July 2014
Documentation for installers and system administrators that describes how to use Upgrade Orchestrator to upgrade Oracle Fusion Applications software between major releases.
# Contents

**Preface** .................................................................................................................................................................................. xi

**What's New in This Guide** .............................................................................................................................................................. xiii

1 **Introduction to the Oracle Fusion Applications Upgrade**
   1.1 Upgrade Process Overview ................................................................................................................................................. 1-1
   1.2 Hosts, Directories, and Files Required by Upgrade Orchestrator ...................................................................................... 1-2
     1.2.1 Host Types ........................................................................................................................................................................ 1-2
     1.2.2 Directories and Files Required by Upgrade Orchestrator .............................................................................................. 1-3
   1.3 Back Up Strategy ................................................................................................................................................................. 1-4
   1.4 Planning Your Downtime ......................................................................................................................................................... 1-4
   1.5 Directories Structure Overview ................................................................................................................................................ 1-5
     1.5.1 Directories Used by Upgrade Orchestrator ..................................................................................................................... 1-5
     1.5.2 Download Directories ......................................................................................................................................................... 1-5
     1.5.3 Relationship of Home Directories ..................................................................................................................................... 1-6
   1.6 Checklist for Performing the Upgrade .................................................................................................................................. 1-6

2 **Preparing to Perform the Release 8 Upgrade**
   2.1 Before You Begin ................................................................................................................................................................. 2-1
   2.2 System Requirements .............................................................................................................................................................. 2-1
     2.2.1 Memory Requirements ......................................................................................................................................................... 2-2
     2.2.2 Free Disk Space Requirements ............................................................................................................................................. 2-2
     2.2.3 Set LBR_PRESENT to True on the Primordial Host .............................................................................................................. 2-3
   2.3 Create Upgrade Directories and Obtain Software ..................................................................................................................... 2-3
     2.3.1 Create a Common User Group and Permissions for Shared Directories ............................................................................... 2-3
     2.3.2 Create Directories in a Shared Location .................................................................................................................................. 2-6
     2.3.3 Create Directories Common to One Environment ............................................................................................................... 2-7
     2.3.4 Download and Unzip the Patch Conflict Manager Utility .................................................................................................. 2-8
     2.3.5 Download and Unzip the Repository and Patches .................................................................................................................. 2-8
     2.3.6 Download the Invalid Objects Patch for Exclusion List ..................................................................................................... 2-11
     2.3.7 Unzip Orchestration.zip ......................................................................................................................................................... 2-12
     2.3.8 Copy and Unzip idmUpgrade.zip .......................................................................................................................................... 2-13
   2.4 Set Up Upgrade Orchestrator .................................................................................................................................................... 2-13
     2.4.1 Set Up Upgrade Orchestrator on a Shared Location ............................................................................................................. 2-13
     2.4.2 Select a Master Orchestration Password ............................................................................................................................. 2-14
3 Updating the Oracle Fusion Applications and Oracle Identity Management Databases

3.1 Apply Exadata Patches for Release 8 ................................................................. 3-1
3.1.1 Quarterly Database Patches ........................................................................ 3-1
3.1.2 Generic Exadata Patches .............................................................................. 3-2
3.1.3 Linux Exadata Patches ................................................................................ 3-2
3.1.4 Solaris Sparc64 Exadata Patches ................................................................. 3-3
3.1.5 Solaris 86 X64 Exadata Patches .................................................................. 3-4
3.2 Run RUP Lite for RDBMS ................................................................................ 3-6
3.2.1 Run RUP Lite for RDBMS ........................................................................... 3-7
3.2.2 Run RUP Lite for RDBMS in a RAC Database ............................................ 3-12
3.2.3 Stop Services on Windows Before Running RUP Lite For RDBMS ............. 3-15
3.2.4 Run Additional Post Database Start Scripts for Patches for Release 8 ........ 3-15

4 Running Pre-Downtime Checks

4.1 Run the Health Checker Utility ........................................................................ 4-1
4.1.1 Pre-Downtime Health Checker Manifests ................................................... 4-1
4.1.2 Run Health Checker on the Primordial Host .............................................. 4-2
4.1.3 Run Health Checker on the Mid Tier Host ................................................ 4-3
4.1.4 Run Health Checker on the OHS Host ...................................................... 4-5
4.1.5 Run Health Checker on the Database Host .............................................. 4-7
4.2 Run the Pre-validation Check on IDM Hosts .................................................. 4-9
4.2.1 Confirm Prerequisite Steps Are Complete ................................................ 4-9
4.2.2 Set Environment Variables .......................................................................... 4-9
4.2.3 Run preValidate.pl on Each Node ............................................................ 4-11
5 Upgrading to Oracle Fusion Applications Release 8

5.1 Steps to Upgrade to Release 8 ................................................................. 5-1
5.1.1 Run Upgrade Orchestrator During Downtime ................................. 5-2
5.1.2 Pause Point 1 - Back Up the OPSS Security Store ............................ 5-4
5.1.3 Update Status to Success ................................................................. 5-4
5.1.4 Resume Upgrade Orchestrator ......................................................... 5-4
5.1.5 Pause Point 2 - Stop Informatica IR (IIR) Servers ............................ 5-5
5.1.6 Update Status to Success ................................................................. 5-5
5.1.7 Resume Upgrade Orchestrator ......................................................... 5-5
5.1.8 Pause Point 3 - Back Up Oracle Fusion Applications ...................... 5-5
5.1.9 Update Status to Success ................................................................. 5-5
5.1.10 Resume Upgrade Orchestrator ......................................................... 5-6
5.1.11 Pause Point 4 - Upgrade Oracle Identity Management to Release 8 5-7
5.1.12 Update Status to Success ................................................................. 5-7
5.1.13 Resume Upgrade Orchestrator ......................................................... 5-8
5.1.14 Pause Point 5 - Start External Servers ............................................. 5-9
5.1.15 Update Status to Success ................................................................. 5-9
5.1.16 Resume Upgrade Orchestrator ......................................................... 5-9
5.1.17 Pause Point 6 - Back Up Oracle Fusion Applications Before Language Pack Upgrade (Language Pack Only) ...................................................... 5-10
5.1.18 Update Status to Success ................................................................. 5-10
5.1.19 Resume Upgrade Orchestrator (Language Pack Only) .................... 5-11
5.1.20 Upgrade Orchestrator Completes Successfully ......................... 5-12
5.2 Pause Point Steps .................................................................................. 5-12
5.2.1 Back Up the OPSS Security Store .................................................... 5-12
5.2.2 Back Up Oracle Fusion Applications ................................................. 5-14
5.2.3 Back Up Oracle Fusion Applications on Windows .......................... 5-15
5.2.4 Run idmUpgrade.pl to Upgrade Oracle Identity Management .......... 5-16
5.2.5 Upgrade the Oracle Identity Management Domain to 11g Release 8 (11.1.8) ............................................. 5-17
5.2.6 Start External Servers ................................................................. 5-24
5.3 Set the SKIP_ROOTPRE Environment Variable (AIX Only) ................ 5-26
5.4 Change the Node Manager Password (Cloned Environment Only) ........ 5-26

6 Running Post-Upgrade Tasks for Oracle Fusion Applications

6.1 Confirm Database Artifact Deployments Were Successful .................. 6-1
6.2 Review the Post RUP Installer Report ............................................... 6-2
6.3 Review the Orchestrator Upgrade Report ........................................... 6-2
6.4 Run the Post Validation Check on Oracle Identity Manager Hosts .......... 6-2
6.5 Review Policy Store (JAZN) Analysis Reports ..................................... 6-3
6.6 Reload Custom Templates for BI Publisher Reports ............................ 6-3
6.7 Add Administration Servers to the Machine Created During Scale Out . 6-4
6.8 Stop and Start Servers to Remove WebChat Connections .................... 6-4
6.9 Confirm the IIR Server is Running ..................................................... 6-4
6.10 Perform Steps in Release Notes ......................................................... 6-4
6.11 Resolve Conflicts That Occurred During Oracle BI Metadata Updates .... 6-5
6.11.1 Resolve Conflicts in the Oracle BI Presentation Catalog ..................... 6-5
7 Monitoring and Troubleshooting the Upgrade

7.1 General Troubleshooting for Upgrade Orchestrator Failures ........................................ 7-1
7.2 Log Locations ................................................................................................................. 7-2
7.2.1 Upgrade Orchestrator Log File Directories ............................................................... 7-2
7.2.2 RUP Installer Log File Directories ............................................................................. 7-8
7.3 Monitoring Upgrade Orchestration Progress .................................................................. 7-9
7.4 Terminating Upgrade Orchestration ................................................................................ 7-10
7.4.1 Terminate an Orchestration Session .......................................................................... 7-11
7.4.2 Clear the Exit Status on All Hosts ............................................................................. 7-11
7.4.3 Get the ExitOrchestration Status .............................................................................. 7-11
7.5 Canceling the Upgrade and Restoring From Backup .................................................... 7-11
7.6 Troubleshooting Upgrade Orchestrator Failures ............................................................ 7-12
7.6.1 Unable to Upload Orchestration Checkpoints .......................................................... 7-12
7.6.2 Safely Exit Upgrade Orchestrator .............................................................................. 7-13
7.6.3 Unable to Find the Orchestrator Upgrade Report After Failure ............................... 7-13
7.6.4 Upgrade Orchestrator Report Fails to Generate Due to Out Of Memory Error .... 7-13
7.6.5 Property Validation Fails Due to Invalid Property Error ........................................... 7-13
7.6.6 Wait for Peer Phase Error After Setting Task to Success Status ............................. 7-14
7.6.7 Unable to Update Task Status From Running to Success ....................................... 7-14
7.6.8 Emails Are Not Being Sent Upon Failure ............................................................... 7-15
7.6.9 Upgrade Orchestrator Does Not Use a Value in the Properties File ....................... 7-15
7.6.10 Stale NFS File Handle Error ..................................................................................... 7-15
7.6.11 Error in Creating_Middleware_Schemas Log ......................................................... 7-15
7.6.12 Cannot Remove Snapshot File Error ....................................................................... 7-16
7.6.13 Informatica Identity Resolution (IIR) Does Not Come Up After the Upgrade .... 7-16
7.6.14 Unable to Initialize the Checkpoint System ............................................................ 7-16
7.6.15 Stop Index Schedule and Deactivate Index Optimization Fails on Primordial Host 7-16
7.7 Troubleshooting Failures During the Installation Phase .................................................. 7-17
7.7.1 CFGLOG-00056: Exception caught while getting node-manager homes ........... 7-17
7.7.2 Invalid Oracle Home .................................................................................................. 7-18
7.7.3 Error in Writing to File, Text File Busy ..................................................................... 7-18
7.7.4 Inventory Pointer File is Empty ................................................................................ 7-19
7.8 Troubleshooting RUP Installer Failures ........................................................................... 7-19
7.8.1 RUP Installer Fails ..................................................................................................... 7-19
7.8.2 Installer Requirement Checks Fail .............................................................................. 7-20
7.8.3 Failure During Apply Pre-PSA Due to Smart Patch Conflict (Oracle VM Only) ........ 7-20
7.8.4 RUP Installer Fails Due To Thread Calls ................................................................... 7-21
7.8.5 Recover From an Installer Session That Was Shut Down ...................................... 7-21
<table>
<thead>
<tr>
<th>Section</th>
<th>Issue Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.6</td>
<td>Deploying New Application Configuration Fails with a &quot;NumberFormatException&quot;</td>
</tr>
<tr>
<td>7.8.7</td>
<td>Importing of Group Space Templates Fails During RUP Installer Part 2</td>
</tr>
<tr>
<td>7.8.8</td>
<td>GST Validation Fails During Import of Group Space Template</td>
</tr>
<tr>
<td>7.8.9</td>
<td>Configuration Assistant Fails Due to &quot;Could not create credential store instance&quot; Error</td>
</tr>
<tr>
<td>7.8.10</td>
<td>First Installer Fails on Primordial Host During Applying Middleware Patchsets</td>
</tr>
<tr>
<td>7.8.11</td>
<td>Importing Oracle Data Integrator Repositories Fails</td>
</tr>
<tr>
<td>7.8.12</td>
<td>Creating Middleware Schema Fails</td>
</tr>
<tr>
<td>7.9</td>
<td>Troubleshooting Node Manager and OPMN failures</td>
</tr>
<tr>
<td>7.9.1</td>
<td>Verifying Node Manager and OPMN Status Fails Due to Bad Certificate Issue</td>
</tr>
<tr>
<td>7.9.2</td>
<td>Stopping OPMN Processes Fails</td>
</tr>
<tr>
<td>7.9.3</td>
<td>Verifying Node Manager and OPMN Status Fails</td>
</tr>
<tr>
<td>7.9.4</td>
<td>Node Manager Does Not Start Between First and Second Installer</td>
</tr>
<tr>
<td>7.10</td>
<td>Troubleshooting RUP Lite for OHS Failures</td>
</tr>
<tr>
<td>7.10.1</td>
<td>RUP Lite for OHS Fails With Missing JDK exception</td>
</tr>
<tr>
<td>7.10.2</td>
<td>RUP Lite for OHS Fails With ReassociateCommonDomain Plug-in</td>
</tr>
<tr>
<td>7.10.3</td>
<td>RUP Lite for OHS Fails With Security Mode Errors</td>
</tr>
<tr>
<td>7.11</td>
<td>Troubleshooting IDM Upgrade Failures</td>
</tr>
<tr>
<td>7.11.1</td>
<td>Communication Exceptions on Primordial Console While Waiting for IDMOHS</td>
</tr>
<tr>
<td>7.11.2</td>
<td>WLS Exception - ESS Server Does Not Respond During Start all Servers</td>
</tr>
<tr>
<td>7.11.3</td>
<td>OAM Configuration Step Fails Due to Special Characters in Password</td>
</tr>
<tr>
<td>7.11.4</td>
<td>Location of GRC Policies in the OAM Applications Domain</td>
</tr>
<tr>
<td>7.11.5</td>
<td>Oracle Identity Federation Application Does Not Start and config.xml is Empty</td>
</tr>
<tr>
<td>7.12</td>
<td>Troubleshooting Applying Middleware Patches</td>
</tr>
<tr>
<td>7.12.1</td>
<td>Log Files for Applying Middleware Patches</td>
</tr>
<tr>
<td>7.12.2</td>
<td>Applying Middleware Patchsets Fails Due to DISPLAY</td>
</tr>
<tr>
<td>7.12.3</td>
<td>Applying Post-PSA Middleware Patchsets Hangs</td>
</tr>
<tr>
<td>7.12.4</td>
<td>Applying Database Client Patches Fails</td>
</tr>
<tr>
<td>7.12.5</td>
<td>ORA-01658: unable to create INITIAL extent for segment in tablespace</td>
</tr>
<tr>
<td>7.12.6</td>
<td>Upgrading Middleware Schema Fails</td>
</tr>
<tr>
<td>7.12.7</td>
<td>Applying Downloaded Patches Fails</td>
</tr>
<tr>
<td>7.13</td>
<td>Troubleshooting Loading Database Components</td>
</tr>
<tr>
<td>7.13.1</td>
<td>Failure During Granting Privileges</td>
</tr>
<tr>
<td>7.13.2</td>
<td>Workers Fail While Loading Database Components</td>
</tr>
<tr>
<td>7.13.3</td>
<td>Database Failure While Loading Database Components</td>
</tr>
<tr>
<td>7.13.4</td>
<td>AutoPatch Validation Fails</td>
</tr>
<tr>
<td>7.13.5</td>
<td>Flexfield Seed Data Upload Fails</td>
</tr>
<tr>
<td>7.13.6</td>
<td>Loading Database Components Fails When JDBC URL is Null</td>
</tr>
<tr>
<td>7.13.7</td>
<td>Active FAPatchMgr Sessions Are Found</td>
</tr>
<tr>
<td>7.13.8</td>
<td>Patch Manager Fails Due to Unique Constraint While Running Abort</td>
</tr>
<tr>
<td>7.14</td>
<td>Troubleshooting Deployment of Applications Policies</td>
</tr>
<tr>
<td>7.14.1</td>
<td>Log Files for Deploying Application Policies</td>
</tr>
<tr>
<td>7.14.2</td>
<td>Applications Policies Analysis Fails</td>
</tr>
<tr>
<td>7.14.3</td>
<td>Deploying Applications Policies Fails</td>
</tr>
<tr>
<td>7.14.4</td>
<td>Deploying Applications Policies Reports a Warning</td>
</tr>
</tbody>
</table>
Deploying Applications Policies Reports a Warning during Migrate Security Store ............................................. 7-41
IDM Server Fails During Deployment of Applications Policies ........................................................................... 7-41
Troubleshooting Server Start and Stop Failures ........................................................................................................ 7-41
Starting All Servers Fails Due to Time Outs ........................................................................................................... 7-42
Starting All Servers Fails to Start BIServer ........................................................................................................... 7-42
Startup Fails for CommonDomain: OHSComponent (Oracle VM Only) ................................................................. 7-43
Online Preverification Reports EditTimedOutException Error ............................................................................... 7-44
Server Startup Reports WLS SocketTimeoutException ......................................................................................... 7-44
The SOA-infra Application is in a Warning State ................................................................................................. 7-44
The SOA-infra Application is in a Warning State on All Domains ........................................................................ 7-44
Custom Domains Fail to Start or Stop .................................................................................................................... 7-45
StartAllServers Task Fails After Language Pack Upgrade on CRM ....................................................................... 7-45
Troubleshooting SOA Composite Deployment Failures ......................................................................................... 7-45
SOA Composite Log Files ....................................................................................................................................... 7-46
SOA Composite Failure Does Not Recover ........................................................................................................... 7-46
Wsm-pm Application is not Running in Domain (Solaris Only) .................................................................................. 7-47
Manually Deploying SOA Composites .................................................................................................................... 7-47
Invoking an Instance of SOA Composite ................................................................................................................. 7-48
Merging SOA Composite JDeveloper Customizations During SOA Preverification ................................................ 7-48
Troubleshooting RUP Lite for OVM Failures ........................................................................................................... 7-49
Troubleshooting RUP Lite for OVM Plug-in Failures .............................................................................................. 7-49
RUP Lite for OVM Hangs During Domain Configuration ...................................................................................... 7-50
Troubleshooting Health Checker Failures and Errors .............................................................................................. 7-50
Upgrade Readiness Checks Fail During Pre-Downtime ......................................................................................... 7-50
DomainsFileOwnership Health Check Fails With Permissions Issues ..................................................................... 7-51
Context Root Check Health Check Fails ................................................................................................................ 7-52
Resolve JAZN Conflicts Found by Health Checker .............................................................................................. 7-52
Failure Due to oracle.sysman.oii.oii.OiitTargetLockNotAvailable Exception ....................................................... 7-53
Troubleshooting Other Issues During the Upgrade ............................................................................................... 7-53
Perl lib Version is not Compatible ........................................................................................................................ 7-53
Policy Store and Oracle Platform Security Services Versions Are Not Compatible ................................................ 7-54
Bootstrapping Patch Manager Fails ....................................................................................................................... 7-54
Propagating Domain Configuration Fails .............................................................................................................. 7-54
Upgrade Failures on Non-Oracle VM Configuration Using OVM Templates ......................................................... 7-56
RUP Lite for Domain Configuration Takes Too Long to Complete ....................................................................... 7-56
Deployment of BI Publisher Artifacts Fails ............................................................................................................. 7-56
Importing IPM Artifacts Fails .................................................................................................................................. 7-56
Extending Certificate Validation Fails on non-Oracle VM Environment ................................................................. 7-57
Multiple Warnings in Data Security Grants Logs .................................................................................................. 7-57
Ignorable Errors Reported by catbundle.sql ........................................................................................................ 7-58
Ignorable Errors During Applying Online BI Metadata and Configuration Updates ................................................ 7-58
Platform Specific Troubleshooting Issues ............................................................................................................... 7-58
Windows Troubleshooting Issues .......................................................................................................................... 7-59
Solaris Troubleshooting Issues ............................................................................................................................. 7-60
AIX Troubleshooting Issues .................................................................................................................................... 7-61
A Additional Information About Upgrade Orchestrator
A.1 Upgrade Orchestrator Features ................................................................. A-1
A.1.1 Upgrade Phases .............................................................................. A-1
A.1.2 Pause Points .................................................................................. A-1
A.1.3 Oracle Fusion Applications Orchestrator Upgrade Report .................. A-2
A.1.4 Language Upgrade ........................................................................ A-3
A.2 Additional Information About Upgrade Orchestrator Commands .......... A-3
A.2.1 Upgrade Orchestrator Command Arguments .................................... A-3
A.2.2 Options for the Orchestration Command When Starting Orchestration A-4
A.2.3 Options for the Orchestration updateStatus Command ....................... A-4
A.2.4 Options for the OrchestrationgetStatus Command ............................. A-5
A.2.5 The validatesetup Argument ............................................................. A-5
A.3 Utilities Run by Upgrade Orchestrator .................................................. A-5
A.3.1 RUP Installer ................................................................................. A-6
A.3.2 Health Checker Utility ...................................................................... A-15
A.3.3 RUP Lite for OVM Utility ................................................................. A-29
A.3.4 RUP Lite for OHS Utility ................................................................. A-31
A.3.5 RUP Lite for BI Utility ................................................................. A-31

B Upgrade Orchestrator Properties Files
B.1 pod.properties ...................................................................................... B-1
B.2 PRIMORDIAL.properties ..................................................................... B-4
B.3 MIDTIER.properties .......................................................................... B-5
B.4 IDM.properties ................................................................................... B-5
B.5 OHS.properties .................................................................................. B-6

