configuration files.
- Apply OHS settings changes.
- Re-register OHS.
- Start the OPMN server process.
- Start the OHS instance.

10.3.5 RUP Lite for BI Utility

The **RUP Lite for BI** utility automates changes to `BIInstance` configurations files required for Oracle Business Intelligence after upgrading.

11
Upgrade Orchestrator Properties Files

This section describes the properties files used by Upgrade Orchestrator. Orchestration reads the properties defined in the following five properties files. The properties files are required by Upgrade Orchestrator:

- pod.properties
- PRIMORDIAL.properties
- MIDTIER.properties
- IDM.properties
- OHS.properties

The properties are set to specific values as part of the preparation to begin the upgrade. To configure any property, follow the instructions for each property's description in the respective property file. Note that even if an optional property is not relevant for your environment, leave the property null and do not remove it from the properties file.

11.1 pod.properties

The following tables provides a description of the pod.properties:

Table 11-1 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.

Table 11-1 (Cont.) pod.properties

Property Name	Mandatory	Description
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.
HOSTNAME_PRIMARY	Yes, for Oracle VM	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, for Oracle VM	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, for Oracle VM	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 Web Tier (APPOHS).
HOSTNAME_IDMOID	Yes	Host name, virtual or actual, of the OID server, for example, *host_name*.oracleoutsourcing.com.
HOSTNAME_IDMOIM	Yes	Host name, virtual or actual, of the OIM server, for example, *host_name*.oracleoutsourcing.com.
HOSTNAME_IDMOHS	Yes	Host name, virtual or actual, of the AuthOHS server, for example, *host_name*.oracleoutsourcing.com.
HOSTNAME_GRC	No	Comma separated list of all host names for the VM GRC. This is an optional property for the midtier. Any host names present in this property must also be present in the HOSTNAME_MIDTIER property.
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.

Table 11-1 (Cont.) pod.properties

Property Name	Mandatory	Description
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.
SMTP_SOCKETFACTORY_CLASS	No	The factory class name to connect to the SMTP server.
REL12_REPOSITORY_LOCATION	Yes	The location where the Release 12 repository is downloaded to a shared mount, for example *SHARED_LOCATION*/11.12.x.0.0/Repository. As a best practice, it should be on the shared mount that is shared across all pods or environments.
REL12_LP_REPOSITORY_LOCATION	Yes, if upgrading languages	The location of all Release 12 Language Pack repositories, as described in Download and Unzip Release 12 Language Packs. As a best practice, this directory should be on a shared mount point that is shared across all pods or environments, for example, *SHARED_LOCATION*/11.12.x.0.0/LPRepository.
REL12_RUPINSTALLER_UPGRADE_PARAM	Yes, for non-Oracle VM	Enter the location for the override file that was created in Create an Override File for RUP Installer. It is also possible to provide a space separated list of command line options passed to the RUP and Language Pack installers. For a list of options, see Table 16-2 in the *Oracle Fusion Applications Installation Guide*. If this parameter is set manually, use only -D options. Do not use -J-D options.
SKIP_UPGRADE_FOR_LANGUAGE	No	A comma separated list of languages that you do not want orchestration to upgrade. The list items must: • Meet ISO language code convention. If the ISO_LANGUAGE code is the same for more than one TERRITORY, enter the format of *ISO_LANGUAGE_ISO_TERRITORY*. For example, if ISO_LANGUAGE code is zh, need to enter either zh_TW or zh_CN but not zh. • Be a previously installed language • Not be the JAZN policy store language

Table 11-1 (Cont.) pod.properties

Property Name	Mandatory	Description
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. It is possible to 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_ROLLBACK_UTILITY_LOCATION	Yes	The location of the patch rollback automation utility created in Download and Unzip the Patch Rollback Automation Script. The default value is `/u01/PatchRollbackUtil`.
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.
REL12_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`*`/11.12.x.0.0/fasaaslcmtools` is an example.
ORCH_REPORT_LOCATION	Yes	A shared location accessible to all hosts that is used to save the orchestration report, as described in Oracle Fusion Applications Orchestration Report.
REL12_DOWNLOADED_PATCHES_LOCATION	No	The location of the post-Release 12 patches that are identified as critical to prevent upgrade failures, as described in Download and Unzip Mandatory Post-Release 12 Patches. This directory should be on a shared mount point shared across all hosts and ideally all pods, for example, *`SHARED_LOCATION`*`/11.12.x.0.0/11.12.x.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 not applicable.
ORCH_JVM_OPTIONS	No	This property is not applicable.