C Stopping and Starting Identity Management Related Servers
C.1 Starting, Stopping, and Restarting Oracle HTTP Server .......................... C-1
C.1.1 Starting Oracle HTTP Server ............................................................. C-1
C.1.2 Stopping Oracle HTTP Server ........................................................... C-1
C.1.3 Restarting Oracle HTTP Server ......................................................... C-2
C.2 Starting, Stopping, and Restarting Oracle Identity Manager .................. C-2
C.2.1 Starting Oracle Identity Manager ....................................................... C-2
C.2.2 Stopping Oracle Identity Manager ..................................................... C-2
C.2.3 Restarting Oracle Identity Manager ................................................... C-3
C.3 Starting and Stopping Oracle Identity Federation Managed Servers .......... C-3
C.3.1 Starting Oracle Identity Federation .................................................... C-3
C.3.2 Stopping Oracle Identity Federation .................................................. C-3
C.3.3 Restarting Oracle Identity Federation ................................................. C-3
C.3.4 Starting and Stopping the EMAgent .................................................... C-3
C.3.5 Stopping the Oracle Identity Federation Instances and EMAgent ........... C-4
C.4 Starting, Stopping, and Restarting Oracle Access Manager Managed Servers C-4
C.4.1 Starting an Access Manager Managed Server When None is Running .... C-4
C.4.2 Starting an Access Manager Managed Server When Another is Running C-4
C.4.3 Stopping Oracle Access Manager Managed Servers ............................... C-4
C.4.4 Restarting Oracle Access Manager Managed Servers ........................... C-5
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>C.5</td>
<td>Starting, Stopping, and Restarting WebLogic Administration Server</td>
<td>C-5</td>
</tr>
<tr>
<td>C.5.1</td>
<td>Starting WebLogic Administration Server</td>
<td>C-5</td>
</tr>
<tr>
<td>C.5.2</td>
<td>Stopping WebLogic Administration Server</td>
<td>C-5</td>
</tr>
<tr>
<td>C.5.3</td>
<td>Restarting WebLogic Administration Server</td>
<td>C-6</td>
</tr>
<tr>
<td>C.6</td>
<td>Starting and Stopping Oracle Virtual Directory</td>
<td>C-6</td>
</tr>
<tr>
<td>C.6.1</td>
<td>Starting Oracle Virtual Directory</td>
<td>C-6</td>
</tr>
<tr>
<td>C.6.2</td>
<td>Stopping Oracle Virtual Directory</td>
<td>C-6</td>
</tr>
<tr>
<td>C.7</td>
<td>Starting and Stopping Oracle Internet Directory</td>
<td>C-6</td>
</tr>
<tr>
<td>C.7.1</td>
<td>Starting Oracle Internet Directory</td>
<td>C-6</td>
</tr>
<tr>
<td>C.7.2</td>
<td>Stopping Oracle Internet Directory</td>
<td>C-6</td>
</tr>
<tr>
<td>C.8</td>
<td>Starting and Stopping Node Manager</td>
<td>C-6</td>
</tr>
<tr>
<td>C.8.1</td>
<td>Starting Node Manager</td>
<td>C-7</td>
</tr>
<tr>
<td>C.8.2</td>
<td>Stopping Node Manager</td>
<td>C-7</td>
</tr>
<tr>
<td>C.8.3</td>
<td>Starting Node Manager for an Administration Server</td>
<td>C-7</td>
</tr>
</tbody>
</table>
Preface

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

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following documents:

- Oracle Fusion Applications Administrator’s Guide
- Oracle Fusion Applications Installation Guide
- Oracle Fusion Applications Patching Guide
- Oracle Fusion Applications Installing and Managing in an Oracle VM Environment
- Oracle Fusion Middleware WebLogic Scripting Tool Command Reference

Conventions

The following text conventions are used in this document:
<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td><strong>monospace</strong></td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
What's New in This Guide

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

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

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

■ You run pre-downtime checks as a separate step, before you start the upgrade. See Chapter 4, "Running Pre-Downtime Checks."

■ Upgrade Orchestrator provides support for the Oracle Identity Management upgrade when you are running Oracle Fusion Applications on an environment that meets the following requirements:
  - Is a Linux environment
  - Uses a SINGLE, 3-NODE, or 4-NODE Oracle Identity Management configuration
  - Is a Release 7 IDM provisioned environment

See Section 5.1.11.1, "Release 7 IDM Provisioned, SINGLE, 3-NODE, or 4-NODE, Linux Platform."

■ You perform the Oracle Identity Management upgrade on AIX and Solaris platforms that use a SINGLE, 3-NODE, or 4-NODE Oracle Identity Management configuration, by running a script. See Section 5.2.4, "Run idmUpgrade.pl to Upgrade Oracle Identity Management."

Other Significant Changes in this Document for 11g Release 8 (11.1.8)

For 11g Release 8 (11.1.8), no other significant changes have been made to this guide.
This chapter provides an introduction to the process of upgrading Oracle Fusion Applications to 11g Release 8 (11.1.8).

This chapter contains the following topics:

- Upgrade Process Overview
- Hosts, Directories, and Files Required by Upgrade Orchestrator
- Back Up Strategy
- Planning Your Downtime
- Directories Structure Overview
- Checklist for Performing the Upgrade

### 1.1 Upgrade Process Overview

Upgrading to Oracle Fusion Applications 11g Release 8 (11.1.8) requires that you run Oracle Fusion Applications Upgrade Orchestrator (Upgrade Orchestrator) on an Oracle Fusion Applications 11g Release 7 (11.1.7) environment. The following figure depicts the upgrade process flow.
For more information about the tools and utilities called by Upgrade Orchestrator, see Appendix A, "Additional Information About Upgrade Orchestrator".

1.2 Hosts, Directories, and Files Required by Upgrade Orchestrator

Familiarize yourself with the following information before proceeding with the upgrade:

- Host Types
- Directories and Files Required by Upgrade Orchestrator

1.2.1 Host Types

The Release 8 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.
Hosts, Directories, and Files Required by Upgrade Orchestrator

1.1.1 Hosts

- **IDM host**: A combination of hosts which hosts OID, OIM, OAM, IDM OHS, and IDM Database services.
- **OHS host**: The host where the Oracle HTTP Server (OHS) software is installed and configured.
- **DB host**: The host where the Oracle Fusion Applications database is installed and configured.
- **Mid tier 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. For more information, see “Scaling Out Oracle Fusion Applications” in the Oracle Fusion Applications Administrator’s Guide.

1.1.2 Directories and Files Required by Upgrade Orchestrator

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

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

- **REPOSITORY_LOCATION**: You create this directory in a shared location. For more information, see Section 2.3.5.1, "Download and Unzip the Release 8 Repository."

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

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

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

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

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

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

Note that backups are manual steps and can be automated outside of Upgrade Orchestrator based on your IT requirements and processes. For detailed information about required backups, see Section 5.2.1, "Back Up the OPSS Security Store" and Section 5.2.2, "Back Up Oracle Fusion Applications".

The following components must be backed up:

- Oracle Fusion Applications, including:
  - Oracle Fusion Applications database
  - APPLICATIONS_BASE
  - APPLICATIONS_CONFIG
  - Oracle Identity Management database
  - Upgrade Orchestration directories
  - OHS and /etc/hosts files
  - Central Inventory

- OPSS Security Store

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

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

For additional back up steps that are specific to Windows, refer to Section 5.2.3, "Back Up Oracle Fusion Applications on Windows".

Upgrade Orchestrator provides default pause points to perform these back up steps, depending on your upgrade path. For more information, see Section 5.1.8, "Pause Point 3 - Back Up Oracle Fusion Applications".

1.4 Planning Your Downtime

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

- Perform pre-downtime steps ahead of time. For more information, see Chapter 2, "Preparing to Perform the Release 8 Upgrade".
- Perform your database patching in a separate maintenance window. For more information, see Chapter 3, "Updating the Oracle Fusion Applications and Oracle Identity Management Databases".
- Perform steps to check system reliability in pre-downtime mode after all prerequisites are met. For more information, see Chapter 4, "Running Pre-Downtime Checks".
1.5 Directories Structure Overview

Upgrade Orchestrator references and uses the following directories:

- Directories Used by Upgrade Orchestrator
- Download Directories
- Relationship of Home Directories

1.5.1 Directories Used by Upgrade Orchestrator

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

![Figure 1–2 Directory Structure of Upgrade Orchestrator]

1.5.2 Download Directories

The following figure shows the directory structure that you create during the preparation of your environment for the upgrade. There are specific files that must be downloaded into each of these directories. For more information, see Section 2.3.2, "Create Directories in a Shared Location".
1.5.3 Relationship of Home 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`). The `/fusionapps` directory is an Oracle Fusion Applications Middleware home (`APPLICATIONS_BASE/fusionapps`).

For more information, see "Oracle Fusion Applications Shared Directory Structure" in the *Oracle Fusion Applications Installation Guide*.

1.6 Checklist for Performing the Upgrade

The following checklist provides the list of tasks to perform the upgrade to Release 8.

**Table 1–1 Checklist of Upgrade Tasks**

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Task Description</th>
<th>Reference Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before You Begin the Upgrade</td>
<td>Information about the resources you must have access to before you start the upgrade.</td>
<td>Section 2.1, &quot;Before You Begin&quot;</td>
</tr>
<tr>
<td>System Requirements</td>
<td>System requirements that must be met for the system to be upgraded.</td>
<td>Section 2.2, &quot;System Requirements&quot;</td>
</tr>
<tr>
<td>Create Directories and Stage the Software</td>
<td>Details about the directories you must create and the software and patches you must download and stage before you start the upgrade.</td>
<td>Section 2.3, &quot;Create Upgrade Directories and Obtain Software&quot;</td>
</tr>
<tr>
<td>Set Up Upgrade Orchestrator</td>
<td>Steps to set up the orchestrator software, to prepare the system for RUP Lite for OVM and to prepare the properties files.</td>
<td>Section 2.4, &quot;Set Up Upgrade Orchestrator&quot;</td>
</tr>
<tr>
<td>Update the properties file for automated IDM upgrade</td>
<td>Steps to update the <code>patchAutomation.properties</code> file if your IDM upgrade is automated.</td>
<td>Section 2.5, &quot;Update the <code>patchAutomation.properties</code> File for the IDM Upgrade&quot;</td>
</tr>
<tr>
<td>Verify Environment before proceeding with downtime</td>
<td>Steps to verify your environment before you start the upgrade.</td>
<td>Section 2.6, &quot;Verify Your Environment Before Proceeding to Downtime&quot;</td>
</tr>
</tbody>
</table>
### Checklist of Upgrade Tasks

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Task Description</th>
<th>Reference Link</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Update Oracle Fusion Applications and Oracle Identity Management Databases</strong></td>
<td>Steps to update your databases.</td>
<td>Chapter 3, &quot;Updating the Oracle Fusion Applications and Oracle Identity Management Databases&quot;</td>
</tr>
<tr>
<td><strong>Run steps to ensure system reliability</strong></td>
<td>Steps to run checks to ensure system reliability.</td>
<td>Chapter 4, &quot;Running Pre-Downtime Checks&quot;</td>
</tr>
<tr>
<td><strong>Run Upgrade Orchestrator during Downtime</strong></td>
<td>Steps to run Upgrade Orchestrator during downtime.</td>
<td>Section 5.1.1, &quot;Run Upgrade Orchestrator During Downtime&quot;</td>
</tr>
<tr>
<td><strong>Pause Point 1 - Back up OPSS Security Store</strong></td>
<td>Steps to back up the OPSS Security Store, followed by steps to update the status of the pause point task to proceed with the upgrade. This pause point is conditionally supported by orchestration.</td>
<td>Section 5.1.2, &quot;Pause Point 1 - Back Up the OPSS Security Store&quot;</td>
</tr>
<tr>
<td><strong>Pause Point 2 - Stop Informatica IR Servers</strong></td>
<td>Steps to stop Informatica IR servers, followed by steps to update the status of the pause point task to proceed with the upgrade.</td>
<td>Section 5.1.5, &quot;Pause Point 2 - Stop Informatica IR (IIR) Servers&quot;</td>
</tr>
<tr>
<td><strong>Pause Point 3 - Back Up Oracle Fusion Applications</strong></td>
<td>Steps to back up Oracle Fusion Applications, followed by steps to update the status of the pause point task to proceed with the upgrade.</td>
<td>Section 5.1.8, &quot;Pause Point 3 - Back Up Oracle Fusion Applications&quot;</td>
</tr>
<tr>
<td><strong>Pause Point 4 - Upgrade Oracle Identity Management</strong></td>
<td>Steps to upgrade Oracle Identity Management, followed by steps to update the status of the pause point task to proceed with the upgrade. This pause point is conditionally supported by orchestration.</td>
<td>Section 5.1.11, &quot;Pause Point 4 - Upgrade Oracle Identity Management to Release 8&quot;</td>
</tr>
<tr>
<td><strong>Pause point 5 - Start External Servers</strong></td>
<td>Steps to start external servers, followed by steps to update the status of the pause point task to proceed with the upgrade. This pause point is conditionally supported by orchestration.</td>
<td>Section 5.1.14, &quot;Pause Point 5 - Start External Servers&quot;</td>
</tr>
<tr>
<td><strong>Pause Point 7 - Back Up Oracle Fusion Applications (Language Pack Only)</strong></td>
<td>Steps to back up Oracle Fusion Applications before proceeding with the language pack upgrade, followed by steps to update the status of the pause point task to proceed with the upgrade.</td>
<td>Section 5.1.17, &quot;Pause Point 6 - Back Up Oracle Fusion Applications Before Language Pack Upgrade (Language Pack Only)&quot;</td>
</tr>
<tr>
<td><strong>Run Upgrade Orchestrator in the DowntimeDuringLP phase</strong></td>
<td>Steps to run orchestration to perform language pack upgrade tasks.</td>
<td>Section 5.1.19, &quot;Resume Upgrade Orchestrator (Language Pack Only)&quot;</td>
</tr>
<tr>
<td><strong>Run Post Upgrade Tasks</strong></td>
<td>Required post upgrade tasks that you must perform after Upgrade Orchestrator runs to successful completion.</td>
<td>Chapter 6, &quot;Running Post-Upgrade Tasks for Oracle Fusion Applications&quot;</td>
</tr>
<tr>
<td><strong>Troubleshoot the Upgrade</strong></td>
<td>Possible failure and error scenarios that may occur during the upgrade, including possible solutions or workarounds.</td>
<td>Chapter 7, &quot;Monitoring and Troubleshooting the Upgrade&quot;</td>
</tr>
</tbody>
</table>
Preparing to Perform the Release 8 Upgrade

This chapter describes the preparation steps for upgrading to Release 8, all of which can be performed before your scheduled downtime.

This chapter contains the following topics:

- Before You Begin
- System Requirements
- Create Upgrade Directories and Obtain Software
- Set Up Upgrade Orchestrator
- Update the patchAutomation.properties File for the IDM Upgrade
- Verify Your Environment Before Proceeding to Downtime
- What To Do Next

2.1 Before You Begin

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

1. Ensure you perform all Release 8 Pre-upgrade steps from Oracle Fusion Applications release notes.

2. If you have installed any languages in addition to US English, ensure you perform all Release 8 Pre-upgrade steps from the Oracle Fusion Applications NLS Release Notes.

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

2.2 System Requirements

Ensure that your environment meets the following system requirements:

- Memory Requirements
- Free Disk Space Requirements
- Set LBR_PRESENT to True on the Primordial Host
2.2.1 Memory Requirements

During the pre-downtime phase, Upgrade Orchestrator reports if your environment does not meet the following memory requirements. For Oracle VM memory requirements, see “Suggested Memory (in GB) and Number of vCPUs” in Oracle Fusion Applications Installing and Managing in an Oracle VM Environment.

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

<table>
<thead>
<tr>
<th>Memory Specifics</th>
<th>Upgrade From Release 7 to Release 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory per Managed Servers</td>
<td>2GB multiplied by the number of managed servers in your environment, plus 4GB</td>
</tr>
<tr>
<td>Memory Per Administration Servers</td>
<td>1GB multiplied by the number of administration servers in your environment</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Topology</th>
<th>FA</th>
<th>Primary</th>
<th>Secondary</th>
<th>BI</th>
<th>AppOHS</th>
<th>IDM3OID</th>
<th>IDM3MW</th>
<th>IDM3OHS</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HCM</td>
<td>14336</td>
<td>32768</td>
<td>62464</td>
<td>13312</td>
<td>2048 Free, 3072 Total</td>
<td>2048 Free, 4096 Total</td>
<td>3072 Free, 11264 Total</td>
<td>256 Free, 1536 Total</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CRM</td>
<td>19456</td>
<td>29696</td>
<td>60416</td>
<td>13312</td>
<td>2048 Free, 3072 Total</td>
<td>2048 Free, 4096 Total</td>
<td>3072 Free, 11264 Total</td>
<td>256 Free, 1536 Total</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FSCM-H</td>
<td>17920</td>
<td>31744</td>
<td>65536</td>
<td>13312</td>
<td>2048 Free, 3072 Total</td>
<td>2048 Free, 4096 Total</td>
<td>3072 Free, 12288 Total</td>
<td>256 Free, 1536 Total</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 2–3 Memory Requirements for Oracle VM Global Single Instance (GSI) Environments (MB)

<table>
<thead>
<tr>
<th>Topology</th>
<th>FA</th>
<th>Primary</th>
<th>Secondary</th>
<th>BI</th>
<th>AppOHS</th>
<th>IDM3OID</th>
<th>IDM3MW</th>
<th>IDM3OHS</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GSI</td>
<td>27593</td>
<td>61440</td>
<td>87040</td>
<td>13312</td>
<td>3072</td>
<td>4096</td>
<td>12288</td>
<td>1536</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

### Table 2–4 Memory Swap Requirements for All Oracle VM Topologies (MB)

<table>
<thead>
<tr>
<th>IDM3OID</th>
<th>IDM3MW</th>
<th>IDM3OHS</th>
<th>FA</th>
<th>Primary</th>
<th>Secondary</th>
<th>BI</th>
<th>AppOHS</th>
</tr>
</thead>
<tbody>
<tr>
<td>4000</td>
<td>4000</td>
<td>4000</td>
<td>4000</td>
<td>4000</td>
<td>4000</td>
<td>4000</td>
<td>4000</td>
</tr>
</tbody>
</table>

2.2.2 Free Disk Space Requirements

The disk space requirements in the following table are recommendations for how much disk space should be added on each host type. During the pre-downtime phase, Upgrade Orchestrator reports if your environment does not meet these requirements. The disk space check is not checking for total space. It is checking only for usable disk space, which is defined as free space, with respect to quotas and permissions. All recommendations and requirements assume non-shared access to the disk space. Therefore, if you have multiple hosts or processes running against the same physical
Create Upgrade Directories and Obtain Software

Preparing to Perform the Release 8 Upgrade

2.2.3 Set LBR_PRESENT to True on the Primordial Host

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

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

2.3 Create Upgrade Directories and Obtain Software

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

- Create a Common User Group and Permissions for Shared Directories
- Create Directories in a Shared Location
- Create Directories Common to One Environment
- Download and Unzip the Patch Conflict Manager Utility
- Download and Unzip the Repository and Patches
- Unzip Orchestration.zip
- Copy and Unzip idmUpgrade.zip

2.3.1 Create a Common User Group and Permissions for Shared Directories

The following steps outline the process for setting up permissions on directories that are shared across multiple hosts and are used by Oracle Fusion Applications Upgrade Orchestrator. These steps are required if you use different operating system (OS) users and groups to own Oracle Fusion Applications components (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. Note that the SHARED_LOCATION must be exported with the no_root_squash option, or its equivalent, to allow root user access to files in the SHARED_LOCATION that are owned by the applications user. For more information about the SHARED_LOCATION, see Section 2.3.2, “Create Directories in a Shared Location”.

Table 2–5  Free Disk Space Requirements

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Upgrade From Release 7 to Release 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primordial</td>
<td>100GB + 4GB for /tmp</td>
</tr>
<tr>
<td>DB</td>
<td>36GB + 4GB for /tmp + 4GB for flash recovery area (if configured)</td>
</tr>
<tr>
<td>OHS</td>
<td>8GB + 4GB for /tmp</td>
</tr>
<tr>
<td>Mid tier</td>
<td>5GB + 4GB for /tmp</td>
</tr>
</tbody>
</table>
1. Determine the OS group and Group ID that you want to use for owning the shared directories. As an example, you can use `orch` as the common group to be used across the hosts.

2. The following steps must be executed as a privileged OS user, such as `root`, on all hosts that participate in orchestration.
   a. Create the common group, if needed.
      
      (Linux) `/usr/sbin/groupadd -g group_ID -f group_name`
      
      (Solaris) `/usr/sbin/groupadd -g group_ID group_name`
      
      (AIX) `/usr/bin/mkgroup id=group_ID group_name`
   
   b. Add each distinct Oracle Fusion Applications component (FA, FMW, DB, IDM) OS owner on each host to the common group.
      
      (Linux) `/usr/sbin/usermod -a -G group_name component_OS_owner`
      
      (Solaris) `EXISTING_GROUPS=$(grep -w component_OS_owner /etc/group | awk '{print $1}' | xargs echo | sed 's/ /,/g')`
      
      `/usr/sbin/usermod -G ${EXISTING_GROUPS},group_name component_OS_owner`
      
      (AIX) `lsgroup -a users group_name`
      
      `/usr/bin/chgroup users=list_of_existing_users,component_OS_owner group_name`
      
      You must log out of any sessions that were open prior to this change for OS users being modified, and then log in again so the changes take effect.
   
   c. Mount the file system to be used for the shared directories on all hosts.
   
   d. Perform the following steps on one of the hosts, such as the primordial host.
      
      - Create a top-level directory that is passed to orchestration under which additional directories and files are created during orchestration. This directory is referred to as `SHARED_LOCATION` and is further described in Section 2.3.2, "Create Directories in a Shared Location".
      
      - Perform the following steps before any additional content is created in the shared directories. These steps are applicable to Linux and UNIX platforms, such as AIX, Solaris Sparc and Solaris X64.
         
         - Change the group ownership of the top-level directory to the common group, such as `orch`.
           
           (Linux and UNIX) `chgrp common_group SHARED_LOCATION`
         
         - Set permissions on the directory so that the group has read, write, and access privileges.
           
           (Linux and UNIX) `chmod g+r,g+w,g+x SHARED_LOCATION`
         
         - Set the Directory group ID bit for the top-level shared directory. This allows for any subdirectories and files created under this shared directory to be owned by the same group, regardless of the host from where they are created.
           
           (Linux and UNIX) `chmod g+s SHARED_LOCATION`
      
3. Perform the following steps on all hosts that participate in orchestration. You must be logged in as the OS user that owns the Oracle Fusion Applications content on the host when you run these steps.
a. Set the default mask for files so that the group has sufficient privileges on the files.

   umask 0007

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

   (Linux and UNIX) `groups`

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

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

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

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

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

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

   (AIX) `istat file_name | grep Group`

   Then remove the temporary file.

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

   `jar -xvf ZIP_archive`

   `unzip -q -o ZIP_archive`

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

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

   b. Run `chmod -R 755 *`.

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

2.3.1.1 Create Shared Folders and Permissions on Windows

Perform the following steps for Windows on one of the hosts, for example, Host1.
1. Create a top-level folder, such as C:\Shared on Host1, that will be passed to orchestration, and under which additional folders and files are created during orchestration.

2. Perform the following steps before any additional content is created in the top-level folder. Repeat these steps to share the top-level folder to one or more Windows Domain users who will be accessing this top-level folder from the hosts in the Oracle Fusion Applications environment (Primordial, OHS, RDBMS, and IDM).
   a. In Windows Explorer, right click on the top-level folder and select Properties from the context menu.
   b. In the Properties window, click the Sharing tab, then click Share.
   c. In the File Sharing window, enter the domain user name using the format DomainName\username.
   d. Click Add. This adds the given domain user name to the list of users with whom the folder is shared.
   e. Select the domain user name that was added and change the permission level to Read/Write.
   f. Click Share and then click Done to save and close the File Sharing window.
   g. Click Close to close the Properties window.

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

3. Perform the following steps on all hosts that participate in orchestration.
   a. Log in to the host using the DomainName\username you used in Step c.
   b. Create a symlink, such as C:\Shared, using following command:

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

### 2.3.2 Create Directories in a Shared Location

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

---

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

---

The directory names in this section are suggested names and are referenced throughout the upgrade steps. You can choose to use your own naming conventions. See Figure 1–3, "Directory Structure of Downloaded Patches and Repositories" for more information.
Note: Avoid creating any repository in a deeply nested directory on Windows. The Windows PATH variable has a limited size, and long directory names may cause it to overflow. For example, c:\work\my_repository is a better choice than c:\Work\WorkInProgress\FusionApps\FusionAppsv1\Nov2012\tempfiles\my_repository.

### 2.3.2.1 Create Release 8 Repository Directories

Create the following directories for Release 8 repositories:

- \SHAREDD_LOCATION/11.1.8.0.0/Repository
- \SHAREDD_LOCATION/11.1.8.0.0_post_repo_patches
- \SHAREDD_LOCATION/11.1.8.0.0/idmUpgrade
- \SHAREDD_LOCATION/11.1.8.0.0/LP (required only if you have installed languages other than US English)

### 2.3.2.2 HCM Workforce Reputation Directory

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

Confirm that the following directory exists for HCM Workforce Reputation Management. Also confirm the permissions on this directory. The directory should be accessible from the host where HWR app is provisioned. In an Oracle VM environment, WorkforceReputationServer_1 is allocated to the secondary node in the OVM template for Release 8, therefore this directory needs to exist only on the secondary node. If the directory does not exist, perform the following steps:

- (Unix) `mkdir /mnt/hwrrepo`
- (Windows) `mkdir \mnt\hwrrepo`
- Use the following command to grant directory permission to the user and group who own the Oracle Fusion Applications WLS domains.

  `chown user_id:group_name /mnt/hwrrepo`
- Use the following command to set the correct read and write permission to the directory.

  `chmod 750 /mnt/hwrrepo`

### 2.3.3 Create Directories Common to One Environment

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

#### 2.3.3.1 Create Orchestration Checkpoint Locations

Create the following directories for storing checkpoint information:

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

- \texttt{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 you select a shared mount point that has high disk I/O performance, especially for writing. Orchestration framework automatically archives the checkpoint file stored under the \texttt{POD\_NAME} directory in the directory specified by the \texttt{ORCHESTRATION\_CHECKPOINT\_LOCATION} property. This location is stored in the \texttt{ORCHESTRATION\_CHECKPOINT\_ARCHIVE\_LOCATION} property in the \texttt{pod.properties} file. It is a best practice not to use \texttt{ORCH\_LOCATION}/\texttt{config} as a value for this property.

2.3.3.2 Create the Shared Upgrade Location

Create a directory referred to as \texttt{SHARED\_UPGRADE\_LOCATION}. This is a temporary directory required by the upgrade to copy files and perform write operations. Ensure that you select a shared mount point that is shared across all hosts for a given environment that has high disk I/O performance, especially for writing. This area can be cleaned up after all of your environments have been successfully upgraded to Release 8.

Also create the following directory:

\texttt{SHARED\_UPGRADE\_LOCATION/healthchecker/common}

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

2.3.4 Download and Unzip the Patch Conflict Manager Utility

Download and unzip the latest version of patch 18164004 from My Oracle Support into the \texttt{SHARED\_LOCATION} directory, which creates the \texttt{PatchConflictManager} directory. Ensure that you unzip this patch as the same user that runs the upgrade.

2.3.5 Download and Unzip the Repository and Patches

Download the following repositories and patches for upgrading to Release 8:

- Download and Unzip the Release 8 Repository
- Download and Unzip Release 8 Language Packs
- Download and Unzip Mandatory Post-Release 8 Patches

2.3.5.1 Download and Unzip the Release 8 Repository

The Release 8 repository contains all patches that are required to upgrade to Release 8 in an existing Oracle Fusion Applications environment. Perform the following steps to download the repository from the Oracle Fusion Applications Product Media Package:

2. Complete the Export Validation process by entering basic identification information using the online form.
3. On the Media Pack Search page, select Oracle Fusion Applications as the product pack and then select your platform to identify the media pack you want to download.

4. Choose the appropriate media pack from the search results, such as Release 8 (11.1.8) for your platform, and download the Release repository (in zipped format) to $SHARED_LOCATION/11.1.8.0.0/Repository$.

5. Extract the contents of all zipped files to the same target directory, $SHARED_LOCATION/11.1.8.0.0/Repository$. This directory is referred to as $REPOSITORY_LOCATION$ in this guide.

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

2.3.5.2 Download and Unzip Release 8 Language Packs

For each language installed in your environment, download the Release 8 language pack from http://edelivery.oracle.com to the $SHARED_LOCATION/11.1.8.0.0/LP$ directory. The location of where you download the language packs is recorded in the REL8_LP_REPOSITORY_LOCATION property in the Primordial host properties file, as described in Table B–2, "PRIMORDIAL.properties".

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

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

2.3.5.3 Download and Unzip Mandatory Post-Release 8 Patches

**Note:** If there are no post-release patches in Release 8 Oracle Fusion Applications release notes when you upgrade, there is no action required for this step and you can proceed to Section 2.3.6, "Download the Invalid Objects Patch for Exclusion List."

Upgrade Orchestrator can apply mandatory post-release patches that are required by Oracle Fusion Applications if you download the patches from My Oracle Support before you start the upgrade. Note that this feature relates only to patches that are documented in Oracle Fusion Applications release notes and that are specifically required for 11g Release 8 (11.1.8).

Perform the following steps to download patches for Release 8:

1. Unzip $SHARED_LOCATION/11.1.8.0.0/Repository/installers/pre_install/PostRepoPatchDirs.zip$, which is part of the repository you downloaded in Section 2.3.5.1, "Download and Unzip the Release 8 Repository", in the 11.1.8.0.0_post_repo_patches directory to create the directory structure for the patches you download.

2. Review the README file that was created when you unzipped PostRepoPatchDirs.zip, to learn how the subdirectories under the 11.1.8.0.0_post_repo_patches directory map to the corresponding components, such as Oracle Fusion Middleware, database client, and database server components.

3. Refer to the section titled "Upgrade Known Issues, Pre-Upgrade Known Issues, Mandatory Patches to be Downloaded" in Oracle Fusion Applications release notes for Release 8 to find any additional patches to be downloaded from My Oracle Support. Note that if you stage a patch which contains translated content
and is translatable, you will also need to stage the corresponding translated patches for the active languages.

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

<table>
<thead>
<tr>
<th>Type of Patches</th>
<th>Location in Oracle Fusion Applications Release Notes, under Upgrade Known Issues, Pre-Upgrade Known Issues, Mandatory Patches to be Downloaded</th>
<th>Orchestrator Step or Utility That Applies the Patches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Database</td>
<td>Oracle Database</td>
<td>RUP Lite for RDBMS</td>
</tr>
<tr>
<td>Oracle Fusion Middleware</td>
<td>Oracle Fusion Middleware</td>
<td>Apply Pre-PSA Middleware Patches and Apply Post-PSA Middleware Patches</td>
</tr>
<tr>
<td>Oracle HTTP Server (OHS)</td>
<td>Oracle HTTP Server (OHS)</td>
<td>Upgrade Oracle Fusion Applications Web Tier (RUP Lite for OHS)</td>
</tr>
<tr>
<td>Oracle Fusion Applications</td>
<td>Oracle Fusion Applications</td>
<td>Apply Downloaded Patches</td>
</tr>
<tr>
<td>Oracle Fusion Applications Release 8</td>
<td>Installer</td>
<td>Oracle Fusion Applications Upgrade Installer</td>
</tr>
<tr>
<td>Oracle Fusion Applications LCM Tools</td>
<td>Oracle Fusion Applications Patch Manager</td>
<td>Update LCM Tools</td>
</tr>
<tr>
<td>Oracle Fusion Applications LCM Tools for Oracle VM</td>
<td>Oracle Fusion Applications Patch Manager</td>
<td>Install Oracle Fusion Applications LCM Tools for Oracle VM</td>
</tr>
</tbody>
</table>

4. Download and unzip the patches listed in the Oracle Fusion Applications release notes, into the appropriate subdirectory under the 11.1.8.0.0_post_repo_patches directory, based on the mapping information in the README file described in Step 2. Downloading a patch to the incorrect directory could result in failure.

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

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

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

The adGenerateFAPatchPlan.pl script is typically located in $SHARED_LOCATION/11.1.8.0.0/Repository/installers/farup/Disk1/upgrade/bin. If the latest LCM patch bundle is included in the downloaded LCM Tools patches, then adGenerateFAPatchPlan.pl is located in download_location_for_lcm_patches_only/patch_bundle_patch_number/files/lcm/ad/bin.
To run this script, use the Perl executable from APPLICATIONS_BASE/dbclient/perl/bin for UNIX platforms and APPLICATIONS_BASE/dbclient/perl/5.8.3/bin/MSWin32-x64-multi-thread for Windows.

Use the following command syntax to create the patch plan file:

(UNIX)
setenv PATH /u01/APPLTOP/dbclient/perl/bin:$PATH
setenv PERL5LIB APPLICATIONS_BASE/dbclient/perl/lib/5.8.3:
APPLICATIONS_BASE/dbclient/perl/lib/site_perl/5.8.3:
APPLICATIONS_BASE/dbclient/perl/lib/site_perl
$APPLICATIONS_BASE/dbclient/perl/bin/perl
SHARED_LOCATION/11.1.8.0.0/Repository/installers/farup/Disk1/upgrade/bin/adGeneratePatchPlan.pl SHARED_LOCATION/11.1.8.0.0_post_repo_patches

(Windows)
set PATH /u01/APPLTOP/dbclient/perl/bin;PATH
SET PERL5LIB=APPLICATIONS_BASE\dbclient\perl\5.8.3;APPLICATIONS_BASE\dbclient\perl\site\5.8.3;APPLICATIONS_BASE\dbclient\perl\site
%APPLICATIONS_BASE%\dbclient\perl\5.8.3\bin\MSWin32-x64-multi-thread\perl
%SHARED_LOCATION%\11.1.8.0.0\Repository\installers\farup\Disk1\upgrade\bin\adGeneratePatchPlan.pl SHARED_LOCATION/11.1.8.0.0_post_repo_patches

An excerpt from a sample patch plan follows:

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

2.3.6 Download the Invalid Objects Patch for Exclusion List

Sets of validations are performed at various stages of the upgrade. One such validation is the check for database objects in an invalid state. In certain scenarios, a set of objects gets into an invalid state during intermediate stages of an upgrade and can be safely ignored. The list of objects to be ignored is delivered as a file through a downloadable patch.
Download patch 17051994 for Release 11.1.8.0.0 from My Oracle Support and copy all files named as FA*overrides.xml, from the patch to the shared upgrade location/healthchecker/common directory. You may need to create this directory if it does not already exist.

2.3.7 Unzip Orchestration.zip

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

1. The latest version of the Orchestration.zip file is uploaded to patch 17375678 on My Oracle Support after Release 8 is released. To ensure you have the latest version of Orchestration.zip, download patch 17375678 from My Oracle Support. The patch contains Orchestration.zip, readme.txt, and validateOrchVersion.py scripts. Extract the patch contents to a temporary location.

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

   If you do not find patch 17375678, no new version of Orchestration.zip was released yet, so use the Orchestration.zip file that is delivered in the Release 8 Repository, located at shared location/11.1.8.0.0/Repository/installers/farup/Disk1/upgrade/orchestration.

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

   When you unzip Orchestration.zip, a directory named orchestration is created. This directory is referred to as ORCH_LOCATION. For more information, see Section 1.5.1, "Directories Used by Upgrade Orchestrator".

3. If you did not download the patch in Step 1, proceed to Step 4. If you downloaded the latest Orchestration.zip file from the patch in Step 1, run validateOrchVersion.py 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. Orchestration.zip contains the Health Checker framework. After unzipping Orchestration.zip, ensure you have the latest version of Health Checker by downloading patch 17375744 from My Oracle Support. If this patch is not available, use the Health Checker packaged with Orchestration.zip.
5. If available, unzip patch 17375744. Then copy the contents of the 17375744/files/lcm/hc directory to the ORCH_LOCATION/fusionapps/applications/lcm/hc directory. Overwrite the contents in this directory. If this patch is not available, there are no newer versions of Health Checker and you can proceed to Section 2.3.8, "Copy and Unzip idmUpgrade.zip."

2.3.8 Copy and Unzip idmUpgrade.zip

If you are running Oracle Fusion Applications on a SINGLE, 3-NODE, or 4-NODE IDM configuration on a Linux, Solaris, or AIX platform that is a Release 7 IDM provisioned environment, follow the steps in this section to stage the latest idmUpgrade.zip file.

1. The latest version of the idmUpgrade.zip file is available in patch 17444252. Ensure that you always uptake the latest version of idmUpgrade.zip from the patch.

   **Note:** To use a new version of the idmUpgrade.zip file downloaded from the patch, after you have 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, to any temporary location, referred to as temporary_unzip_location.

3. Copy the contents of temporary_unzip_location/rel8/idmUpgrade to SHARED_LOCATION/11.1.8.0.0/idmUpgrade.

2.4 Set Up Upgrade Orchestrator

Perform the following steps to set up Upgrade Orchestrator:

- Set Up Upgrade Orchestrator on a Shared Location
- Select a Master Orchestration Password
- Prepare RUP Lite for OVM
- Update Orchestrator Properties Files
- Update PCM_config.properties

2.4.1 Set Up Upgrade Orchestrator on a Shared Location

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

1. Perform this step only if you are on Windows.
   
   Install python from http://www.python.org/ftp/python/2.7.3/python-2.7.3.msi

2. Run the orchestsetup script on the primordial host:

   (UNIX)
   
   cd ORCH_LOCATION/bin
   ./orchsetup.py -r SHARED_LOCATION/11.1.8.0.0/Repository --appbase APPLICATIONS_
BASE

(Windows)
cd ORCH_LOCATION\bin
orchsetup.py -r SHARED_LOCATION\11.1.8.0.0\Repository --appbase APPLICATIONS_BASE

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

This location can be configured to be shared across multiple environments that are being upgraded. In this case, this location is referred to as POD_NAME. For example, you could use this location for your test, production, and development environments, if you are upgrading all three environments to Release 8.

cd ORCH_LOCATION/config
mkdir POD_NAME

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

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

2.4.2 Select a Master Orchestration Password

Select a password at this time, which is referred to as the "Master Orchestration Password" in this documentation. Note that this password is referenced by Upgrade Orchestration but it is not used during the upgrade to Release 8, so it does not have to be a secure password. This password can be anything, such as "welcome123", for example.

2.4.3 Prepare RUP Lite for OVM

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

To determine if the Oracle VM environment was created from official releases of Oracle VM templates for Oracle Fusion applications Release 2 and higher, you can verify if the /assemblybuilder directory is present in the Oracle VM environment. This confirms that the environment is an OVAB. To confirm the release version, you must review the .labelinfo.txt and .misclabels.txt files in the u01/APPLTOP/ovabext directory to check the rehydration labels that correlate to the release version. Also check if there is a /u01/ovmext directory to determine if it is an Oracle VM IDM instance.
Perform the following steps to install the Oracle Fusion Applications 11.1.8.0.0 Lifecycle Management Tools for Oracle VM Installer repository on the Oracle VM hosts. This repository includes RUP Lite for OVM.

1. The latest version of the fasaaslcmtools.zip file, after Release 8 is released, will be uploaded to patch 17976770 on My Oracle Support. To ensure that you have the latest version of fasaaslcmtools.zip, download patch 17976770 from My Oracle Support. The patch contains fasaaslcmtools.zip, readme.txt, validate.py, and validate.label. Extract the contents of the patch to a temporary location.

2. If you do not find patch 17976770, no new version of fasaaslcmtools.zip was released yet, and you can obtain fasaaslcmtools.zip from the Release 8 OVAR_HOME. OVAR_HOME is the top-level directory for the Oracle Virtual Assembly Builder that contains all software needed to deploy Oracle Fusion Applications as an Oracle VM instance.

3. Unzip fasaaslcmtools.zip to a temporary location and ensure that you specify this temporary_location/fasaaslcmtools location in the REL8_SAAS_LCM_INSTALLER_DIR property in the pod.properties file. For more information, see Section 2.4.4, "Update Orchestrator Properties Files".

4. Copy the entire contents of the REL8_SAAS_LCM_INSTALLER_DIR/Disk1/preupg/rupliteovm directory to SHARED_LOCATION/ORCHLOCATION/config/POD_NAME/11.1.8.0.0/rupliteovm.

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

   validate.py fasaaslcmtools_SHIPHOME_LOCATION

   The value for SHIPHOME_LOCATION is the value for the REL8_SAAS_LCM_INSTALLER_DIR property from Step 3. If the script finishes with errors, confirm that the command and the argument passed to it are correct. If both values are correct, contact Oracle support for further assistance.

6. Update the env.properties file under the SHARED_LOCATION/ORCHLOCATION/config/POD_NAME/11.1.8.0.0/rupliteovm/metadata directory with the required property values for the following plug-ins:

   - **ApplyMemorySettings** (runs in offline mode)
     
     ovm.plugin.ApplyMemorySettings.enabled=true

   - **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

   - **UpdateODIUnicastConfiguration** (runs in offline mode)
     
     ovm.plugin.UpdateODIUnicastConfiguration.enabled=true

   - **FixReferenceProperties** (runs in offline mode)
     
     ovm.plugin.FixReferenceProperties.enabled=true

   - **UpdateFusionIIRScripts** (runs in offline mode)
Update the `patchAutomation.properties` File for the IDM Upgrade

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

Refer to Section A.3.3, "RUP Lite for OVM Utility" to see the overall flow of running RUP Lite for OVM during the upgrade.

### 2.4.4 Update Orchestrator Properties Files

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

**Note:** The following `HOSTNAME` properties must contain a host name: `HOSTNAME_PRIMORDIAL`, `HOSTNAME_MIDTIER`, `HOSTNAME_PRIMARY`, `HOSTNAME_SECONDARY`, `HOSTNAME_BIINSTANCE`, `HOSTNAME_OSN`, `HOSTNAME_OHS`, `HOSTNAME_IDMOID`, `HOSTNAME_IDMOIM`, and `HOSTNAME_IDMOHS`. Note that on Windows, the host name is case sensitive and can be obtained from the Control Panel, under System, then Full computer name.

### 2.4.5 Update `PCM_config.properties`

Edit the `SHARED_LOCATION/PatchConflictManager/PCM_Config.properties` file and set the `IS_SAAS_ENV` property to false.