Table 11-1 (Cont.) pod.properties

Property Name	Mandatory	Description
RUN_PREDOWNTIME_CHECKS	No	This property indicates whether orchestration runs the pre-downtime health checks and the preValidation check in IDM hosts. By default, this property is set to false to indicate that orchestration does not run pre-downtime checks on any host. It is recommended that you do not enable this property by setting its value to true unless otherwise required.
PERFORM_INCREMENTAL_PROVISIONING	Yes	This property can be set to true to indicate that Incremental Provisioning should be performed by orchestration. The default value is false.
INC_PROV_BINARY_HOME	Yes, conditionally, see Description	This property is the path to the directory where incremental provisioning binaries are installed. This location must be accessible from all hosts within a POD. If the directory already exists, it must be empty before orchestration runs. This property is mandatory if PERFORM_INCREMENTAL_PROVISIONING is set to true; it is ignored otherwise.
RESPONSE_FILES_DIR_LOC	No	This property is applicable only if the PERFORM_INCREMENTAL_PROVISIONING property is set to true.
EMAIL_STARTNOTIFICATION_DELAY	No	The default value is 120 (seconds), and the value should be in the range of [0,300], which represents no delay to a maximum 5 minutes delay for email notifications.
EMAIL_LEVEL	Yes	This property describes the level of email notifications that users receive from Upgrade Orchestration. It is set to INFO by default. Valid values are: • INFO: Users receive all emails • ALERT: Users receive alert and pause point emails • PAUSEPOINT: Users receive only pause point emails • NONE: No emails are sent
FA_CURRENT_VERSION	Yes	The current release of your Oracle Fusion Applications environment, for example, 11.1.8.0.0 or 11.1.9.1.0.
FA_TARGET_VERSION	Yes	The release of Oracle Fusion Applications to which you want to upgrade this environment, such as 11.12.x.0.0.
RUN_LP_FROM_HOST	Yes, if language packs are installed	The host on which you run Language Pack Installer. This must be one of the Primordial or Midtier hosts.
SMARTCLONE_ENABLED	Yes	This property indicates whether the pod is SmartClone enabled. Valid values are true and false. The default value is false.

11.2 PRIMORDIAL.properties

The following tables provides a description of the PRIMORDIAL.properties:

Table 11-2 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. For the Release 12 upgrade, the value should be *ORCH_LOCATION*/config/rel12_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/jdk.
PRE_UPGRADE_JRE_LOC	Yes	The absolute path where the Java Runtime Environment is installed during pre-upgrade activities. This property does not support relative paths. The default value is /u01/APPLTOP/fusionapps/jdk6.
CSF_ENCRYPTED_FILE	Yes	The absolute path and file name for the CSF encrypted file generated by the iniGen.sh script. This property is used by Orchestration to pass the value to schemaPasswordChangeTool.sh. • If you use -output *file_name* to specify an output file name, the value of this property is: *PCU_LOCATION*/fusionapps/applications/lcm/util/config/*file_name*.ini • If you do not specify an output file name, iniGen.sh generates the following: *PCU_LOCATION*/fusionapps/applications/lcm/util/config/csf_encrypted.ini Note that PCU_LOCATION is defined in PRIMORDIAL.properties also.
PCU_LOCATION	Yes	The temporary location where pcubindle.zip is unzipped in Prepare to Register Database Schema Information.
CSF_SYSTEM_USERS_ENCRYPTED_INI	Yes	The absolute path and file name for the encrypted .ini file for adding new system users. An example is *PCU_LOCATION*/fusionapps/applications/lcm/util/config/system_user_encrypted.ini. Note that PCU_LOCATION is defined in PRIMORDIAL.properties also.
REL12_FASAAS_INSTALLER_DIR	Yes, if SAAS_ENV is true	The absolute path to the Saas Home installer directory. This is relevant only to SaaS environments and is ignored on non-SaaS environments.

11.3 MIDTIER.properties

The following tables provides a description of the MIDTIER.properties:

Table 11-3 MIDTIER.properties

Property Name	Mandatory	Description
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 the Release 12 upgrade, the value should be *`ORCH_LOCATION`*`/config/rel12_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/jdk`.
PRE_UPGRADE_JRE_LOC	Yes	Path where Java Runtime Environment (version 6) is installed during pre-upgrade activities for a Release 12 Upgrade. In Release 12 JDK is upgraded from JDK6 to JDK7.