### 2.5 Update the `patchAutomation.properties` File for the IDM Upgrade

Perform the steps in this section only if you are running Oracle Fusion Applications on a SINGLE, 3-NODE, or 4-NODE IDM configuration on a Linux, Solaris, or AIX platform that is a Release 7 IDM provisioned environment. If your environment does not meet these requirements, this section is not applicable, and the IDM upgrade is manual, for which the `IDM_SETUP_TYPE` property in the `IDM.properties` file must be set to `MANUAL`.

Set the following properties in the `SHARED_LOCATION/11.1.8.0.0/idmUpgrade/patchAutomation.properties` file:

- **IDM_DB_SYS_PWD**: Password for the `sys` user on the OIM database.
- **DB_ADMIN_PASSWORD**: Password for the `sys` user on the OID database.
- **OID_PASSWORD**: Admin password for the OID domain (for `cn=orcladmin`).
- **OIM_USER_PWD**: Admin password for the OIM domain admin password (for `xelsaysdm`).
- **OAM_ADMIN_PWD**: Admin password for the OAM domain (for `oamadminuser`).
- **OID_ADMIN_PWD**: Admin password for the OID domain (for `oimadminuser`).
- **IDSTORE_READ_ONLY_PWD**: Password for the identity store read only user.
- **IDSTORE_READ_WRITE_PWD**: Password for the identity store read/write user.
■ **ACCESS_CLIENT_PASSPHRASE_PWD**: Password for the access client pass phrase. You can leave this field empty if you are running on AIX, because OAM is configured on OPEN mode.

■ **OVD_PASSWORD**: Admin password for OVD (for cn=orcladmin).

■ **PATCHCONFLICT_TOOL_INSTALLER_LOC**: Location of the extracted Patch Conflict Manager utility. For more information, see Section 2.3.4, “Download and Unzip the Patch Conflict Manager Utility.”

■ **LOG_DIR**: Location of the log directory for the IDM upgrade. The default is /u01/logs.

■ **TOPOLOGY_XML_FILE_LOC**: Location of topology.xml. You can use the default if you chose /u01/IDMTOP/config while provisioning.

■ **IDM_LCM_LIB_PATH**: Location of IDM lcm libraries. You can use the default if you installed IDM in /u01.

■ **IDMLCM_HOME**: Location of IDMLCM home. You can use the default if you chose /u01/idmlcm/ while provisioning.

■ **START_STOP_SCRIPT_WORKING_DIR**: Location of the start/stop script. You can use the default if you chose /u01/IDMTOP/config while provisioning.

■ **OID_DOMAIN_DIR**: Location of the OID domain. You can use the default if you chose /u01/IDMTOP/config/domains/IDMDomain while provisioning.

■ **OIM_DOMAIN_DIR**: Location of the OIM domain. You can use the default if you chose /u01/IDMTOP/config/domains/IDMDomain while provisioning.

■ **OHS_HOME**: Location of OHS home. You can use the default if you chose /u01/IDMTOP/products/ohs/ohs while provisioning.

■ **IDMCONTROL_SCRIPT_LOC**: Location of the IDM control start/stop script.

■ **WALLET_DIR**: Location of the directory relative to the patchAutomation.properties file. The default value is ./patchAutomation. On the first run of prevalidate.pl or idmUpgrade.pl, the WALLET_DIR/cwallet.sso file is created if it does not exist, and any passwords that you have specified in patchAutomation.properties are moved out of the properties file and into this wallet file. This wallet file will contain sensitive passwords, so you may want to edit this property if you want to store the wallet in a separate location.

■ **OIM_ADMIN_USER**: Admin user for the OIM domain, required only for a SINGLE NODE environment.

■ **OIM_ADMIN_PWD**: Admin password for the OIM domain, required only for a SINGLE NODE environment.

■ **NODE_MANAGER_PWD**: Password for the node manager user, required only for a SINGLE NODE environment.

■ **IDSTORE_OIMADMINPWD**: Admin password for the OIM identity store OIM, required only for a SINGLE NODE environment.

### 2.6 Verify Your Environment Before Proceeding to Downtime

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

■ **Confirm Database Settings**

■ **Confirm JDeveloper Customizations Can Be Merged**
Verify Your Environment Before Proceeding to Downtime

- Maintain Versions of Customized BI Publisher Reports
- Remove Distributed Order Orchestration Customizations
- Verify the FUSION User Quota on FUSION_TS* Tablespaces
- Validate Domain Directories
- Verify the Node Manager Configuration is Correct
- Verify the Default Realm Name is myrealm
- Verify That etc/hosts Entries Are Correct
- Verify the Version of /bin/bash on All Hosts (Unix Platforms)
- Confirm nfslock is Up and Running on IDM Nodes
- Confirm Oracle Enterprise Manager Agents are Shut Down
- Register Oracle Homes in Central Inventory (Windows Only)
- Install the MKS Toolkit (Windows Only)

2.6.1 Confirm Database Settings
Refer to Release Notes for Oracle Fusion Applications 11g Release 8 (11.1.8) to verify that your database and Sql*Net tuning parameters are set properly to avoid time out errors during the upgrade.

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

You will merge your customizations after the SOA Preverification configuration assistant fails during the upgrade. For more information, see Section 7.16.6, "Merging SOA Composite JDeveloper Customizations During SOA Preverification".

2.6.3 Maintain Versions of Customized BI Publisher Reports
Ensure that you have your own versions of any customized BI Publisher reports. If an upgrade includes an update to a catalog object that was delivered with an Oracle Fusion application, the patch will overwrite any customizations applied to the original report.

Related Link
The following document provides additional information related to subjects discussed in this section:

- For more information, see "Reports Customization" in the "Customizing Reports and Analytics" chapter of the Oracle Fusion Applications Extensibility Guide.

2.6.4 Remove Distributed Order Orchestration Customizations
If you are using Extended Flexfields and you have customized the DOO SOA composites for mapping between EBO and DOO SDO, you can remove these...
customizations before you upgrade to Release 8 and use the new automap feature. For more information see "Preserving SOA Composite JDeveloper Customizations Before Applying a Patch" in the Oracle Fusion Applications Patching Guide. For more information about the automap feature in Release 8 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.

2.6.5 Verify the FUSION User Quota on FUSION_TS* Tablespaces

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

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

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

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

2.6.6 Validate Domain Directories

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

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

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

1. Unzip `domainvalidate.zip` from the `SHARED_LOCATION/11.1.8.0.0/Repository/installers/farup/Disk1/upgrade/validate` directory into any directory on the primordial host.
   
a. If `FA_MW_HOME` is `APPLICATIONS_BASE/fusionapps`, run the following command.
      (UNIX)
      
      ```bash
      ./validatedomains.sh APPLICATIONS_BASE
      ```
      
      (Windows)
      
      ```bash
      set JAVA_HOME=c:\AT\fusionapps\jdk6
      set PATH=\%PATH%;\JAVA_HOME\bin
      validatedomains.bat APPLICATIONS_BASE
      ```
      
      Example:
      
      `validatedomains.sh /u01/APPLTOP`
   
b. If `APPLICATIONS_CONFIG` is `APPLICATIONS_BASE/instance`, run the following command.
      (UNIX) `./validatedomains.sh FA_MW_HOME APPLICATIONS_CONFIG`
Verify Your Environment Before Proceeding to Downtime

2-20 Upgrade Guide

(Windows)
set JAVA_HOME=c:\AT\fusionapps\jdk6
set PATH=%PATH%;%JAVA_HOME%\bin
validatordomains.bat FA_MW_HOME APPLICATIONS_CONFIG

Example:
validatordomains.sh /u01/APPLTOP/fusionapps /u01/APPLTOP/instance

2. If validatordomains.sh reports any domains that failed the validation, and if you have scaled out hosts, then perform the following steps on the Administration Server of each of the reported domains.

   If validatordomains.sh reports any domains that failed the validation, and if you do not have scaled out hosts, then skip to Step 3.

   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 validatordomains.sh reports any domains that failed the validation, and if you do not have scaled out hosts, then perform the following steps:

   a. Download the patch 18062458 to a local directory.
   b. Run the extracted script against each domain directory under APPLICATIONS_CONFIG.

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

      For Windows:
      FA_MW_HOME\oracle_common\common\bin\wlst.cmd fixadminconfig.wlst APPLICATIONS_CONFIG/domains/<HOST>/<DOMAIN NAME>

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

2.6.7 Verify the Node Manager Configuration is Correct

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

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

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

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

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

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

   b. Open the domain in offline mode:

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

   c. Run the following commands for each impacted machine:

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

   d. Save the domain and exit WLST:

   ```bash
   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.

### 2.6.8 Verify the Default Realm Name is myrealm

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

1. Log in to the WLS Console for the Common Domain.
2. Click Security Realms on the domain structure pane.
3. A list of realms displays in the Summary of Security Realms window.
4. Verify there is an entry for myrealm and that "true" displays in the Default Realm column.

### 2.6.9 Verify That etc/hosts Entries Are Correct

Review /etc/hosts on all hosts to confirm that the entries are correct, including the following requirements.

1. For example, ensure that the oam-admin.oracleoutsourcing.com entry is in /etc/hosts for APPOHS.
2. Ensure that there are no duplicate IPs in /etc/hosts. Duplicate entries registered in DNS may cause failures during the Starting All Servers tasks.
2.6.10 Verify the 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.

2.6.11 Confirm nfslock is Up and Running on IDM Nodes

The IDM upgrade uses flock to obtain shared locks and update the patchAutomation.properties file. Ensure that the nfslock daemon is up and running before beginning the upgrade. If the daemon is down, restart it as the root user, as shown in the following example.

```
# service nfslock restart
```

2.6.12 Confirm Oracle Enterprise Manager Agents are Shut Down

Ensure that all Oracle Enterprise Manager agents are shut down to prevent the creation of /tmp/*pki* files during the upgrade. You can skip this step if you are not using Oracle Enterprise Manager.

2.6.13 Register Oracle Homes in Central Inventory (Windows Only)

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

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

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

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

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

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

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

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

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

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

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

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

   (Windows) WEBTIER_WEBGATE_HOME\\oui\bin\attachHome.bat -jreLoc JAVA_HOME_LOCATION
7. Run `attachHome` from the Oracle Common Oracle home, for example, `APPLICATIONS_BASE\fusionapps\oracle_common`.

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

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

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

   `HOME_DEPENDENCY_LIST=(ORACLE_HOME:DEPENDENT_ORACLE_HOME)`

   Example for Business Intelligence:

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

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

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

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

    Example entries in `inventory.xml`:

    ```xml
    <HOME NAME="OH1109401105" LOC="APPLICATIONS_BASE/fusionapps/gop" TYPE="O" IDX="11">
    <DEPHOMELIST>
    <DEPHOME LOC="APPLICATIONS_BASE/fusionapps/oracle_common"/>
    </DEPHOMELIST>
    </HOME>
    <HOME NAME="OH198367808" LOC="APPLICATIONS_BASE/fusionapps/bi" TYPE="O" IDX="12">
    <DEPHOMELIST>
    <DEPHOME LOC="APPLICATIONS_BASE/fusionapps/oracle_common"/>
    </DEPHOMELIST>
    </HOME>
    <HOME NAME="OH987588708" LOC="APPLICATIONS_BASE/webtier_mwhome/webtier" TYPE="O" IDX="13">
    <DEPHOMELIST>
    <DEPHOME LOC="APPLICATIONS_BASE/webtier_mwhome/oracle_common"/>
    </DEPHOMELIST>
    </HOME>
    <HOME NAME="OH1271096710" LOC="APPLICATIONS_BASE/webtier_mwhome/oracle_common" TYPE="O" IDX="14">
    <REFHOMELIST>
    <REFHOME LOC="APPLICATIONS_BASE/webtier_mwhome/webtier"/>
    </REFHOMELIST>
    </HOME>
    ```

Preparing to Perform the Release 8 Upgrade 2-23
What To Do Next

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

2.6.14 Install the MKS Toolkit (Windows Only)

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


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

2.7 What To Do Next

To proceed with the upgrade, follow the steps in Chapter 3, "Updating the Oracle Fusion Applications and Oracle Identity Management Databases".
This chapter describes how to update your Oracle Fusion Applications database and Oracle Identity Management database before an upgrade.

This chapter contains the following topics:

- Apply Exadata Patches for Release 8
- Run RUP Lite for RDBMS

If you use Oracle Exadata Database Machine, run only the steps in Section 3.1, "Apply Exadata Patches for Release 8". If you do not use Oracle Exadata Database Machine, start with Section 3.2, "Run RUP Lite for RDBMS".

---

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

**Note:** 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. For more information, see "Backing Up and Recovering Oracle Fusion Applications" in the *Oracle Fusion Applications Administrator’s Guide*.

### 3.1 Apply Exadata Patches for Release 8

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

#### 3.1.1 Quarterly Database Patches

Apply the quarterly database patch (Patch 16474946 - QUARTERLY DATABASE PATCH FOR EXADATA (APR 2013 - 11.2.0.3.17) for your platform.

- Linux: p16474946_112030_Linux-x86-64.zip
- Solaris Sparc64: p16474946_112030_SOLARIS64.zip
- Solaris86-64: p16474946_112030_Solaris86-64.zip
3.1.2 Generic Exadata Patches

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

- p12317925_112030_Generic.zip
- p13470616_112030_Generic.zip
- p13498243_112030_Generic.zip
- p13508115_112030_Generic.zip
- p13992953_112030_Generic.zip
- p14802958_1120317ExadataDatabase_Generic.zip
- p16287905_112030_Generic.zip
- p16763016_112030_Generic.zip

3.1.3 Linux Exadata Patches

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

- p10255235_112030_Linux-x86-64.zip
- p12552578_1120317ExadataDatabase_Linux-x86-64.zip
- p12646746_112030_Linux-x86-64.zip
- p12738119_1120317ExadataDatabase_Linux-x86-64.zip
- p12977501_112030_Linux-x86-64.zip
- p12985184_112030_Linux-x86-64.zip
- p13014128_112030_Linux-x86-64.zip
- p13078786_112030_Linux-x86-64.zip
- p13365700_112030_Linux-x86-64.zip
- p13404129_112030_Linux-x86-64.zip
- p13429702_112030_Linux-x86-64.zip
- p134304129_112030_Linux-x86-64.zip
- p13632653_112030_Linux-x86-64.zip
- p13741583_1120317ExadataDatabase_Linux-x86-64.zip
- p13743357_1120317ExadataDatabase_Linux-x86-64.zip
- p13863932_1120317ExadataDatabase_Linux-x86-64.zip
- p13989379_1120317ExadataDatabase_Linux-x86-64.zip
- p14015403_1120317ExadataDatabase_Linux-x86-64.zip
- p14029429_112030_Linux-x86-64.zip
- p14058884_112030_Linux-x86-64.zip
- p14164849_112030_Linux-x86-64.zip
- p14343501_1120317ExadataDatabase_Linux-x86-64.zip
- p14373728_1120317ExadataDatabase_Linux-x86-64.zip
- p14555370_1120317ExadataDatabase_Linux-x86-64.zip
- p14571027_112030_Linux-x86-64.zip
Apply the following Exadata patches if you are on the Solaris Sparc64 platform:

- p10255235_112030_SOLARIS64.zip
- p12552578_1120317ExadataDatabase_SOLARIS64.zip
- p12646746_112030_SOLARIS64.zip
- p12738119_1120317ExadataDatabase_SOLARIS64.zip
- p12977501_112030_SOLARIS64.zip
- p12985184_112030_SOLARIS64.zip
- p13014128_112030_SOLARIS64.zip
- p13078786_112030_SOLARIS64.zip
- p13365700_112030_SOLARIS64.zip
- p13404129_112030_SOLARIS64.zip
- p13429702_112030_SOLARIS64.zip
- p13632653_112030_SOLARIS64.zip
- p13741583_1120317ExadataDatabase_SOLARIS64.zip
- p13743357_1120311ExadataDatabase_SOLARIS64.zip
- p13863932_1120317ExadataDatabase_SOLARIS64.zip
- p13989379_1120317ExadataDatabase_SOLARIS64.zip

3.1.4 Solaris Sparc64 Exadata Patches

Apply the following Exadata patches if you are on the Solaris Sparc64 platform:
3.1.5 Solaris 86 X64 Exadata Patches

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

- p10255235_112030_Solaris86-64.zip
- p12552578_1120317ExadataDatabase_Solaris86-64.zip
- p12646746_112030_Solaris86-64.zip
- p12738119_1120317ExadataDatabase_Solaris86-64.zip
- p12977501_112030_Solaris86-64.zip
- p12985184_112030_Solaris86-64.zip
- p13014128_112030_Solaris86-64.zip
- p13078786_112030_Solaris86-64.zip
- p13365700_112030_Solaris86-64.zip
- p13404129_112030_Solaris86-64.zip
- p13429702_112030_Solaris86-64.zip
- p13632653_112030_Solaris86-64.zip
- p13741583_1120317ExadataDatabase_Solaris86-64.zip
- p13743357_1120311ExadataDatabase_Solaris86-64.zip
- p13863932_1120317ExadataDatabase_Solaris86-64.zip
- p13989379_1120317ExadataDatabase_Solaris86-64.zip
- p14015403_1120317ExadataDatabase_Solaris86-64.zip
- p14029429_112030_Solaris86-64.zip
- p14058884_112030_Solaris86-64.zip
- p14164849_112030_Solaris86-64.zip
- p14343501_1120317ExadataDatabase_Solaris86-64.zip
- p14373728_1120317ExadataDatabase_Solaris86-64.zip
- p14555370_1120317ExadataDatabase_Solaris86-64.zip
- p14571027_112030_Solaris86-64.zip
- p14632583_1120317ExadataDatabase_Solaris86-64.zip
- p14679292_112030_Solaris86-64.zip
- p14734989_1120317ExadataDatabase_Solaris86-64.zip
- p15826962_1120317ExadataDatabase_Solaris86-64.zip
- p15866520_1120317ExadataDatabase_Solaris86-64.zip
- p15933374_1120317ExadataDatabase_Solaris86-64.zip
- p16100861_1120317ExadataDatabase_Solaris86-64.zip
- p16196536_1120317ExadataDatabase_Solaris86-64.zip
- p16664800_1120317ExadataDatabase_Solaris86-64.zip
- p16744704_1120317ExadataDatabase_Solaris86-64.zip
- p16751621_1120317ExadataDatabase_Solaris86-64.zip
- p16809786_1120317ExadataDatabase_Solaris86-64.zip
- p16832587_1120317ExadataDatabase_Solaris86-64.zip
- p16853054_1120317ExadataDatabase_Solaris86-64.zip
- p16870100_1120317ExadataDatabase_Solaris86-64.zip
- p17036973_112030_Solaris86-64.zip
- p17284817_1120317ExadataDatabase_Solaris86-64.zip
- p17449940_1120317ExadataDatabase_Solaris86-64.zip
3.2 Run RUP Lite for RDBMS

Run the RUP Lite for RDBMS utility to perform the tasks required to update your Oracle Fusion Applications database before you upgrade to Release 8. RUP Lite for RDBMS can be run in the following modes:

- **Validate mode:**
  - Validates database parameters as described in Table 3–1.

- **Set database parameters mode:**
  - Sets database parameters to the values described in Table 3–1, if required.
  - Restarts the database instance, if requested.

- **Apply mode:**
  - Stops the listener and shuts down the database instance. (optional)
  - Configures Oracle Configuration Manager (OCM) in disconnected mode, if required.
  - Unzips Opatch, if it is available in `REPOSITORY_LOCATION`.
  - Applies patch set updates (PSUs) and one-off patches in `REPOSITORY_LOCATION`.
  - Applies downloaded one-off patches in the `11.1.8.0.0_post_repo_patches` directory.
  - Starts the listener and the database instance. (optional)
  - Runs `catbundle.sql` if any PSUs were applied. (optional)
  - For each patch applied, runs the post installation script, `postinstall.sql`, if it exists. (optional)
  - Runs `catmetx.sql`. (optional)

- **Apply Post Changes mode:**
  - Runs `catbundle.sql` if any PSUs exist.
  - For each patch, runs the post installation script, `postinstall.sql`, if it exists.
  - Runs `catmetx.sql`.

The following table displays the recommendations for tuning the database parameters. The validate mode of RUP Lite for RDBMS verifies whether these parameters contain the recommended value. The setdbparameter mode of RUP Lite for RDBMS updates the parameters to the recommended value.

**Table 3–1  Recommended Values for Database Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Location</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISK_ASYNCH_IO</td>
<td>Disk IO</td>
<td>Spfile/pfile</td>
<td>true</td>
</tr>
<tr>
<td>FILESYSTEMIO_OPTIONS</td>
<td>Disk IO</td>
<td>Spfile/pfile</td>
<td>unset so the database chooses a default value based on the platform</td>
</tr>
<tr>
<td>INBOUND_CONNECT_TIMEOUT_listener_name</td>
<td>Connection timeout</td>
<td>TNS_ADMIN/listener.ora</td>
<td>120</td>
</tr>
<tr>
<td>SQLNET.INBOUND_CONNECT_TIMEOUT</td>
<td>Connection timeout</td>
<td>TNS_ADMIN/sqlnet.ora</td>
<td>130</td>
</tr>
</tbody>
</table>
RUP Lite for RDBMS uses non-interactive OPatch calls to apply RDBMS patches. OPatch tries to install and configure Oracle Configuration Manager (OCM) if OCM has not already been installed and configured. This causes non-interactive OPatch calls to fail in some cases. To avoid this issue, Oracle recommends that you install OCM prior to running RUP Lite for RDBMS. If you plan to use OCM, you should configure it after you install it. If you do not plan to use OCM, you can either configure it in disconnected mode or let RUP Lite for RDBMS configure it. If you install OCM and do not configure it, RUP Lite for RDBMS will automatically configure it in disconnected mode.

If you do not use Oracle Exadata Database Machine, run RUP Lite for RDBMS to automatically apply the mandatory Oracle Database patches mentioned in the "Oracle Database" section of Oracle Fusion Applications release notes. This step applies Oracle Database patches that reside in both the REPOSITORY_LOCATION and the 11.1.8.0.0_post_repo_patches directories, which you downloaded in Section 2.3.5, "Download and Unzip the Repository and Patches". Follow the steps in Section 3.2.1, "Run RUP Lite for RDBMS".

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

**Related Links**
The following document provides additional information related to subjects discussed in this section:

- For more information about installing and configuring OCM, see "Installing Oracle Configuration Manager Using the Command Line Interface" in the *Oracle Configuration Manager Installation and Administration Guide*.

---

**3.2.1 Run RUP Lite for RDBMS**

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

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

1. Apply the version of OPatch that is delivered in the repository. It is available at REPOSITORY_LOCATION/installers/database/opatch/p6880880_112000_Linux-x86-64.zip.

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

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

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

   ```
   createTPBundle.jar
   createTPBundle.cmd
   createTPBundle.sh
   ojdl.jar
   tpBundleConfig_DB.xml
   ```

---

Here is the table containing recommended values for database parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Location</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>ACTIVE_SESSION_LEGACY</em></td>
<td>Initialization</td>
<td>Spfile/pfile</td>
<td>true</td>
</tr>
</tbody>
</table>

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

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

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

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

The following options are available for `createTPBundler`:
- `-shiphomelocation`: Location of the `createTPBundler` repository.
- `-tempdir`: Destination directory to which the generated zip file was copied.
- `-target`: Target against which the copy should be initiated. Use the value, DB.
- `-patchdownloadloc`: Location of the patch directory where you downloaded the patches in Section 2.3.5, "Download and Unzip the Repository and Patches". Use this option only if you downloaded patches to a directory other than the default patch download directory, which is `11.1.8.0.0_post_repo_patches`.
- `-logfile`: Full path of the `createTPbundle` log file. The default is `createTPBundle.log` in the current directory.
- `-loglevel`: Log level for the `createTPbundler` utility. Valid values are SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST. The default value is INFO.

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

6. Log in to the database server host.

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