11.4 IDM.properties

The following tables provides a description of the IDM.properties:

Table 11-4 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 the Release 12 upgrade, the value should be *`ORCH_LOCATION`*`/config/rel12_idm.xml`.
JRE_LOC	Yes	The path where the Java Runtime Environment is installed.
IDM_SETUP_TYPE	Yes	The IDM Upgrade is supported by Upgrade Orchestrator, if your deployment is a Linux-64 bit platform and is Release 7 IDM provisioned. This property indicates topology configuration of the system to be upgraded.
REL12_IDM_UPGRADE_BINARIES_LOCATION	Optional	The location where Release 12 IDM binaries are downloaded, for example *`SHARED_LOCATION`*`/11.12.x.0.0/idmUpgrade`. This property is not used for the manual IDM upgrade.

Table 11-4 (Cont.) IDM.properties

Property Name	Mandatory	Default Value
REL12_IDM_UPGRADE_AUTOMATION_PROPERTIES_FILE	Optional	The absolute location of the `upgradeOnpremise.properties` file to be used by the Release 12 IDM upgrade scripts. All properties related to IDM nodes (OID, OIM and OHS) are maintained in this file. This property is not used for the manual IDM upgrade.
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.
PERL_LOCATION	Yes	The location where Perl binary is installed. The default value is `/usr`.

11.5 OHS.properties

The following tables provides a description of the OHS.properties:

Table 11-5 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 the Release 12 upgrade, the value should be *`ORCH_LOCATION`*`/config/rel12_ohs.xml`.
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. The default value 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, `/APPTOP/webtier_mwhome`. 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.

Table 11-5 (Cont.) OHS.properties

Property Name	Mandatory	Default Value
WT_ORACLE_HOME	Yes	Location of the Web Tier instance configuration home, for example, `/APPTOP/webtier_mwhome/webtier`. 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 webtier directory location on the specific host.
WT_CONFIG_HOME	Yes	Location of the Web Tier instance directory, for example, `/APPTOP/instance/CommonDomain_webtier`. 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.
SUPPLIER_PORTAL_VIRTUAL_HOSTNAME	Conditional	The external virtual host name dedicated to the Supplier Portal application. This property is mandatory if the Virtual Host Mode is "NAME". 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 external virtual host name dedicated to the Supplier Portal application on the specific host.
SUPPLIER_PORTAL_VIRTUAL_PORT	Conditional	The external virtual host port dedicated to the Supplier Portal application. This property is mandatory if the Virtual Host Mode is "IP" or "PORT". 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 external virtual host port dedicated to the Supplier Portal application on the specific host.

12

Stop and Start Identity Management Related Servers

This section describes how to start, stop, and restart the various components of the Oracle Enterprise Deployment for Identity Management. The following topics are discussed:

12.1 Start, Stop, and Restart Oracle HTTP Server

Prior to starting or stopping the Oracle HTTP server, perform the following steps:

- 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`*.

12.1.1 Start Oracle HTTP Server

Start the Oracle Web Tier by issuing the following command:

```
opmnctl startall
```

12.1.2 Stop Oracle HTTP Server

Stop the Web Tier by issuing the following command. This command is to stop the entire Web Tier:

```
opmnctl stopall
```

Or issue the following command to stop Oracle HTTP Server only:

```
opmnctl stoproc process-type=OHS
```

12.1.3 Restart Oracle HTTP Server

It is possible to restart the Web Tier by issuing a `Stop` followed by a `Start` command as described in the previous sections.

To restart the Oracle HTTP server only, use the following command:

```
opmnctl restartproc process-type=OHS
```

12.2 Start, Stop, and Restart Oracle Identity Manager

Start and stop Oracle Identity Manager and Oracle SOA Suite servers as described in the following sections:

- Start Oracle Identity Manager
- Stop Oracle Identity Manager
- Restart Oracle Identity Manager
- Start and Stop All IDM Components on a Host

12.2.1 Start Oracle Identity Manager

To start the Oracle Identity Manager Managed Server(s), log in to the WebLogic console at: `http://ADMIN.mycompany.com/console`, 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)**.

   It is possible to 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 the start of the server(s).