```
|-- DB_timestamp
   |-- db_server_bundle
      |-- README.txt
      |-- bin
      |   |-- ruplite.bat
      |   |-- ruplite.sh
      |-- metadata
      |   |-- env.properties
      |   |-- installer.properties
      |   |-- plugin-metadata.txt
      |-- custom_db_server
         |-- database
         |   |-- patch
```
8. Perform this step only if you are running RUP Lite for RDBMS on an Oracle VM environment.

As the root user, change the permissions on the DB_timestamp subdirectory:

```bash
chmod -R 777 DB_timestamp
```

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

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

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

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

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

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

11. Update the following properties in the work_dir/DB_timestamp/db_server_bundle/metadata/env.properties file. Example values are shown.

    - ORACLE_SID=Use an instance name that belongs to the fusionapps database.
    - ORACLE_HOME=Use an Oracle home directory on which patches must be applied, such as /u01/db/11.2.0.3. Ensure that you do not include any trailing characters after this directory path, such as a "/".
    - TNS_ADMIN=Use a valid location that contains SQL*Net configuration files for the database.
    - LISTENER_NAME=Use a listener name.
    - PFILE=/u01/db/11.2.0.3/dbs/init.ora, for example. Update PFILE if your database is started using pfile. You can retrieve this value by running the following query:
      ```sql
      select NAME, VALUE from v$parameter where NAME like '%file%';
      ```
    - DBSERVER_RESTART=true or false
      To minimize downtime, you can use "false" for setdbparameters mode, and "true" for apply mode.
If `DBSERVER_RESTART` is set to "false", the database server, listener and other related services must be manually stopped before running RUP Lite in apply mode. Then after running RUP Lite in apply mode, you must run Step 21.

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

- **a.** Start the database instance.
- **b.** Start the listener.
- **c.** Run `catbundle.sql` with arguments "psu apply" on non-Windows and "winbundle apply" on Windows.
  
  (UNIX)
  
  `$ORACLE_HOME/rdbms/admin/catbundle.sql psu apply`
  
  (Windows)
  
  `%ORACLE_HOME%/rdbms/admin/catbundle.sql winbundle apply`
  
  For a list of `catbundle.sql` errors that can be ignored, see Section 7.19.11, "Ignorable Errors Reported by catbundle.sql".

- **d.** For each patch applied, run the post installation script, `postinstall.sql`, if it exists.

- **e.** Run `ORACLE_HOME/rdbms/admin/catmetx.sql`.
  
  (UNIX)
  
  `$ORACLE_HOME/rdbms/admin/catmetx.sql`
  
  (Windows)
  
  `%ORACLE_HOME%/rdbms/admin/catmetx.sql`

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

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

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

**13.** Stop all user applications.

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

  `DB_timestamp/db_server_bundle/bin`

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

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

**16.** Review the log file, `output/logs/ruplitewritevalidate.log`, to confirm whether the database parameters contain the values you set in Step 11 and the values displayed in Table 3–1, “Recommended Values for Database Parameters”, and to review any errors that may have occurred.
If any of the parameters do not contain the recommended value, proceed to the next step to run RUP Lite for RDBMS in `setdbparameters` mode. If all parameters are correct, proceed to Step 19 to run RUP Lite for RDBMS in `apply` mode.

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

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

**18. Review the log file, `output/logs/rruplitesetdbparameters.log`, to confirm whether the database parameters contain the values displayed in Table 3–1, "Recommended Values for Database Parameters", and to review any errors that may have occurred.**

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

You can set the parameter `DBSERVER_RESTART` (available in `metadata/env.properties`) to "false" if you want to manually shut down the database, stop the listener before patching, and start it up after applying the patches. For Windows, if you set `DBSERVER_RESTART` to "false", follow the steps in Section 3.2.3, "Stop Services on Windows Before Running RUP Lite For RDBMS".

---

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

---

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

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

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

- ruplitedb.log
- tp_property_editor_timestamp.log
- db_apply_repository_patches_timestamp.log
- db_validate_repository_patches_timestamp.log
- repository_patch_validate_results_timestamp.xml
- post_db_restart_actions_timestamp.log

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

The `post_db_restart_actions_timestamp.log` file includes the output from `catbundle.sql` and `catmetx.sql`. For a list of `catbundle.sql` errors that can be ignored, see Section 7.19.11, "Ignorable Errors Reported by catbundle.sql".

**21. If you set `DBSERVER_RESTART` to "false", perform the following steps:**
Run RUP Lite for RDBMS

3.1.2 Run RUP Lite for RDBMS

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

1. Follow Steps 1 through 10 in Section 3.2.1, "Run RUP Lite for RDBMS".
2. Stop all user applications that use the Oracle home directory being patched.
3. Update the following properties in the work_dir/DB_timestamp/db_server_bundle/metadata/env.properties file. Example values are shown.
   - ORACLE_HOME=Use an Oracle home directory on which patches must be applied, such as /u01/db/11.2.0.3. Ensure that you do not include any trailing characters after this directory path, such as a "/".
   - ORACLE_SID=Use an instance name that belongs to the fusionapps database and is run against the Oracle home set in the previous property.
   - TNS_ADMIN=Use a valid tns_admin location, which is typically located under the grid infra and contains listener.ora and sqlnet.ora files.
   - LISTENER_NAME=Use a listener name.
   - PFILE=/u01/db/11.2.0.3/dbs/init.ora, for example.
     Update PFILE if your database is started using pfile.
   - DBSERVER_RESTART=false
     Note that the value of DBSERVER_RESTART must be "false".
4. Verify that the java version is 1.6 or above by using the following command:

(UNIX)
$JAVA_HOME/bin/java -version
(Windows)
%JAVA_HOME%\bin\java -version

5. Change directory to the following location:
   DB_timestamp/db_server_bundle/bin

6. Run RUP Lite for RDBMS in validate mode. The database instance and listener must be up.
   (UNIX) ruplite.sh validate
   (Windows) ruplite.bat validate

7. Review the log file, output/logs/ruplitevalidate.log, to confirm whether the database parameters contain the values you set in Step 3 and the values displayed in Table 3–1, "Recommended Values for Database Parameters", and to review any errors that may have occurred.

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

8. Run RUP Lite for RDBMS in setdbparameters mode. The database instance and listener must be up.
   (UNIX) ruplite.sh setdbparameters
   (Windows) ruplite.bat setdbparameters

9. Review the log file, output/logs/ruplitesetdbparameters.log, to confirm whether the database parameters contain the values displayed in Table 3–1, "Recommended Values for Database Parameters", and to review any errors that may have occurred.

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

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

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

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

11. Stop the listener that is running from all Oracle homes in the cluster, using the following command:

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

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

12. To avoid an issue with active files while patching, ensure that no applications or processes are running from the ORACLE_HOME that is referenced in metadata/env.properties.
13. Run RUP Lite for RDBMS in apply mode.
   (UNIX) ruplite.sh
   (Windows) ruplite.bat

14. Review the following log files located under the output/logs directory if any errors occurred:
   ruplitedb.log
   tp_property_editor_timestamp.log
   db_apply_repository_patches_timestamp.log
   db_validate_repository_patches_timestamp.log
   repository_patch_validate_results_timestamp.xml

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

15. RAC databases often share a single ORACLE_HOME for all RAC instances. If you have this configuration, continue to the next step.
    If you do not have this configuration, you must update the files in the other ORACLE_HOMEs for your RAC database. To update the other ORACLE_HOMEs, repeat Steps 4 through 8 in Section 3.2.1, “Run RUP Lite for RDBMS” for RAC instances with non-shared ORACLE_HOMEs. Then repeat Steps 3 through 15 in this section for all RAC instances. Note that this may involve multiple hosts and nodes.

16. Start the database.

17. Run RUP Lite for RDBMS in applypostchanges mode.
   (UNIX) ruplite.sh applypostchanges
   (Windows) ruplite.bat applypostchanges

18. Review the following log files, located under the output/logs directory, if any errors occurred:
   ruplitedbapplypostchanges.log
   post_db_restart_actions_timestamp.log

   These log files are generated by running ruplite in applypostchanges mode. The post_db_restart_actions_timestamp.log file includes the output from catbundle.sql and catmetx.sql. For a list of catbundle.sql errors that can be ignored, see Section 7.19.11, “Ignorable Errors Reported by catbundle.sql”.

19. You must manually execute any manual steps that are documented in the README.txt file of the patches you applied with RUP Lite for RDBMS. RUP Lite for RDBMS executes postinstall.sql if it is mentioned as a manual step. All other steps have to be done manually.
    If there is more than one ORACLE_HOME in the RAC database, you do not need to run SQL scripts again when patching the 2nd through the nth ORACLE_HOME, but you do need to perform any manual steps that update ORACLE_HOME.

20. Start the listener from all Oracle homes in the cluster. For Windows, start the services described Section 3.2.3, "Stop Services on Windows Before Running RUP Lite For RDBMS”.

21. Proceed to Section 3.2.4, "Run Additional Post Database Start Scripts for Patches for Release 8".
3.2.3 Stop Services on Windows Before Running RUP Lite For RDBMS

For a Windows platform, the following services should be stopped before you run RUP Lite for RDBMS:

- OracleOraDb11g_home1TNSListenerLISTENER_<SID>
- OracleOraDb11g_home1ClrAgent
- OracleDBConsole<SID>
- OracleJobScheduler<SID>
- OracleService<SID>
- OracleMTSRecoveryService
- Windows Management Instrumentation
- Distributed Transaction Coordinator
- Oracle <SID> VSS Writer Service

If RUP Lite for RDBMS fails to stop or start a service, you can manually manage each service from the Control Panel. Select Administrative Tools, then Services. Right click on each service and choose the Stop or Start option.

3.2.4 Run Additional Post Database Start Scripts for Patches for Release 8

RUP Lite for RDBMS consolidates the README.txt files for all applied patches into one consolidated README.txt file, which is located in the OUI_Component README.txt directory. You must manually execute any manual steps that are documented in the consolidated README.txt file. RUP Lite for RDBMS executes postinstall.sql if it is mentioned as a manual step. All other steps have to be performed manually on the DB host by any user that has system privileges. Perform these steps on only one of the nodes in the case of a RAC setup.

Database patches can be found at the following locations:

```
SHARED_UPGRADE_LOCATION/POD_NAME/RELEASE_VERSION/DB/RUPLiteDB/DB_TIME_STAMP/db_server_bundle/db_server/database/psu (if exists)
SHARED_UPGRADE_LOCATION/POD_NAME/RELEASE_VERSION/DB/RUPLiteDB/DB_TIME_STAMP/db_server_bundle/db_server/database/patch
```

Example location:

```
/u01/shared_location/CRM/11.1.8.0.0/DB/RUPLiteDB/DB_2012-08-07_03-43-22/db_server_bundle/db_server/database/patch/
```
This chapter describes the steps to ensure system reliability by running Pre-downtime checks.

This chapter includes the following topics:

- Run the Health Checker Utility
- Run the Pre-validation Check on IDM Hosts

4.1 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 which 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.

This section contains the following topics:

- Pre-Downtime Health Checker Manifests
- Run Health Checker on the Primordial Host
- Run Health Checker on the Mid Tier Host
- Run Health Checker on the OHS Host
- Run Health Checker on the Database Host

4.1.1 Pre-Downtime Health Checker Manifests

When you run Health Checker, you specify a manifest file, depending on which checks you are running. During pre-downtime, you run the following manifests.

- GeneralSystemHealthChecks.xml: Run on the Primordial, Mid tier, OHS, and Database hosts
- PreDowntimeUpgradeReadinessHealthChecks.xml: Run on the Primordial, Mid tier, OHS, and Database hosts
- DataQualityChecks.xml: Run on the Primordial host only

For more information about the checks performed by Health Checker, see Section A.3.2.2, "Health Checker Plug-ins."
4.1.2 Run Health Checker on the Primordial Host

Perform the following steps to run Health Checker on the Primordial host.

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 `/server01/APPTOP/fusionapps`, then set the `APPLICATIONS_BASE` environment variable to `/server01/APPTOP`.
   - `REPOSITORY_LOCATION`: The directory where the repository is staged, `SHARE_UPGRADE_LOCATION/11.1.8.0.0/Repository`.
   - `FA_SCRIPTS_DOWNLOAD_DIR`: The location of the `PatchConflictManager.py` utility, `SHARE_UPGRADE_LOCATION/PatchConflictManager`, which you downloaded in Section 2.3.4, "Download and Unzip the Patch Conflict Manager Utility".
   - `DOWNLOAD_PATCH_DIR`: The location where you downloaded post-release patches, `SHARE_UPGRADE_LOCATION/11.1.8.0.0_posw_repo_patches`, in Section 2.3.5.3, "Download and Unzip Mandatory Post-Release 8 Patches".
   - Note that the following environment variables are set in the primordial host but the values come from the OHS host. For example, `/u01/mw_home/Oracle_WT1/instances/CommonDomain_webtier` does not exist on the primordial host and this path is a path on the OHS host. However, Health Checker requires this environment variable on the primordial host.
     - `OHS_INSTANCE_ID`: The OHS instance id being upgraded, for example, ohs1.
     - `WT_CONFIG_HOME`: The web tier instance configuration directory, for example, `/APPTOP/instance/CommonDomain_webtier`.
     - `OHS_HOST_NAME`: The OHS host name, for example, ohs_host.my.company.com.
   - `HC_OVERRIDE_FILES`: The location of any Health Checker overrides that you may have created, as described in Section A.3.2.3.1, "Create Override Files." The default location is `SHARE_UPGRADE_LOCATION/healthchecker/POD_NAME`. You can skip this variable if you do not have Health Checker overrides.

3. Run Health Checker for each manifest. Note that this is one command.

   (UNIX)
   ```bash
   ORCH_LOCATION/fusionapps/applications/lcm/hc/hcplug.sh -hostType PRIMORDIAL -manifest ORCH_LOCATION/fusionapps/applications/lcm/hc/bin/hcplug.sh -hostType PRIMORDIAL -manifest ORCH_LOCATION/fusionapps/applications/lcm/hc/bin/hcplug.sh -hostType PRIMORDIAL -manifest ORCH_LOCATION/fusionapps/applications/lcm/hc/bin/hcplug.sh -hostType PRIMORDIAL -manifest ORCH_LOCATION/fusionapps/applications/lcm/hc/bin/hcplug.sh -hostType PRIMORDIAL -manifest
   ```

4-2 Upgrade Guide
Run the Health Checker Utility

Running Pre-Downtime Checks

(Windows)
ORCH_LOCATION\fusionapps\applications\lcm\hc\bin\hcplug.cmd -hostType PRIMORDIAL -manifest
ORCH_LOCATION\fusionapps\applications\lcm\hc\config\ga\GeneralSystemHealthChecks.xml -DlogLevel=FINEST

ORCH_LOCATION\fusionapps\applications\lcm\hc\bin\hcplug.cmd -hostType PRIMORDIAL -manifest
ORCH_LOCATION\fusionapps\applications\lcm\hc\config\ga\PreDowntimeUpgradeReadinessHealthChecks.xml -DlogLevel=FINEST

ORCH_LOCATION\fusionapps\applications\lcm\hc\bin\hcplug.cmd -hostType PRIMORDIAL -manifest
ORCH_LOCATION\fusionapps\applications\lcm\hc\config\ga\DataQualityChecks.xml -DlogLevel=FINEST

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. If the failure is a known issue and you want to exclude the check, refer to Section A.3.2.3, "Override Health Checks."

The following table provides the location of log files and reports on the Primordial host. Note that Health Checker log directories are created with reference to version you are upgrading from during the pre-upgrade phase.

<table>
<thead>
<tr>
<th>Manifest File Name</th>
<th>Log File Location</th>
<th>Report Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>GeneralSystemHealthChecks.xml</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/healthchecker/PRIMORDIAL_hostname-GeneralSystemHealthChecks_timestamp.log</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/healthchecker/PRIMORDIAL_hostname-GeneralSystemHealthChecks_timestamp.html</td>
</tr>
<tr>
<td>PreDowntimeUpgradeReadinessHealthChecks.xml</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/healthchecker/PRIMORDIAL_hostname-PreDowntimeUpgradeReadinessHealthChecks_timestamp.log</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/healthchecker/PRIMORDIAL_hostname-PreDowntimeUpgradeReadinessHealthChecks_timestamp.html</td>
</tr>
<tr>
<td>DataQualityChecks</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/healthchecker/PRIMORDIAL_hostname-DataQualityHealthChecks_timestamp.log</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/healthchecker/PRIMORDIAL_hostname-DataQualityHealthChecks_timestamp.html</td>
</tr>
</tbody>
</table>

4.1.3 Run Health Checker on the Mid Tier Host

Perform the following steps to run Health Checker on the Mid tier host.

1. Set the following environment variables:
   - APPLICATIONS_BASE: The directory that contains Oracle Fusion Applications. For example, if Oracle Fusion Applications is installed in /server01/APPTOP/fusionapps, then set the APPLICATIONS_BASE environment variable to /server01/APPTOP.
Run the Health Checker Utility

- **REPOSITORY_LOCATION**: The directory where the repository is staged, `SHARED_LOCATION/11.1.8.0.0/Repository`.

- **IS_SECONDARY_NODE**: A value of `yes` or `no`, to indicate whether the Mid tier node is secondary.

- **HC_OVERRIDE_FILES**: The location of any Health Checker overrides that you may have created, as described in Section A.3.2.3.1, "Create Override Files." The default location is `SHARED_UPGRADE_LOCATION/healthchecker/POD_NAME`. You can skip this variable if you do not have Health Checker overrides.

2. Run Health Checker for each manifest. 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/ga/GeneralSystemHealthChecks.xml -DlogLevel=FINEST
   ORCH_LOCATION/fusionapps/applications/lcm/hc/bin/hcplug.sh -hostType MIDTIER -manifest
   ORCH_LOCATION/fusionapps/applications/lcm/hc/config/ga/PreDowntimeUpgradeReadinessHealthChecks.xml -DlogLevel=FINEST
   ```

   (Windows)
   ```
   ORCH_LOCATION/fusionapps\applications\lcm\hc\bin\hcplug.cmd -hostType MIDTIER -manifest
   ORCH_LOCATION/fusionapps\applications\lcm\hc\config\ga\GeneralSystemHealthChecks.xml -DlogLevel=FINEST
   ORCH_LOCATION/fusionapps\applications\lcm\hc\bin\hcplug.cmd -hostType MIDTIER -manifest
   ORCH_LOCATION/fusionapps\applications\lcm\hc\config\ga\PreDowntimeUpgradeReadinessHealthChecks.xml -DlogLevel=FINEST
   ```

3. If any health checks fail, refer to the Health Checker log files and reports to find the corrective action 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. If the failure is a known issue and you want to exclude the check, refer to Section A.3.2.3, "Override Health Checks."

   The following table provides the location of log files and reports on the Mid tier host.

<table>
<thead>
<tr>
<th>Manifest File Name</th>
<th>Log File Location</th>
<th>Report Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>GeneralSystemHealthChecks.xml</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/healthchecker/MIDTIER_hostname-GeneralSystemHealthChecks_timestamp.log</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/healthchecker/MIDTIER_hostname-GeneralSystemHealthChecks_timestamp.html</td>
</tr>
</tbody>
</table>
Run the Health Checker Utility

4.1.4 Run Health Checker on the OHS Host

Perform the following steps to run Health Checker on the OHS host.

1. Set the following environment variables:

   - **APPLICATIONS_BASE**: `ORCH_LOCATION`, which was created in Section 2.3.7, "Unzip Orchestration.zip".
   - **REPOSITORY_LOCATION**: The directory where the repository is staged, `SHARE_HOME/11.1.8.0.0/Repository`.
   - **JAVA_HOME**: The jdk6 location under APPLTOP, for example, `/u01/APPLTOP/webtier_mwhome/webtier/jdk`. Do not use the jdk under the orchestration directory. Note that you use this same location for the `-jreloc` argument when running the commands in this section.
   - **WT_MW_HOME**: Location of the web tier `MW_HOME`, for example, `/oracle/work/MW_HOME`.
   - **WT_ORACLE_HOME**: Location of the web tier directory, which is a subdirectory under **WT_MW_HOME**, for example, `/APPTOP/webtier_mwhome`, or `/APPTOP/webtier_mwhome/webtier`.
   - **WT_CONFIG_HOME**: Location of the web tier instance directory, for example, `/oracle/work/MW_HOME/Oracle_WT1/instances/instance1`.
   - **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.
   - **UPGRADEOHS_PROP_FILE**: The location for the OHS `env.properties` file on each OHS host, which you created in Step 1.
   - **OHS_UPGRADE_BINARY_HOSTNAME**: A comma separated list of your OHS host names which do not share binaries. For example, if you have 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, which is 11.1.7.0.0.
   - **FA_SCRIPTS_DOWNLOAD_DIR**: The location of the PatchConflictManager.py utility, `SHARE_HOME/11.1.8.0.0_post_repo_patches`, which you downloaded in Section 2.3.5.3, "Download and Unzip Mandatory Post-Release 8 Patches".
   - **DOWNLOAD_PATCH_DIR**: The location of downloaded post-release patches, `SHARE_HOME/11.1.8.0.0_post_repo_patches`, which you downloaded in Section 2.3.5.3, "Download and Unzip Mandatory Post-Release 8 Patches".
   - **HC_OVERRIDE_FILES**: The location of any Health Checker overrides that you may have created, as described in Section A.3.2.3.1, "Create Override Files."
The default location is `SHARE_UPGRADE_LOCATION/healthchecker/POD_NAME`. You can skip this variable if you do not have Health Checker overrides.

2. Run Health Checker for each manifest. 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/ga/GeneralSystemHealthChecks.xml -DlogLevel=FINEST -jreLoc JDK6_LOCATION -logDir /u01/logs/OHS/
```

(UNIX)
```
FRONT_LOCATION/fusionapps/applications/lcm/hc/bin/hcplug.sh -hostType OHS -manifest ORCH_LOCATION/fusionapps/applications/lcm/hc/config/ga/PreDowntimeUpgradeReadinessHealthChecks.xml -DlogLevel=FINEST -jreLoc JDK6_LOCATION -logDir /u01/logs/OHS/
```

(Windows)
```
ORCH_LOCATION\fusionapps\applications\lcm\hc\bin\hcplug.cmd -hostType OHS -manifest ORCH_LOCATION\fusionapps\applications\lcm\hc\config\ga\GeneralSystemHealthChecks.xml -DlogLevel=FINEST -jreLoc JDK6_LOCATION -logDir C:\Shared\webgate\log\logs\healthchecker
```

(Windows)
```
ORCH_LOCATION\fusionapps\applications\lcm\hc\bin\hcplug.cmd -hostType OHS -manifest ORCH_LOCATION\fusionapps\applications\lcm\hc\config\ga\PreDowntimeUpgradeReadinessHealthChecks.xml -DlogLevel=FINEST -jreLoc JDK6_LOCATION -logDir C:\Shared\webgate\log\logs\healthchecker
```

3. If any health checks fail, refer to the Health Checker log files and reports to find the corrective action 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. If the failure is a known issue and you want to exclude the check, refer to Section A.3.2.3, "Override Health Checks."

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

<table>
<thead>
<tr>
<th>Manifest File Name</th>
<th>Log File Location</th>
<th>Report Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>PreDowntimeUpgradeReadinessHealthChecks.xml</td>
<td>/u01/logs/OHS/logs/healthchecker/hostname-PreDowntimeUpgradeReadinessHealthChecks_timestamp.log</td>
<td>/u01/logs/OHS/logs/healthchecker/hostname-PreDowntimeUpgradeReadinessHealthChecks_timestamp.html</td>
</tr>
</tbody>
</table>
4.1.5 Run Health Checker on the Database Host

Perform the following steps to run Health Checker from the database host. Note that you run Health Checker from the Oracle Fusion Applications database host and not from the Oracle Identity Management database host.

1. Create a ZIP archive of the Health Checker framework that exists on the primordial host, by extracting the contents from the Release 8 Repository. You created this repository, $SHARED_LOCATION/11.1.8.0.0/Repository, in Section 2.3.2.1, “Create Release 8 Repository Directories.”

Run the following commands. If you are on a RAC database, run the commands from both nodes.

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

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

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

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

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

4. Set the following environment variables. Note that all environment variables must reference the absolute path.

- APPLICATIONS_BASE - The HC_TOP directory, where hc.zip was unzipped
- $REPOSITORY_LOCATION: The directory where the repository is staged, $SHARED_LOCATION/11.1.8.0.0/Repository.
- JAVA_HOME: The jdk6 location under APPLTOP, for example, /u01/APPLTOP/webtier_mwhome/webtier/jdk. Do not use the jdk under the orchestration directory. Note that you use this same location for the -jreloc argument when running the commands in this section.
- ORACLE_HOME - The Oracle Database Home directory
- PATH - $PATH:$ORACLE_HOME/bin
- LISTENER_NAME - The Oracle database listener name
- ORACLE_SID - The Oracle database SID
- TNS_ADMIN - $ORACLE_HOME/network/admin
- LD_LIBRARY_PATH - $ORACLE_HOME/lib
- GRID_HOME - On RAC configurations, set this to GRID_HOME, otherwise set to ORACLE_HOME

On Windows, append ORACLE_HOME/bin to the current path, as follows:
Run the Health Checker Utility

5. Run Health Checker for both manifests and specify -hostType and the -jreLoc.

(UNIX)
APPLICATIONS_BASE/fusionapps/applications/lcm/hc/bin/hcplug.sh -hostType DB -jreLoc JDK_version_1.6_under_APPLTOP -manifest APPLICATIONS_BASE/fusionapps/applications/lcm/hc/config/PreDowntimeUpgradeReadinessHealthChecks.xml -DlogLevel=FINEST -logDir logfile_directory
APPLICATIONS_BASE/fusionapps/applications/lcm/hc/bin/hcplug.sh -hostType DB -jreLoc JDK_version_1.6_under_APPLTOP -manifest APPLICATIONS_BASE/fusionapps/applications/lcm/hc/config/GeneralSystemHealthChecks.xml -DlogLevel=FINEST -logDir logfile_directory

(Windows)
APPLICATIONS_BASE/fusionapps\applications\lcm\hc\bin\hcplug.cmd -hostType DB -jreLoc JDK_version_1.6_under_APPLTOP -manifest APPLICATIONS_BASE/fusionapps\applications\lcm\hc\config\PreDowntimeUpgradeReadinessHealthChecks.xml -DlogLevel=FINEST -logDir logfile_directory
APPLICATIONS_BASE/fusionapps\applications\lcm\hc\bin\hcplug.cmd -hostType DB -jreLoc JDK_version_1.6_under_APPLTOP -manifest APPLICATIONS_BASE/fusionapps\applications\lcm\hc\config\GeneralSystemHealthChecks.xml -DlogLevel=FINEST -logDir logfile_directory

6. If any health checks fail, refer to the Health Checker logs 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. If the failure is a known issue and you want to exclude the check, refer to Section A.3.2.3, “Override Health Checks.”

The following table provides the location of log files and reports on the database host. Note that Health Checker log directories are created with reference to version you are upgrading from, 11.1.8.0.0.

<table>
<thead>
<tr>
<th>Manifest File Name</th>
<th>Log File Location</th>
<th>Report Location - html and xml formats</th>
</tr>
</thead>
<tbody>
<tr>
<td>GeneralSystemHealthChecks.xml</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/healthchecker/DB_hostname-GeneralSystemHealthChecks_timestamp.log</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/healthchecker/DB_hostname-GeneralSystemHealthChecks_timestamp.html</td>
</tr>
<tr>
<td>PreDowntimeUpgradeReadinessHealthChecks.xml</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/healthchecker/DB_hostname-PreDowntimeUpgradeReadinessHealthChecks_timestamp.log</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.7.0.0/healthchecker/DB_hostname-PreDowntimeUpgradeReadinessHealthChecks_timestamp.html</td>
</tr>
</tbody>
</table>
4.2 Run the Pre-validation Check on IDM Hosts

If you are running Oracle Fusion Applications on a SINGLE, 3-NODE, or 4-NODE IDM configuration on a Linux, Solaris, or AIX platform that is a Release 7 IDM provisioned environment, follow the steps in this section. Otherwise, proceed to Chapter 5, "Upgrading to Oracle Fusion Applications Release 8" when you are ready to begin the upgrade.

4.2.1 Confirm Prerequisite Steps Are Complete

Ensure that you have completed the steps in Section 2.3.8, "Copy and Unzip idmUpgrade.zip" and Section 2.5, "Update the patchAutomation.properties File for the IDM Upgrade".

4.2.2 Set Environment Variables

The steps for setting the environment variables on each node vary by platform. Refer to the section that is appropriate for your platform:

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

4.2.2.1 Environment Variables Required for Linux

On Linux, use the system perl, which is perl version 5.8.8 on Oracle Enterprise Linux version 5 and perl version 5.10.1 on Oracle Enterprise Linux version 6.

Set LD_LIBRARY_PATH as follows, only if Oracle Identity Management is not installed in the default location of /u01/IDMTOP.

- 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
  ```

4.2.2.2 Environment Variables Required for AIX

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

- Set LIBPATH.
  - On OID and OIM nodes:
    
    ```
    LIBPATH=OID_ORACLE_HOME/lib
    export LIBPATH
    ```
  - On the OHS node:
    
    ```
    LIBPATH=OHS_ORACLE_HOME/lib
    export LIBPATH
    ```

- Set PERL5LIB to the ORACLE_HOME/perl location.
  - On OID and OIM nodes:
Run the Pre-validation Check on IDM Hosts

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 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

4.2.2.3 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 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 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 OID and OIM nodes:
    PATH=OID_ORACLE_HOME/perl/bin:$PATH
    export PATH
  - On OHS node
    PATH=OHS_ORACLE_HOME/perl/bin:$PATH
    export PATH
4.2.3 Run preValidate.pl on Each Node

Run preValidate.pl on each node as follows. Note that the `REPOSITORY_LOCATION/installers,SHARED_LOCATION/11.1.8.0.0_post_repo_patches` argument is optional and if you include it, the patch conflict manager runs.

- On the OID node:
  ```
  cd SHARED_LOCATION/11.1.8.0.0/idmUpgrade
  perl preValidate.pl OID REPOSITORY_LOCATION/installers,SHARED_LOCATION/11.1.8.0.0_post_repo_patches patchAutomation.properties
  ```

- On the OIM node:
  ```
  cd SHARED_LOCATION/11.1.8.0.0/idmUpgrade
  perl preValidate.pl OIM REPOSITORY_LOCATION/installers,SHARED_LOCATION/11.1.8.0.0_post_repo_patches patchAutomation.properties
  ```

- On the AuthOHS node:
  ```
  cd SHARED_LOCATION/11.1.8.0.0/idmUpgrade
  perl preValidate.pl OHS REPOSITORY_LOCATION/installers,SHARED_LOCATION/11.1.8.0.0_post_repo_patches patchAutomation.properties
  ```

Confirm that the return code is successful on each node.
Run the Pre-validation Check on IDM Hosts
This chapter describes the steps required to upgrade to Oracle Fusion Applications 11g Release 8 (11.1.8).

This chapter contains the following topics:

- Steps to Upgrade to Release 8
- Pause Point Steps

5.1 Steps to Upgrade to Release 8

Perform the following steps to upgrade to Release 8:

- Run Upgrade Orchestrator During Downtime
- Pause Point 1 - Back Up the OPSS Security Store
- Update Status to Success
- Resume Upgrade Orchestrator
- Pause Point 2 - Stop Informatica IR (IIR) Servers
- Update Status to Success
- Resume Upgrade Orchestrator
- Pause Point 3 - Back Up Oracle Fusion Applications
- Update Status to Success
- Resume Upgrade Orchestrator
- Pause Point 4 - Upgrade Oracle Identity Management to Release 8
- Update Status to Success
- Resume Upgrade Orchestrator
- Pause Point 5 - Start External Servers
- Update Status to Success
- Resume Upgrade Orchestrator
- Pause Point 6 - Back Up Oracle Fusion Applications Before Language Pack Upgrade (Language Pack Only)
- Update Status to Success
5.1.1 Run Upgrade Orchestrator During Downtime

Ensure you have successfully completed the steps in Chapter 2, "Preparing to Perform the Release 8 Upgrade," Chapter 3, "Updating the Oracle Fusion Applications and Oracle Identity Management Databases," and Chapter 4, "Running Pre-Downtime Checks."

Start Upgrade Orchestrator during downtime by running the following commands on all host types, including the respective scaled out hosts. Note that the value `POD_NAME`, for the `-pod` argument, refers to the directory you created in Section 2.3.7, "Unzip Orchestration.zip".

You are prompted for the Master Orchestration Password, for which you can enter any value.

If you are upgrading an instance of Oracle Fusion Applications that is the result of a clone, change the Node Manager password as described in Section 5.4, "Change the Node Manager Password (Cloned Environment Only)."

If you are running on an AIX platform, set the environment variables that are described in Section 4.2.2.2, "Environment Variables Required for AIX." Also perform the step in Section 5.3, "Set the SKIP_ROOTPRE Environment Variable (AIX Only).".

---

**Note:** If you set the DISPLAY variable, confirm it is accessible. If you do not set the DISPLAY variable, run `unset/unsetenv DISPLAY` before you run orchestration.

---

1. Run the following command to start orchestration on the Primordial host:

   (Unix)
   ```
   cd ORCH_LOCATION/bin
   ./orchestration.sh -pod POD_NAME -hosttype PRIMORDIAL [-DlogLevel=log_level]
   ```

   (Windows)
   ```
   cd ORCH_LOCATION\bin
   orchestration.cmd -pod POD_NAME -hosttype PRIMORDIAL [-DlogLevel=log_level]
   ```

2. Run the following command to start orchestration on each Mid tier host that is listed in the `HOSTNAME_MIDTIER` property in the `pod.properties` file:

   (Unix)
   ```
   cd ORCH_LOCATION/bin
   ./orchestration.sh -pod POD_NAME -hosttype MIDTIER [-DlogLevel=log_level]
   ```

   (Windows)
   ```
   cd ORCH_LOCATION\bin
   orchestration.cmd -pod POD_NAME -hosttype MIDTIER [-DlogLevel=log_level]
   ```

3. Run the following command to start orchestration on each OHS host that is listed in the `HOSTNAME_OHS` property in the `pod.properties` file:

   (Unix)
   ```
   cd ORCH_LOCATION/bin
   ./orchestration.sh -pod POD_NAME -hosttype OHS [-DlogLevel=log_level]
   ```

   (Windows)
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]

   (Windows)
   cd ORCH_LOCATION\bin
   orchestration.cmd -pod POD_NAME -hosttype IDM [-DlogLevel=log_level]

Section A.2, "Additional Information About Upgrade Orchestrator Commands" provides a complete list of options for the orchestration.sh command.

Upgrade Orchestrator runs the tasks listed in the following table.

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Task ID</th>
<th>Host Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop Index Schedules and Deactivate Index Optimization</td>
<td>StopIndexSchedules</td>
<td>Primordial</td>
</tr>
<tr>
<td>Stop All Servers</td>
<td>StopAllServers</td>
<td>Primordial, OHS, Mid tier</td>
</tr>
<tr>
<td>Set CrashRecoveryEnabled Property to False</td>
<td>DisableCrashRecoveryEnabled</td>
<td>Primordial</td>
</tr>
<tr>
<td>Stop OPMN Control Processes</td>
<td>StopOPMNProcesses</td>
<td>Primordial, OHS, Mid tier</td>
</tr>
<tr>
<td>Stop Node Managers</td>
<td>StopNodeManager</td>
<td>Primordial, Mid tier</td>
</tr>
</tbody>
</table>

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 Section 7.3, "Monitoring Upgrade Orchestration Progress". For information about troubleshooting, see Chapter 7, "Monitoring and Troubleshooting the Upgrade".

**Note:** If the orchestration command results in any hanging tasks on any host, do not use ctrl-C or ctrl-Z to exit. You must update the status of the task that is hanging by using the commands in Section 7.6.2, "Safely Exit Upgrade Orchestrator". After you exit and fix the issue that caused the hanging, restart Upgrade Orchestrator, using the commands specified in this section, on the hosts that were forced to exit.
5.1.2 Pause Point 1 - Back Up the OPSS Security Store

If your environment is a SINGLE, 3-NODE, or 4-NODE IDM configuration and is running on Linux and a Release 7 IDM provisioned environment, Upgrade Orchestrator runs the tasks listed in the following table and this pause point does not occur. Proceed to Section 5.1.5, "Pause Point 2 - Stop Informatica IR (IIR) Servers."

For other environments, orchestration pauses so that you can back up the OPSS Security Store on the IDM host. Perform the steps in Section 5.2.1, "Back Up the OPSS Security Store."

Table 5–2  Tasks Run During the Downtime PreFA Phase for IDM Upgrade

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Task ID</th>
<th>Host Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop Oracle Identity Management - AUTHOHS</td>
<td>StopOHS</td>
<td>IDM</td>
</tr>
<tr>
<td>Stop Oracle Identity Management - OIM</td>
<td>StopOIM</td>
<td>IDM</td>
</tr>
<tr>
<td>Stop Oracle Identity Management - OID</td>
<td>StopOID</td>
<td>IDM</td>
</tr>
<tr>
<td>Back Up OPSS Security Store</td>
<td>BackupOPSS</td>
<td>IDM</td>
</tr>
</tbody>
</table>

5.1.3 Update Status to Success

After you successfully back up the OPSS Security Store, update the task status to "success" by running the `updateStatus` command.

**Note:** The `updateStatus` command must not be run on a host where orchestration is already running. If, for some reason you have to run `updateStatus` for a task on a running host, you must ensure that it is safe to exit orchestration first across the entire environment. Then follow the steps below:

1. Terminate orchestration by following the instructions in Section 7.4, "Terminating Upgrade Orchestrator".
2. Update the task status using the `updateStatus` command.
3. Restart orchestration on all the hosts when ready.

*(Unix)*
cd `ORCH_LOCATION/bin`
./orchestration.sh updateStatus -pod `POD_NAME` -hosttype IDM -hostname `host_name` -release REL8 -phase DowntimePreFA -taskid BackupOPSS -taskstatus success

*(Windows)*
cd `ORCH_LOCATION\bin`
orchestration.cmd updateStatus -pod `POD_NAME` -hosttype IDM -hostname `host_name` -release REL8 -phase DowntimePreFA -taskid BackupOPSS -taskstatus success

5.1.4 Resume Upgrade Orchestrator

Resume orchestration on the IDM host using the command in Section 5.1.1, "Run Upgrade Orchestrator During Downtime", Step 4.
Steps to Upgrade to Release 8

5.1.5 Pause Point 2 - Stop Informatica IR (IIR) Servers

Orchestration pauses if you have IIR installed on the Mid tier secondary host and configured in your environment, because you must stop IIR before performing any backups. Refer to the steps in "Informatica Identity Resolution Server Maintenance and Administration: Procedures" in the Oracle Fusion Applications Installation Guide.

If you do not have IIR installed, proceed to Section 5.1.8, "Pause Point 3 - Back Up Oracle Fusion Applications."

5.1.6 Update Status to Success

After you successfully stop IIR servers, update the task status to "success" by running the following command:

(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_name -release REL8 -phase DowntimePreFA -taskid StopIIRPausePointPlugin -taskstatus success

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_name -release REL8 -phase DowntimePreFA -taskid StopIIRPausePointPlugin -taskstatus success

5.1.7 Resume Upgrade Orchestrator

Resume orchestration on the MIDTIER host using the command in Section 5.1.1, "Run Upgrade Orchestrator During Downtime", Step 4.

5.1.8 Pause Point 3 - Back Up Oracle Fusion Applications

Orchestration pauses so that you can back up the Oracle Fusion Applications environment. Perform the steps in Section 5.2.2, "Back Up Oracle Fusion Applications".

5.1.9 Update Status to Success

---

**Note:** Ensure that you have backed up your Oracle Fusion Applications database and Oracle Identity Management database, as specified in Section 5.2.2, "Back Up Oracle Fusion Applications", before you run the commands in this section.

---

After you successfully perform the backups, update the task status to "success" on all hosts by running the following commands.