12.2.2 Stop Oracle Identity Manager

To stop the Oracle Identity Manager Managed Server(s), log in to the WebLogic console at: `http://ADMIN.mycompany.com/oamconsole`, and 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).

12.2.3 Restart Oracle Identity Manager

Restart the server by following the `Stop` and `Start` procedures in the previous sections.

12.2.4 Start and Stop All IDM Components on a Host

To start and stop all IDM components on a particular host in IDM provisioned environments, you can use the start/stop scripts as described in Starting and Stopping Servers in the *Oracle Fusion Applications Installation Guide*. Ensure the order is maintained when starting/stopping the servers in distributed nodes.

An IDM provisioned environment refers to the Type 1 environment and to the Type 2 only after migration or upgrade are run on it. For more information, see Upgrade Type I IDM Environments and Upgrade Type II IDM Environments.

12.3 Start and Stop Oracle Identity Federation Managed Servers

Start and stop Oracle Identity Federation Managed Servers as described in the following sections:

- Start Oracle Identity Federation
- Stop Oracle Identity Federation
- Restart Oracle Identity Federation
- Start and Stop the EMAgent
- Stop the Oracle Identity Federation Instances and EMAgent

12.3.1 Start Oracle Identity Federation

To start the Oracle Identity Federation Managed Server(s), log in to the WebLogic console at: `http://ADMIN.mycompany.com/oamconsole`, and 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 the start of the server(s).

12.3.2 Stop Oracle Identity Federation

To stop the Oracle Identity Federation Managed Server(s), log in to the WebLogic console at: `http://ADMIN.mycompany.com/oamconsole`, and 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 the shutdown of the server(s).

12.3.3 Restart Oracle Identity Federation

Restart the server by following the previous Stop and Start procedures.

12.3.4 Start and Stop the EMAgent

To start and stop the EMAgent, perform the following steps:

- Start the EMAgent by executing the following command:

  ```
  ORACLE_INSTANCE/bin/emctl start all
  ```

  It is possible to verify that the instance started successfully by executing the following command:

  ```
  ORACLE_INSTANCE/bin/emctl status -l
  ```

- Stop the EMAgent by executing the following command:

  ```
  ORACLE_INSTANCE/bin/emctl stop all
  ```

12.3.5 Stop 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
```

12.4 Start, Stop, and Restart Oracle Access Manager Managed Servers

Start and stop Oracle Access Manager Managed Servers as described in the following sections:

- Start an Access Manager Managed Server When None is Running
- Start an Oracle Access Manager Managed Server When Another is Running
- Stop Oracle Access Manager Managed Servers
- Restart Oracle Access Manager Managed Servers

12.4.1 Start an Access Manager Managed Server When None is Running

Normally, Access Manager managed servers are started by using the WebLogic console. After enabling Single Sign-On for the administration consoles. However, there must be at least one Access Manager Server running in order to access a console. If no Access Manager server is running, the only way to start one is from the command line.

To start WLS_OAM1 manually, use the following command:

```
MSERVER_HOME/bin/startManagedWeblogic.sh WLS_OAM1 t3://ADMINVHN:7001
```

where `7001` is *`WLS_ADMIN_PORT`* in Section 8.3.

12.4.2 Start an Oracle Access Manager Managed Server When Another is Running

To start an Oracle Access Manager Managed Server when there is another already 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 the start of the server(s).

   After enabling single sign-on for the administration consoles, ensure that at least one Oracle Access Manager Server is running to enable console access.

   If the Oracle WebLogic console was used 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
   ```

12.4.3 Stop 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 the shutdown of the server(s).

12.4.4 Restart Oracle Access Manager Managed Servers

Restart the server by following the `Stop` and `Start` procedures in the previous sections.

12.5 Start, Stop, and Restart WebLogic Administration Server

Start and stop the WebLogic Administration Server as described in the following sections:

- Stop WebLogic Administration Server
- Stop WebLogic Administration Server
- Restart WebLogic Administration Server

`Admin_user` and `Admin_Password` are only used to authenticate connections between Node Manager and clients. These are independent from the server administration ID and password and are stored in the *`ASERVER_HOME`*`/config/nodemanager/nm_password.properties` file.