1. Update the task status on the Primordial host.

(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname host_name -release REL8 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin -taskstatus success

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname host_name -release REL8 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin -taskstatus success

2. Update the task status on each Mid tier host that is listed in the HOSTNAME_MIDTIER property in the pod.properties file.
   (Unix)
   cd ORCH_LOCATION/bin
   ./orchestration.sh updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_name -release REL8 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin -taskstatus success
   (Windows)
   cd ORCH_LOCATION\bin
   orchestration.cmd updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_name -release REL8 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin -taskstatus success

3. Update the task status on each OHS host that is listed in the HOSTNAME_OHS property in the pod.properties file.
   (Unix)
   cd ORCH_LOCATION/bin
   ./orchestration.sh updateStatus -pod POD_NAME -hosttype OHS -hostname host_name -release REL8 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin -taskstatus success
   (Windows)
   cd ORCH_LOCATION\bin
   orchestration.cmd updateStatus -pod POD_NAME -hosttype OHS -hostname host_name -release REL8 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin -taskstatus success

4. Update the task status on each IDM host that is listed in following properties in the pod.properties file:
   - HOSTNAME_IDM_OID
   - HOSTNAME_IDM_OIDM
   - HOSTNAME_IDM_OHS
   (Unix)
   cd ORCH_LOCATION/bin
   ./orchestration.sh updateStatus -pod POD_NAME -hosttype IDM -hostname host_name -release REL8 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin -taskstatus success
   (Windows)
   cd ORCH_LOCATION\bin
   orchestration.cmd updateStatus -pod POD_NAME -hosttype IDM -hostname host_name -release REL8 -phase DowntimePreFA -taskid BackupOracleFAPausePointPlugin -taskstatus success

5.1.10 Resume Upgrade Orchestrator

Resume orchestration on all host types, including the respective scaled out hosts, using the commands in Section 5.1.1, "Run Upgrade Orchestrator During Downtime", Steps 1 through 4.
5.1.11 Pause Point 4 - Upgrade Oracle Identity Management to Release 8

Refer to the section for upgrading Oracle Identity Management (IDM) that is appropriate for your environment.

- Release 7 IDM Provisioned, SINGLE, 3-NODE, or 4-NODE, Linux Platform
- Release 7 IDM Provisioned, SINGLE, 3-NODE, or 4-NODE, AIX or Solaris Platform
- Other Configurations

5.1.11.1 Release 7 IDM Provisioned, SINGLE, 3-NODE, or 4-NODE, Linux Platform

If your environment is a SINGLE, 3-NODE, or 4-NODE IDM configuration and is running on Linux and a Release 7 IDM provisioned environment, Upgrade Orchestration performs the IDM upgrade by running the tasks listed in the following table. This pause point does not occur and you can proceed to Section 5.1.14, "Pause Point 5 - Start External Servers."

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Task ID</th>
<th>Host Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade Oracle Identity Management - OID</td>
<td>OIDApplyPatches</td>
<td>IDM</td>
</tr>
<tr>
<td>Upgrade Oracle Identity Management - OIM</td>
<td>OIMApplyPatches</td>
<td>IDM</td>
</tr>
<tr>
<td>Upgrade Oracle Identity Management - AUTHOHS</td>
<td>OHSApplyPatches</td>
<td>IDM</td>
</tr>
<tr>
<td>Validate Oracle Identity Management Setup &amp; Configuration</td>
<td>IDMPostValidate</td>
<td>IDM</td>
</tr>
</tbody>
</table>

5.1.11.2 Release 7 IDM Provisioned, SINGLE, 3-NODE, or 4-NODE, AIX or Solaris Platform

If your environment is a SINGLE, 3-NODE, or 4-NODE IDM configuration and is running on AIX or Solaris and a Release 7 IDM provisioned environment, you upgrade IDM by following the steps for running idmUpgrade.pl in Section 5.2.4, "Run idmUpgrade.pl to Upgrade Oracle Identity Management".

5.1.11.3 Other Configurations

If your environment does not meet the criteria in either Section 5.1.11.1 or Section 5.1.11.2, orchestration pauses so that you can perform the IDM upgrade by following the steps in Section 5.2.5, "Upgrade the Oracle Identity Management Domain to 11g Release 8 (11.1.8)".

5.1.12 Update Status to Success

After you successfully upgrade Oracle Identity Management, update the task status to "success" on the IDM host. Note that this section is not applicable if you upgrade IDM based on the information in Section 5.1.11.1, "Release 7 IDM Provisioned, SINGLE, 3-NODE, or 4-NODE, Linux Platform".

(UNIX)

cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hostype IDM -hostname host_name -release REL8 -phase DowntimePreFA -taskid UpgradeIDMPausePointPlugin -taskstatus
success

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype IDM -hostname host_name
-hosttype IDM -hostname host_name
-release REL8 -phase DowntimePreFA -taskid UpgradeIDMPausePointPlugin -taskstatus
success

5.1.13 Resume Upgrade Orchestrator

Resume orchestration on each IDM host that is listed in the following properties in the
pod.properties file, using the command in Section 5.1.1, "Run Upgrade Orchestrator
During Downtime", Step 4:

- HOSTNAME_IDMOID
- HOSTNAME_IDMOIM
- HOSTNAME_IDMOHS

Upgrade Orchestrator runs the tasks in the following table.

Table 5–4  Tasks Run During the DowntimePreFA Phase

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Task ID</th>
<th>Host Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Upgrade Readiness (During Downtime) Checks</td>
<td>DuringDowntimeChecks</td>
<td>Primordial, OHS, Mid tier</td>
</tr>
<tr>
<td>Remove Conflicting Patches for Oracle Fusion Middleware Component Oracle Homes</td>
<td>RemoveConflictingPatches</td>
<td>Primordial</td>
</tr>
<tr>
<td>Upgrade JDK</td>
<td>UpgradeJDK</td>
<td>Primordial</td>
</tr>
<tr>
<td>Install Oracle Fusion Applications LCM Tools for Oracle VM</td>
<td>InstallFaSaasLcmTools</td>
<td>Primordial, OHS, IDM</td>
</tr>
<tr>
<td>Prepare for Oracle Fusion Applications LCM Tools for Oracle VM Upgrade</td>
<td>PrepareLCMToolsForOVMUpgrade</td>
<td>Primordial</td>
</tr>
<tr>
<td>Apply Oracle Fusion Applications LCM Tools for Oracle VM Patches</td>
<td>ApplyLCMToolsForOVMPatches</td>
<td>Primordial, OHS, IDM</td>
</tr>
<tr>
<td>Run RUP Lite for OVM in Offline Mode as Application User</td>
<td>RupLiteOvmOffline</td>
<td>Primordial, OHS, Mid tier, IDM</td>
</tr>
<tr>
<td>Run Oracle Fusion Applications RUP Installation Part 1 of 2</td>
<td>RunFirstRUPInstaller</td>
<td>Primordial</td>
</tr>
<tr>
<td>Run RUP Lite for Domain Configuration</td>
<td>RunRUPLiteForDomainsConfig</td>
<td>Mid tier</td>
</tr>
<tr>
<td>Start Node Managers</td>
<td>StartNodeManager</td>
<td>Primordial, Mid tier</td>
</tr>
<tr>
<td>Start OPMN Control Processes</td>
<td>StartOPMNProcesses</td>
<td>Primordial, OHS, Mid tier,</td>
</tr>
<tr>
<td>Run Oracle Fusion Applications RUP Installation Part 2 of 2</td>
<td>RunSecondRUPInstaller</td>
<td>Primordial</td>
</tr>
<tr>
<td>DowntimePostFA Phase</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Run Vital Signs Checks</td>
<td>VitalSignsChecks</td>
<td>Primordial</td>
</tr>
<tr>
<td>Invoke an Instance of UpdateSOAMDS SOA Composite</td>
<td>UpdateMDSSOACComposite</td>
<td>Primordial</td>
</tr>
</tbody>
</table>
5.1.14 Pause Point 5 - Start External Servers

Orchestration pauses on the Mid tier host so you can start the GOP server and IIR instance.

Perform the steps in Section 5.2.6, "Start External Servers".

5.1.15 Update Status to Success

After the GOP server and IIR instance start, set the task status to "success" on the Mid tier host.

(Unix)
```
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_name -release REL8 -phase DowntimePostFA -taskid StartExternalServersPausePointPlugin -taskstatus success
```

(Windows)
```
cd ORCH_LOCATION\bin
\ orchestration.cmd updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_name -release REL8 -phase DowntimePostFA -taskid StartExternalServersPausePointPlugin -taskstatus success
```

5.1.16 Resume Upgrade Orchestrator

Resume orchestration on the Mid tier host using the command in Section 5.1.1, "Run Upgrade Orchestrator During Downtime", Step 2.

Upgrade Orchestrator runs the tasks in the following table.

<table>
<thead>
<tr>
<th>Table 5–5 Tasks Run During the DowntimePostFA Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task Name</td>
</tr>
<tr>
<td>Set CrashRecoveryEnabled Property to True</td>
</tr>
</tbody>
</table>
5.1.17 Pause Point 6 - Back Up Oracle Fusion Applications Before Language Pack Upgrade (Language Pack Only)

If only the US English language is installed on your environment, proceed to Section 5.1.20, "Upgrade Orchestrator Completes Successfully".

If you have set the `SKIP_UPGRADE_FOR_LANGUAGE` option to skip languages, the upgrade for those languages will not be performed as part of orchestration. In this case, you must manually upgrade your installed languages after Upgrade Orchestrator completes successfully and proceed to Section 5.1.20, "Upgrade Orchestrator Completes Successfully" at this time. For more information, see "Installing and Maintaining Oracle Fusion Applications Languages" in the Oracle Fusion Applications Administrator’s Guide.

If you have languages other than US English installed on your Oracle Fusion Applications environment, Upgrade Orchestrator pauses so you can back up your Oracle Fusion Applications environment before your languages are upgraded. Perform the steps in Section 5.2.2, "Back Up Oracle Fusion Applications".

5.1.18 Update Status to Success

After you successfully back up the Oracle Fusion Applications environment, update the task status to "success" on all hosts:

1. Update the task status on the primordial host:
   
   (Unix)
   ```bash
   cd ORCH_LOCATION/bin
   ./orchestration.sh updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname host_name -release REL8 -phase DowntimePostFA -taskid BackupOracleFAPausePointPlugin -taskstatus success
   ```

   (Windows)
   ```cmd
   cd ORCH_LOCATION\bin
   orchestration.cmd updateStatus -pod POD_NAME -hosttype PRIMORDIAL -hostname host_name -release REL8 -phase DowntimePostFA -taskid BackupOracleFAPausePointPlugin -taskstatus success
   ```

2. Update the task status on each Mid tier host that is listed in the `HOSTNAME_MIDTIER` property in the `pod.properties` file:
   
   (Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_name -release REL8 -phase DowntimePostFA -taskid BackupOracleFAPausePointPlugin -taskstatus success

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype MIDTIER -hostname host_name -release REL8 -phase DowntimePostFA -taskid BackupOracleFAPausePointPlugin -taskstatus success

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

(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype OHS -hostname host_name -release REL8 -phase DowntimePostFA -taskid BackupOracleFAPausePointPlugin -taskstatus success

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype OHS -hostname host_name -release REL8 -phase DowntimePostFA -taskid BackupOracleFAPausePointPlugin -taskstatus success

4. Update the task status on each IDM host that is listed in following properties in the pod.properties file:
   - HOSTNAME_IDMOID
   - HOSTNAME_IDMOIM
   - HOSTNAME_IDMOHS

(Unix)
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype IDM -hostname host_name -release REL8 -phase DowntimePostFA -taskid BackupOracleFAPausePointPlugin -taskstatus success

(Windows)
cd ORCH_LOCATION\bin
orchestration.cmd updateStatus -pod POD_NAME -hosttype IDM -hostname host_name -release REL8 -phase DowntimePostFA -taskid BackupOracleFAPausePointPlugin -taskstatus success

5.1.19 Resume Upgrade Orchestrator (Language Pack Only)

Resume orchestration on all host types, including the respective scaled out hosts, using the commands in Section 5.1.1, "Run Upgrade Orchestrator During Downtime", Steps 1 through 4.

Upgrade Orchestrator runs the tasks in the following table. Note that the LanguagePackInstall task runs both the General System and pre-language pack readiness Health Checks and it runs for each installed language. The PostLangPackChecks task runs both the General System and post-language pack Health Checks.
### Table 5–6  Tasks Run For the Language Pack Upgrade

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Task ID</th>
<th>Host Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade All Installed Languages</td>
<td>LanguagePackInstall</td>
<td>Primordial</td>
</tr>
<tr>
<td>Stop All Servers</td>
<td>StopServersAfterLP</td>
<td>Primordial</td>
</tr>
<tr>
<td>Start All Servers</td>
<td>StartServersAfterLP</td>
<td>Primordial</td>
</tr>
<tr>
<td>Run Post Language Pack Health Checks</td>
<td>PostLangPackChecks</td>
<td>Primordial</td>
</tr>
</tbody>
</table>

---

#### 5.1.20 Upgrade Orchestrator Completes Successfully

Upgrade Orchestrator generates the Oracle Fusion Applications Orchestrator Upgrade Report upon successful completion of the upgrade, which you review as a post-upgrade task. To continue with the upgrade after all tasks complete successfully, proceed to Chapter 6, "Running Post-Upgrade Tasks for Oracle Fusion Applications".

#### 5.2 Pause Point Steps

This section describes the detailed steps required by each of the following default pause points:

- Back Up the OPSS Security Store
- Back Up Oracle Fusion Applications
- Back Up Oracle Fusion Applications on Windows
- Upgrade the Oracle Identity Management Domain to 11g Release 8 (11.1.8)
- Start External Servers

##### 5.2.1 Back Up the OPSS Security Store

The upgrade process upgrades all WLS domains to the 11gR1 PS5 MLR1 (11.1.1.6.1) level, so you must back up the OPSS Security Store and the Bootstrap Wallet, as described in this section. This section also includes information about restoring from a backup. Ensure you perform your backups in directories from which you can restore. You can use any directory to back up the data, as long as you know where to restore the backup from.

##### 5.2.1.1 Back Up Data Under the Root Node of the OPSS Security Store

Perform the following steps to back up all data under the root node of the OPSS Security Store.

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. Note that in the case of an upgrade failure, you must 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

(Windows)
set ORACLE_HOME=OID_ORACLE_HOME
set ORACLE_INSTANCE=OID_INSTANCE_HOME

Example:

(Unix)
setenv ORACLE_HOME /u01/oid/oid_home
setenv ORACLE_INSTANCE /u01/oid/oid_inst

(Windows)
set ORACLE_HOME=\u01\oid\oid_home
set ORACLE_INSTANCE=\u01\oid\oid_inst

b. Create the backup. The backup is created in the \$SHARED_UPGRADE_LOCATION/POD_NAME/release/ directory.

In the system where the Oracle Internet Directory is located, produce an LDIF file by running ldifwrite as illustrated in the following command. Note that you are prompted for the Operational Data Store (ODS) password.

OID_HOME/ldap/bin/ldifwrite connect="srcOidDbConnectStr" basedn="cn=FAPolicies", "c=us" ldiffile="srcOid.ldif"

Example:

/u01/oid/oid_home/ldif/bin/ldifwrite connect="oidddb" basedn="cn=FAPolicies" ldiffile="srcOid.ldif"

This command writes all entries under the node cn=FAPolicies to the file srcOid.ldif. After generated, move this file to the directory that was previously identified, to hold all backup data.

c. Perform the following steps if you need to restore the backup.

- Ensure Oracle Internet Directory is up and running.
- Perform a bulkdelete on Oracle Internet Directory nodes.
- In the Oracle Internet Directory system, verify that there are no schema errors or bad entries by running bulkload, as illustrated in the following command:

OID_HOME/ldap/bin/bulkload connect="dstOidDbConnectStr" check=true generate=true restore=true file="fullPath2SrcOidLdif"

If duplicate DNs (common entries between the source and destination directories) are detected, review them to prevent unexpected results.
- Load data into the Oracle Internet Directory by running bulkload as illustrated in the following command:

OID_HOME/ldap/bin/bulkload connect="dstOidDbConnectStr" load=true file="fullPath2SrcOidLdif"
5.2.1.2 Back Up the Bootstrap Wallet

Back up the cwallet.sso file in the DOMAIN_HOME/config/fmwconfig/bootstrap directory for each WLS domain in an Oracle Fusion Applications installation. You must take backups of each cwallet.sso file for each domain and when you restore, you must be careful to restore the correct file. For example, if you back up cwallet.sso from the Common Domain, then you must restore it in the Common Domain upon failure. If you back up cwallet.sso from the BI domain, you must restore it to the BI Domain upon failure.

Proceed to Section 5.1.3, "Update Status to Success" to continue the upgrade.

Related Links

The following documents provide additional information related to subjects discussed in this section:

- For more information about identifying the root node in the Oracle Internet Directory hosting the OPSS Security store using Fusion Applications Control, see "Reassociating with Fusion Middleware Control" in the Oracle Fusion Middleware Application Security Guide.

- For more information about the bulkload command, see "Performing Bulk Operations" in the Oracle Fusion Middleware Administrator’s Guide for Oracle Internet Directory.

- For more information about migrating Oracle Internet Directory, see "Migrating Large Volume Policy and Credential Stores" in the Oracle Fusion Middleware Application Security Guide.

5.2.2 Back Up Oracle Fusion Applications

Back up your entire Oracle Fusion Applications environment by following the steps for performing a full offline backup in "Backing Up and Recovering Oracle Fusion Applications" in the Oracle Fusion Applications Administrator’s Guide. Include the following components in your backup:

- Back Up Your Database
- Back Up Upgrade Orchestrator Directories
- Back Up OHS Host and /etc/hosts
- Back Up the Central Inventory

For additional back up steps that are specific to Windows, refer to Section 5.2.3, "Back Up Oracle Fusion Applications on Windows".

5.2.2.1 Back Up Your Database

Database upgrade and patching is a prerequisite to the Oracle Fusion Applications Upgrade. You must backup your Oracle Fusion Applications database and Oracle Identity Management database before and after applying all prerequisite patches and before starting the Oracle Fusion Applications upgrade. For more information, see "Backing Up and Recovering Oracle Fusion Applications" in the Oracle Fusion Applications Administrator’s Guide. Turn on Oracle Flashback Database as a best practice before taking a backup of the Oracle Fusion Applications database.
5.2.2.2 Back Up Upgrade Orchestrator Directories
Upgrade Orchestrator writes to work areas specified by properties in the pod.properties file. Ensure that you back up the work directories during all Oracle Fusion Applications backup pause points. During any restore of your environment, you must restore the orchestration work directories to the same backup point.

Backup directories are specified by the following properties in the pod.properties file:

- ORCHESTRATION_CHECKPOINT_LOCATION
- ORCHESTRATION_CHECKPOINT_ARCHIVE_LOCATION
- SHARED_UPGRADE_LOCATION

If these directories are shared among multiple environments then the backups of these directories must be specific to the environment (POD_NAME). The restore should also be specific to that environment (POD_NAME), as shown in the following examples:

- ORCHESTRATION_CHECKPOINT_LOCATION/POD_NAME
- ORCHESTRATION_CHECKPOINT_ARCHIVE_LOCATION/ARCHIVE/POD_NAME
- SHARED_UPGRADE_LOCATION/POD_NAME

**Note:** When restoring the Oracle Fusion Applications environment from a backup, you must restore the orchestration directories if you want to continue using orchestration from the backup pause points in the orchestration flow.

5.2.2.3 Back Up OHS Host and /etc/hosts
On the OHS host, back up /u01/APPLTOP and /u02/instance.
Also back up the /etc/hosts file.

5.2.2.4 Back Up the Central Inventory
Upgrade Orchestrator upgrades and applies Oracle Fusion Middleware and Oracle Fusion Application patches to your Oracle Fusion Applications environment. As a best practice, back up your central inventory along with other Oracle homes before the upgrade. On the primordial host, the location of the central inventory can be obtained by looking at the inventory pointer file (oraInst.loc on Linux), located in FA_ORACLE_HOME.

After your backups are complete, and if you are performing the steps to upgrade to Release 8, proceed to Section 5.1.9, "Update Status to Success" to continue the upgrade.

If you are performing the steps to upgrade your installed languages, proceed to Section 5.1.18, "Update Status to Success."

5.2.3 Back Up Oracle Fusion Applications on Windows
Back up the Oracle Fusion Applications environment, including APPLICATIONS_BASE, inventory, registry entries, Oracle Identity Management, the database and the System environment PATH variable of the Oracle Fusion Applications host machine.

1. APPLICATIONS_BASE contains many files whose path is more than 256 characters. The Microsoft Windows Copy function is limited to copying only those files with a path of less than 256 characters. Therefore, many files fail to copy.
Use Robust File Copy (Robocopy), which is available as part of the Windows Resource Kit, to copy APPLICATIONS_BASE. Use the following command:

```bash
robocopy <source> <destination> /MIR > <file>
```

Sample output from the robocopy command:

<table>
<thead>
<tr>
<th></th>
<th>Total</th>
<th>Copied</th>
<th>Skipped</th>
<th>Mismatch</th>
<th>FAILED</th>
<th>Extras</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dirs:</td>
<td>112640</td>
<td>112640</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Files:</td>
<td>787114</td>
<td>787114</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Bytes:</td>
<td>63,822 g</td>
<td>63,822 g</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Times:</td>
<td>2:22:20</td>
<td>2:19:00</td>
<td>0:00:00</td>
<td>0:03:19</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Back up the inventory.
   Back up the inventory location referenced in the registry HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\inst_loc.