12.5.1 Start 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 the WLST shell, execute

```
nmConnect('Admin_User','Admin_Password','ADMINHOST1','5556',
'IDMDomain','ASERVER_HOME')
nmStart('AdminServer')
```

Alternatively, it is possible to start the Administration server by using the command:

```
DOMAIN_HOME/bin/startWeblogic.sh
```

12.5.2 Stop WebLogic Administration Server

To stop the Administration Server, log in to the WebLogic console at: `http://ADMIN.mycompany.com/oamconsole`, and 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 the shutdown of the Administration Server.

12.5.3 Restart WebLogic Administration Server

Restart the server by following the `Stop` and `Start` procedures in the previous sections.

12.6 Start and Stop Oracle Internet Directory

Start and stop Oracle Internet Directory as described in the following sections:

- Start Oracle Internet Directory
- Stop Oracle Internet Directory

12.6.1 Start Oracle Internet Directory

Start system components such as Oracle Internet Directory by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl startall
```

To verify that the system components have started, execute the following command:

```
ORACLE_INSTANCE/bin/opmnctl status -l
```

12.6.2 Stop Oracle Internet Directory

Stop system components such as Oracle Internet Directory by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl stopall
```

12.7 Start and Stop Node Manager

Start and stop the Node Manager as described in the following sections:

- Start Node Manager
- Stop Node Manager
- Start Node Manager for an Administration Server

12.7.1 Start 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 following commands:

```
cd IAM_MW_HOME/wlserver_10.3/server/bin
./startNodeManager.sh
```

12.7.2 Stop Node Manager

To stop Node Manager, kill the process started in the previous section.

12.7.3 Start Node Manager for an Administration Server

Set the environment variable `JAVA_OPTIONS` to `-DDomainRegistrationEnabled=true` and issue the following commands:

```
cd IAM_MW_HOME/wlserver_10.3/server/bin
./startNodeManager.sh
```

It is important to set `-DDomainRegistrationEnabled=true` whenever starting a Node Manager that manages the Administration Server.

13

Resource Manager Plan - SQL Script

This section contains the contents of the Resource Manager Plan script that must be run after the upgrade, if Oracle Fusion Applications is running on an Oracle Virtual Machine (VM) environment. This script can be used to create FUSION Resource plan in Oracle 11*g* as well as in Oracle 12*c* for both PDB and Non-CDB.

To apply the FUSIONAPPS_PLAN (Resource Manager Plan) post upgrade, run the following SQL script as the privileged database user (SYSTEM/SYS):

```
SET LINES 200 PAGES 300
WHENEVER SQLERROR EXIT

DECLARE
comp varchar2(20);
pdbs varchar2(20);
USRROW NUMBER(2):= 0;
BEGIN
select substr(value,1,2) into comp from v$parameter where name='compatible';
SELECT COUNT(1) INTO USRROW FROM user_role_privs WHERE GRANTED_ROLE='DBA';
    IF USRROW=0 THEN
      RAISE_APPLICATION_ERROR (-20100, 'Insufficient privileges. You need DBA
privileges to run this script.');
    END IF;

IF comp>11 then
select sys_context('userenv','con_name') into pdbs from dual;
   IF pdbs='CDB$ROOT' then
   RAISE_APPLICATION_ERROR (-20111, 'Please run this script connnecting as FUSION
PDB, You are connected to CDB.');
   END iF;
END IF;

  DBMS_RESOURCE_MANAGER.CLEAR_PENDING_AREA();
  DBMS_RESOURCE_MANAGER.CREATE_PENDING_AREA();

  --Removing FUSIONAPPS_PLAN from scheduler windows before deleting
  begin
    for REC in  (select WINDOW_NAME from DBA_SCHEDULER_WINDOWS where RESOURCE_PLAN =
'FUSIONAPPS_PLAN' )  LOOP
        DBMS_SCHEDULER.SET_ATTRIBUTE (rec.window_name,'resource_plan','');
    end LOOP;
  end;

  begin
    DBMS_RESOURCE_MANAGER.SWITCH_PLAN( PLAN_NAME => '');
    DBMS_RESOURCE_MANAGER.DELETE_PLAN('FUSIONAPPS_PLAN');
  EXCEPTION WHEN OTHERS THEN NULL;
  END;

  BEGIN
    dbms_resource_manager.delete_consumer_group(CONSUMER_GROUP =>
'FUSIONAPPS_ONLINE_GROUP');
  EXCEPTION  WHEN OTHERS THEN NULL;
  END;
```

```
  BEGIN
    dbms_resource_manager.delete_consumer_group(CONSUMER_GROUP =>
'FUSIONAPPS_BATCH_GROUP');
  EXCEPTION  WHEN OTHERS THEN NULL;
  END;

  BEGIN
    dbms_resource_manager.delete_consumer_group(CONSUMER_GROUP =>
'FUSIONAPPS_DIAG_GROUP');
  EXCEPTION  WHEN OTHERS THEN NULL;
  END;

  dbms_resource_manager.create_consumer_group(CONSUMER_GROUP =>
'FUSIONAPPS_ONLINE_GROUP', COMMENT => 'Consumer Group for online users');
  dbms_resource_manager.create_consumer_group(CONSUMER_GROUP
=>'FUSIONAPPS_BATCH_GROUP', COMMENT => 'Consumer Group for batch');

  dbms_resource_manager.create_consumer_group(CONSUMER_GROUP
=>'FUSIONAPPS_DIAG_GROUP', COMMENT => 'Consumer Group for FUSION_RO and FUSION_ERO');
  dbms_resource_manager.create_plan(PLAN => 'FUSIONAPPS_PLAN', COMMENT => 'Fus
Applications Resource Plan');

  DBMS_RESOURCE_MANAGER.CREATE_PLAN_DIRECTIVE( plan => 'FUSIONAPPS_PLAN',
                                               GROUP_OR_SUBPLAN =>
'FUSIONAPPS_ONLINE_GROUP',
                                               comment => 'Online users at level 1',
                                               MGMT_P1 => 35,
                                               PARALLEL_DEGREE_LIMIT_P1 => 0,
                                               SWITCH_TIME => 1200,
                                               SWITCH_IO_MEGABYTES => 10000,
                                               SWITCH_GROUP => 'CANCEL_SQL',
                                               switch_for_call => TRUE );

  DBMS_RESOURCE_MANAGER.CREATE_PLAN_DIRECTIVE( plan => 'FUSIONAPPS_PLAN',
                                               GROUP_OR_SUBPLAN =>
'FUSIONAPPS_BATCH_GROUP',
                                               comment => 'Batch users at level 1',
                                               MGMT_P1 => 25);

  DBMS_RESOURCE_MANAGER.CREATE_PLAN_DIRECTIVE( plan => 'FUSIONAPPS_PLAN',
                                               GROUP_OR_SUBPLAN => 'SYS_GROUP',
                                               comment => 'System administrator
group at level 1',
                                               MGMT_P1 => 10);

  DBMS_RESOURCE_MANAGER.CREATE_PLAN_DIRECTIVE( plan => 'FUSIONAPPS_PLAN',
                                               GROUP_OR_SUBPLAN => 'OTHER_GROUPS',
                                               comment => 'Other users at level 1',
                                               MGMT_P1 => 5);

  --Add directives for maintenance and diag process during maintenance windows
  --Note: These allocations are only active during maintenance windows.

      IF pdbs<>'CDB$ROOT' and comp='12' then
        DBMS_RESOURCE_MANAGER.CREATE_PLAN_DIRECTIVE( plan => 'FUSIONAPPS_PLAN',
                                               GROUP_OR_SUBPLAN => 'ORA$AUTOTASK',
                                               comment => 'Maintenance Tasks',
                                               MGMT_P1 => 20);
      ELSE IF comp<>'12' then
      DBMS_RESOURCE_MANAGER.CREATE_PLAN_DIRECTIVE( plan => 'FUSIONAPPS_PLAN',
```

```
                                                GROUP_OR_SUBPLAN =>
'ORA$AUTOTASK_SUB_PLAN',
                                                comment => 'Maintenance Tasks',
                                                MGMT_P1 =>
15);

      DBMS_RESOURCE_MANAGER.CREATE_PLAN_DIRECTIVE( plan => 'FUSIONAPPS_PLAN',
                                                GROUP_OR_SUBPLAN =>
'ORA$DIAGNOSTICS',
                                                comment => 'Background Diag
Processes',
                                                mgmt_P1 => 5);
     END IF;
     END IF;



   DBMS_RESOURCE_MANAGER.CREATE_PLAN_DIRECTIVE( plan => 'FUSIONAPPS_PLAN',
                                                GROUP_OR_SUBPLAN =>
'FUSIONAPPS_DIAG_GROUP',
                                                comment => 'Diagnostic users at level
1',
                                                mgmt_P1 =>
5,

                                                PARALLEL_DEGREE_LIMIT_P1 => 0,
                                                SWITCH_TIME => 120,
                                                SWITCH_IO_MEGABYTES => 10000,
                                                SWITCH_GROUP => 'CANCEL_SQL',
                        MAX_EST_EXEC_TIME => 100,
                                                switch_for_call => TRUE );

  FOR rec IN  (SELECT username FROM dba_users WHERE (username LIKE '%FUSION%'  or
username ='FMW_RUNTIME'))  LOOP
    IF (rec.username = 'FUSION_RO' OR rec.username = 'FUSION_ERO') THEN
      dbms_resource_manager.set_consumer_group_mapping(attribute =>
DBMS_RESOURCE_MANAGER.ORACLE_USER, value => rec.username, CONSUMER_GROUP =>
'FUSIONAPPS_DIAG_GROUP');
    ELSIF (rec.username <> 'FUSION_READ_ONLY') THEN
      dbms_resource_manager.set_consumer_group_mapping(attribute =>
DBMS_RESOURCE_MANAGER.ORACLE_USER, value => rec.username, CONSUMER_GROUP =>
'FUSIONAPPS_BATCH_GROUP');
    END IF;
  end LOOP;

  begin
    DBMS_RESOURCE_MANAGER.SET_CONSUMER_GROUP_MAPPING(attribute =>
DBMS_RESOURCE_MANAGER.ORACLE_USER,value => 'SEARCHSYS', CONSUMER_GROUP =>
'FUSIONAPPS_BATCH_GROUP');
    --Specifically for RMAN: any session running a backup/copy operation with RMAN
is automatically switched to SYS_GROUP when the operation begins.
    DBMS_RESOURCE_MANAGER.SET_CONSUMER_GROUP_MAPPING( attribute =>
DBMS_RESOURCE_MANAGER.ORACLE_FUNCTION, value => 'BACKUP', CONSUMER_GROUP =>
'SYS_GROUP');
    DBMS_RESOURCE_MANAGER.SET_CONSUMER_GROUP_MAPPING( attribute =>
DBMS_RESOURCE_MANAGER.ORACLE_FUNCTION, value => 'COPY', consumer_group =>
'SYS_GROUP');
  EXCEPTION  WHEN OTHERS THEN NULL;
  end;
```

```
  DBMS_RESOURCE_MANAGER.VALIDATE_PENDING_AREA();
  DBMS_RESOURCE_MANAGER.SUBMIT_PENDING_AREA();
  DBMS_RESOURCE_MANAGER.CLEAR_PENDING_AREA();

dbms_resource_manager_privs.grant_switch_consumer_group('PUBLIC','FUSIONAPPS_ONLINE_G
ROUP',FALSE);

DBMS_RESOURCE_MANAGER_PRIVS.GRANT_SWITCH_CONSUMER_GROUP('PUBLIC','FUSIONAPPS_BATCH_GR
OUP',false);

DBMS_RESOURCE_MANAGER_PRIVS.GRANT_SWITCH_CONSUMER_GROUP('PUBLIC','FUSIONAPPS_DIAG_GRO
UP',false);
  --Grant DBA role privilege to switch to SYS_GROUP. Assumption is that any ADMIN
task (including RMAN) will be performed by user with DBA Privileges.
  ---SYS/SYSTEM already map to SYS_GROUP by default.
  DBMS_RESOURCE_MANAGER_PRIVS.GRANT_SWITCH_CONSUMER_GROUP('DBA','SYS_GROUP',FALSE);

  --Associate FUSIONAPPS_PLAN to  all defined maintenance windows
  begin
    for REC in  (SELECT WINDOW_NAME FROM DBA_SCHEDULER_WINDOWS WHERE resource_plan
IS NULL OR RESOURCE_PLAN = '' )  LOOP
        DBMS_SCHEDULER.SET_ATTRIBUTE
(rec.window_name,'resource_plan','FUSIONAPPS_PLAN');
    end LOOP;
  end;

begin
    --Sets the current resource manager plan
    DBMS_RESOURCE_MANAGER.SWITCH_PLAN( PLAN_NAME => 'FUSIONAPPS_PLAN');
  end;


END;
/

--- Setting newly created FUSION resource plan.
alter system set resource_manager_plan='FUSIONAPPS_PLAN' scope=both;
```