3. Back up the registry.
   Use Regedit.exe to back up the following registries related to Oracle Fusion Applications.
   - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
     - Web Tier service
     - BI Service
     - Node Manager service
   - HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE
   - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Oblix

4. Ensure that the System PATH has the following values:
   ```
   C:\APPLICATIONS_BASE\dbclient\bin
   C:\APPLICATIONS_BASE\webtier_mwhome\webtier\bin
   C:\APPLICATIONS_BASE\webtier_mwhome\webtier\perl\bin
   C:\APPLICATIONS_BASE\webtier_mwhome\webtier\opmn\lib
   C:\APPLICATIONS_BASE\fusionapps\bi\products\Essbase\EssbaseServer\bin
   C:\APPLICATIONS_BASE\fusionapps\bi\bin
   C:\<APPLICATIONS_BASE>\fusionapps\bi\opmn\bin
   C:\<APPLICATIONS_BASE>\fusionapps\bi\perl\bin
   ```
   Add any of the previous values that are missing to the system PATH. Missing values cause failures in launching the OPMN services and BI Presentation Catalog deployment configuration assistants in RUP Installer.

5. Save the system PATH variable.
   Proceed to Section 5.1.9, "Update Status to Success" to continue the upgrade.

### 5.2.4 Run idmUpgrade.pl to Upgrade Oracle Identity Management

Perform the following steps to run idmUpgrade.pl. The idmUpgrade.pl script requires the 64-bit perl version 5.10.0. Use the 64-bit perl from OHS_ORACLE_HOME or OID_ORACLE_HOME.
1. Perform the steps to set the environment variables on each node, as required for your platform. For more information, see Section 4.2.2, "Set Environment Variables."

2. Stop the servers and processes on each of the following nodes by executing `IDM_TOP/config/scripts/stopall.sh` in the following order:
   - AuthOHS Node
   - OIM Node
   - OID Node

3. Run `idmUpgrade.pl` on each node as follows:
   - On the OID node:
     ```
     cd SHARED_LOCATION/11.1.8.0.0/idmUpgrade
     perl idmUpgrade.pl OID REPOSITORY_LOCATION/installer,SHARED_LOCATION/11.1.8.0.0_post_repo_patches patchAutomation.properties
     ```
   - On the OIM node:
     ```
     cd SHARED_LOCATION/11.1.8.0.0/idmUpgrade
     perl idmUpgrade.pl OIM REPOSITORY_LOCATION/installer,SHARED_LOCATION/11.1.8.0.0_post_repo_patches patchAutomation.properties
     ```
   - On the AuthOHS node:
     ```
     cd SHARED_LOCATION/11.1.8.0.0/idmUpgrade
     perl idmUpgrade.pl OHS REPOSITORY_LOCATION/installer,SHARED_LOCATION/11.1.8.0.0_post_repo_patches patchAutomation.properties
     ```

4. After you complete the IDM upgrade, proceed to Section 5.1.12, "Update Status to Success" to continue the upgrade.

### 5.2.5 Upgrade the Oracle Identity Management Domain to 11g Release 8 (11.1.8)

Before performing an upgrade to 11g Release 8 (11.1.8), check the Technical Release Notes for Oracle Fusion Applications 11g Release 8 (11.1.8) for the latest information on required patches.

Perform the following steps to upgrade the Oracle Identity Management domain to 11g Release 8 (11.1.8):

#### 5.2.5.1 Overview
Oracle Identity Management for Oracle Fusion Applications 11g, Release 8 (11.1.8.0) includes patches for the following products that are installed in the Oracle Identity Management domain:
   - Oracle Identity Manager
   - Oracle IDM Tools
   - Oracle Access Manager
   - Oracle WebGate
   - Oracle Internet Directory
The Oracle Fusion Applications Release 8 Identity Management software and patches for your appropriate platform are available in the Oracle Fusion Applications repository under shared_location/11.1.8.0.0/Repository/installers. Review the individual patch Readme files before applying them.

5.2.5.2 About Identity Management Domain, Nodes and Oracle homes
This section explains the various nodes and Oracle homes in the Identity Management domain for Oracle Fusion Applications 11g, Release 8 (11.1.8.0.0).

- **Identity Management (IDM) Node**
  - WEBLOGIC_ORACLE_HOME
    - Oracle WebLogic Server
  - IDM_ORACLE_HOME: This is also known as the OID_ORACLE_HOME. The following Oracle Identity Management products are installed in this Oracle home:
    - Oracle Internet Directory
    - Oracle Virtual Directory
    - Oracle Directory Services Manager
  - IDM_ORACLE_COMMON_HOME: The following Oracle Identity Management products are installed in this Oracle home:
    - Oracle Platform Security Services (OPSS)
    - Oracle Web Services Manager (OWSM)

- **Identity and Access Management (IAM) Node**
  - WEBLOGIC_ORACLE_HOME
    - Oracle WebLogic Server
  - IAM_ORACLE_HOME: This is also known as the OIM_ORACLE_HOME. The following Oracle Identity Management products are installed in this Oracle home:
    - Oracle Identity Manager
    - Oracle Access Manager
    - Oracle IDM Tools
    - Oracle Identity Federation
  - SOA_ORACLE_HOME: This is typically installed under the IAM_ORACLE_HOME. The following products are installed in this Oracle home:
    - Oracle SOA Suite
  - IAM_ORACLE_COMMON_HOME: The following Oracle Identity Management products are installed in this Oracle home:
    - OPSS
    - OWSM

- **OHS Node**
  - OHS_ORACLE_HOME: This is also known as the WEB_ORACLE_HOME. The following Oracle Identity Management products are installed in this Oracle home:
    - Oracle WebGate
5.2.5.3 Performing Pre-installation Tasks

Perform the following tasks before installation.

5.2.5.3.1 Verifying Prerequisites

Ensure that your environment meets the following requirements before you install or uninstall the patch:

- Review and download the latest version of OPatch 11.1.x via Patch 6880880 (OPatch version 11.1.0.8.2 or later).
  - Oracle recommends that you use the latest version of OPatch. Review the My Oracle Support note 224346.1-Opatch-Where Can I Find the Latest Version of Opatch?
- Verify the OUI Inventory
  OPatch needs access to a valid OUI inventory to apply patches. Validate the OUI inventory with the following command:
  
  opatch lsinventory

  If the command errors out, contact Oracle Support for assistance in validating and verifying the inventory setup before proceeding.
- Confirm the executables appear in your system PATH.
  The patching process uses the unzip and the OPatch executables. After setting the ORACLE_HOME environment, confirm whether the following executables exist, before proceeding to the next step.
  - which opatch
  - which unzip

5.2.5.3.2 Stop the Servers and Processes

Stop the servers and processes, as follows:

- In the Oracle Identity Management domain, stop all Oracle Identity Management services and processes using the following sequence. Do not stop the database.

  Note: Refer to Appendix C, “Stopping and Starting Identity Management Related Servers” for specific commands for stopping components.

Stop the following servers and processes:

- Oracle HTTP Server
- Oracle Identity Manager managed servers
Pause Point Steps

- 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

5.2.5.3.3 Create Backups

At a minimum, create the following backups:

- Middleware home directory (including the Oracle home directories inside the Middleware home)
- Local domain home directory
- Local Oracle instances
- Domain home and Oracle instances on any remote systems that use the Middleware home
- Back up your database and ensure the backup includes the schema version registry table, as each Fusion Middleware schema has a row in this table. The name of the schema version registry table is `SYSTEM.SCHEMA_VERSION_REGISTRY$`.
- Back up your Configurations and Stores—specifically, all data under the root node of the LDAP store.
- Back up any Oracle Identity Federation Java Server Pages (JSP) that you customized.

**Note:** The patching process overwrites JSPs included in the `oif.ear` file. After you complete the patching process, restore your custom JSPs.

In addition to the preceding backups, Oracle recommends performing your organization’s typical backup processes.

5.2.5.3.4 Patch the Database (RDBMS_ORACLE_HOME)

Ensure the patches listed in Chapter 3, "Updating the Oracle Fusion Applications and Oracle Identity Management Databases" are applied on the Identity Management database to keep both Oracle Fusion Applications and Identity Management databases synchronized. Follow the steps in Chapter 3 to apply the patches.

5.2.5.3.5 Patch the Database Clients

The Database Client patches are available under the `SHARED_LOCATION/11.1.8.0.0/Repository/installers/dbclient/patch` directory. Follow the `Readme` and apply all patches in the directory. Proceed as follows to apply all patches:

- Set your Oracle home to RDBMS_ORACLE_HOME, for example:

  cd `SHARED_LOCATION/11.1.8.0.0/Repository/installers/dbclient/patch`
setenv ORACLE_HOME/u01/oid/oid_home

- Run opatch using the napply option.

5.2.5.3.6 Patch the WebLogic Server on the IDM Node

Oracle Fusion Applications 11g Release 8 (11.1.8) Identity Management continues to use Oracle WebLogic Server 10.3.6. However, there may be additional Oracle WebLogic Server patches that you must apply.

The WebLogic server patches are available under the `{SHARED_LOCATION}11.1.8.0.0/Repository/installers/smart_update/weblogic` directory. Follow the patch Readme and apply all patches in the directory. Use the following commands to apply all the patches on the IDM NODE:

cd `{SHARED_LOCATION}11.1.8.0.0/Repository/installers/smart_update/weblogic`

ls *.jar

Take the list of jars from the output of the ls command and create a comma separated list without the file extension, for example:

setenv WLS_PATCH_LIST '1IHE,1PI6,BEJG,CM68,...'

chmod a+w /u01/oid/utils/bsu/cache_dir/patch-catalog.xml
java -jar {SHARED_LOCATION}11.1.8.0.0/Repository/installers/smart_update/weblogic/update/bsu-wrapper.jar
  -bsu_home=/u01/oid/utils/bsu/
  -install -patchlist=$WLS_PATCH_LIST
  -prod_dir=/u01/oid/wlserver_10.3/
  -patch_download_dir={SHARED_LOCATION}11.1.8.0.0/Repository/installers/smart_update/weblogic/
  -meta={SHARED_LOCATION}11.1.8.0.0/Repository/installers/smart_update/suwrapper/suw_metadata.txt

5.2.5.3.7 Patch the WebLogic Server on the IAM Node

Oracle Fusion Applications 11g Release 8 (11.1.8) Identity and Access Management continues to use Oracle WebLogic Server 10.3.6. However, there may be additional Oracle WebLogic Server patches that you must apply.

Use the following commands:

cd `{SHARED_LOCATION}11.1.8.0.0/Repository/installers/smart_update/weblogic`

ls *.jar

Take the list of jars from the output of "ls" and create a comma separated list without the file extension, for example:

setenv WLS_PATCH_LIST '1IHE,1PI6,BEJG,CM69,...'

chmod a+w /u01/oim/utils/bsu/cache_dir/patch-catalog.xml
java -jar {SHARED_LOCATION}11.1.8.0.0/Repository/installers/smart_update/weblogic/update/bsu-wrapper.jar
  -bsu_home=/u01/oim/utils/bsu/
  -install -patchlist=$WLS_PATCH_LIST
  -prod_dir=/u01/oim/wls_server_10.3/
  -patch_download_dir={SHARED_LOCATION}11.1.8.0.0/Repository/installers/smart_update/weblogic/
  -meta={SHARED_LOCATION}11.1.8.0.0/Repository/installers/smart_update/suwrapper/suw_metadata.txt
5.2.5.3.8 Patch IDM_ORACLE_HOME

The patches for this Oracle home are available under the `SHARED_LOCATION/11.1.8.0.0/Repository/installers/pltsec/patch` directory for your appropriate platform. Follow the patch Readme and apply all patches in the directory as follows:

1. Set your Oracle home to `IDM_ORACLE_HOME`, for example:
   ```bash
cd SHARED_LOCATION/11.1.8.0.0/Repository/installers/pltsec/patch
setenv ORACLE_HOME /u01/oid/oid_home
```

2. Run `opatch` using the `napply` option.

5.2.5.3.9 Patch the Common Oracle homes on All Nodes

Your deployment should have at least the following, if not more, Oracle Common homes:

- `IDM_ORACLE_COMMON_HOME`
- `IAM_ORACLE_COMMON_HOME`
- `OHS_ORACLE_COMMON_HOME`

The patches for these Oracle homes are available under the `SHARED_LOCATION/11.1.8.0.0/Repository/installers/oracle_common/patch` directory for your platform. Follow the patch Readme and apply all patches in the directory to the Oracle Common homes as follows:

1. Set your Oracle home to `IDM_ORACLE_COMMON_HOME`, for example:
   ```bash
cd SHARED_LOCATION/11.1.8.0.0/Repository/installers/oracle_common/patch
setenv ORACLE_HOME /u01/oid/oracle_common
```

2. Run `opatch` using the `napply` option.

3. Set your Oracle home to `ORACLE_COMMON_HOME`, for example:
   ```bash
setenv ORACLE_HOME /u01/oim/oracle_common
```

4. Run `opatch` using the `napply` option.

5. Set your Oracle home to `OHS_ORACLE_COMMON_HOME`, for example:
   ```bash
setenv ORACLE_HOME /u01/ohsauth/oracle_common
```

6. Run `opatch` using the `napply` option.

---

**Note:** You must apply all the patches to all the Common Oracle homes.

---

5.2.5.3.10 Patch IAM_ORACLE_HOME on the IAM Node

The patches for this Oracle home are available under the `SHARED_LOCATION/11.1.8.0.0/Repository/installers/idm/patch` directory for your platform. Follow the patch Readme and apply all patches in the directory as follows:

1. Set your Oracle home to `IAM_ORACLE_HOME`, for example:
   ```bash
cd SHARED_LOCATION/11.1.8.0.0/Repository/installers/idm/patch
setenv ORACLE_HOME /u01/oim/oim_home
```
2. Run opatch using the napply option.

---

**Note:** Some of the patches have post-patch steps mentioned in the README of the patch. Only apply the patches using opatch napply now, as you will run the post-patch steps later.

### 5.2.5.3.11 Patch OIF_ORACLE_HOME on the IAM Node

The patches for this Oracle home are available under the `SHARED_LOCATION/11.1.8.0.0/Repository/installers/oif/patch` directory for your platform. Follow the patch Readme and apply all patches in the directory as follows:

1. Set your Oracle home to `OIF_ORACLE_HOME`, for example:
   ```
   cd SHARED_LOCATION/11.1.8.0.0/Repository/installers/idm/patch
   setenv ORACLE_HOME /u01/oim/fmw_idm_home
   ```

2. Run opatch using the napply option.

### 5.2.5.3.12 Patch SOA_ORACLE_HOME on the IAM Node

The patches for this Oracle home are available under the `SHARED_LOCATION/11.1.8.0.0/Repository/installers/soa/patch` directory for your platform. Follow the patch Readme and apply all patches in the directory as follows:

1. Set your Oracle home to `SOA_ORACLE_HOME`, for example:
   ```
   cd SHARED_LOCATION/11.1.8.0.0/Repository/installers/soa/patch
   setenv ORACLE_HOME /u01/oim/soa_home
   ```

2. Run opatch using the napply option.

### 5.2.5.3.13 Patch OHS_ORACLE_HOME on the OHS Node

The patches for this Oracle home are available under the `SHARED_LOCATION/11.1.8.0.0/Repository/installers/webtier/patch` directory for your platform. Follow the patch Readme and apply all patches in the directory as follows:

1. Set your Oracle home to `OHS_ORACLE_HOME`, for example:
   ```
   cd SHARED_LOCATION/11.1.8.0.0/Repository/installers/webtier/patch
   setenv ORACLE_HOME /u01/ohsauth/ohsauth_home
   ```

2. Run opatch using the napply option.

### 5.2.5.3.14 Patch WEBGATE_ORACLE_HOME on the OHS Node

The patches for this Oracle home are available under the `SHARED_LOCATION/11.1.8.0.0/Repository/installers/webgate/patch` directory for your platform. Follow the patch Readme and apply all patches in the directory as follows:

1. Set your Oracle home to `WEBGATE_ORACLE_HOME`, for example:
   ```
   cd SHARED_LOCATION/11.1.8.0.0/Repository/11.1.8.0.0/Repository/installers/webgate/patch
   setenv ORACLE_HOME /u01/ohsauth/webgate
   ```

2. Run opatch using the napply option.
5.2.5.4 Post-Patch Procedures

Note: Some patches have online post-patch steps that must be completed. These are documented in the individual patch readme. Review and follow the post-patch steps.

Perform the procedures in the following sections:

5.2.5.4.1 Start the Servers and Apply Post-Patch Steps

Note: For information about starting the components, see Appendix C, "Stopping and Starting Identity Management Related Servers."

Start servers and processes in the following sequence:

1. Oracle Internet Directory (if not already started)
2. Oracle Virtual Directory
3. Oracle WebLogic Administration Server for the IDM node (if not already started)
4. Oracle Directory Services Manager (ODSM) managed servers
5. Oracle Access Manager managed servers (if not already started)
6. Oracle Identity Federation managed servers
7. Oracle SOA managed servers (if not already started)
8. Oracle Identity Manager managed servers (if not already started)
9. Oracle HTTP Server and Webgate (if not already started)

5.2.5.4.2 Verify the Oracle Identity Management Domain

To verify that the upgrades and patches to the Oracle Identity Management domain were applied correctly, perform the following steps:

- Confirm you can access and log in to the Oracle WebLogic Administration Server console at:
  
  - http://HOST:ADMIN_SERVER_PORT/console
  - https://HOST:SECURE_ADMIN_SERVER_PORT/console

- Confirm you can access and log in to Oracle Enterprise Manager Fusion Middleware Control at:
  
  http://HOST:ADMIN_SERVER_PORT/em

After you complete the IDM upgrade, proceed to Section 5.1.12, "Update Status to Success" to continue the upgrade.

5.2.6 Start External Servers

Perform the following steps:

- Start GOP Processes
- Start the Informatica IR (IIR) Instance
5.2.6.1 Start GOP Processes

Perform the following steps to start the GOP processes. Note that the opmnctl process for gop_1 should be started only on the host machine which contains the AdvancedPlanning Managed Server. Do not start it on the primordial host.

1. Proceed to Step 2 if your GOP processes have been previously configured and have run before.

   If you are starting GOP processes for the first time, confirm that a datasource exists, in the form of XML files, under the APPLICATIONS_BASE/instance/gop_1/GOP/GlobalOrderPromisingServer1/datastore directory. Then run the RefreshOpDatastore ESS job by performing the following steps:
   
   a. Ensure that the AdvancePlanning Managed Server is running in the SCM domain.
   
   b. Invoke http://scm - AdvancePlanning managedserver:port/advancedPlanning/faces/MscCentralEssUi
   
   c. In the bottom list applet click on Actions, then Schedule New Process.
   
   d. Select Search under Name, and query for %Order%.
   
   e. Select Refresh Order Promising Data and click OK.
   
   f. Select all check boxes in the Process Details popup.
   
   g. You can customize some options in the Advanced pane, but this is not mandatory.
   
   h. Click Submit and note the process ID.
   
   i. After you confirm that the process is complete, you should see information from the log file that is similar to the following example:

      Running RefreshOpDatastore Job...
      Got service proxy successfully.
      Got callback url successfully.
      Getting the job-parameters in the Map.
      Added job parameters in the map
      Web service successfully invoked
      ***** callback received *****
      Return Status of job is SUCCESS

   j. Proceed to Step 2.

2. Log in to Fusion Applications Control. For more information, see "Accessing Fusion Applications Control" in the Oracle Fusion Applications Administrator’s Guide.

3. Access GOP by navigating to Oracle Fusion Supply Chain Management, then Global Order Promising, then GlobalOrderPromisingServer1.

4. Click GlobalOrderPromisingServer1 to open the GlobalOrderPromisingServer1 page.

5. Select Control from the menu, then Start Up.

5.2.6.2 Start the Informatica IR (IIR) Instance

If you have IIR installed and configured in your environment, you must start IIR before resuming with next steps. For more information, see "Informatica Identity Resolution Server Maintenance and Administration: Procedures" in the Oracle Fusion Applications Installation Guide.
Proceed to Section 5.1.15, "Update Status to Success."

5.3 Set the SKIP_ROOTPRE Environment Variable (AIX Only)

Set the SKIP_ROOTPRE environment variable before starting Upgrade Orchestrator on an AIX platform, as follows:

```bash
export SKIP_ROOTPRE=TRUE
```

5.4 Change the Node Manager Password (Cloned Environment Only)

When you upgrade a cloned instance, the upgrade process does not expect the Node Manager password to be different than the keystore password. This difference in passwords causes a failure during the upgrade which includes the following error text:

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

To prevent this issue, change the Node Manager password to be the same as the keystore password before you start the upgrade. Essentially, you change it back to the original password that is used by the Node Manager in the source environment for your clone. Change the values for the Node Manager password and properties using the Administration Console.

After the upgrade, you can change the password back to what it was in your cloned environment after the clone was complete.
Running Post-Upgrade Tasks for Oracle Fusion Applications

This chapter describes the tasks you must perform after you complete the steps in Chapter 5, "Upgrading to Oracle Fusion Applications Release 8".

This chapter contains the following topics:

- Confirm Database Artifact Deployments Were Successful
- Review the Post RUP Installer Report
- Review the Orchestrator Upgrade Report
- Run the Post Validation Check on Oracle Identity Manager Hosts
- Review Policy Store (JAZN) Analysis Reports
- Reload Custom Templates for BI Publisher Reports
- Add Administration Servers to the Machine Created During Scale Out
- Stop and Start Servers to Remove WebChat Connections
- Confirm the IIR Server is Running
- Perform Steps in Release Notes
- Resolve Conflicts That Occurred During Oracle BI Metadata Updates
- Perform Upgrade Steps for Oracle BI Applications
- Upgrade Oracle Fusion Project Portfolio Management Integration with Primavera P6 or Later
- Allocate Memory for HCM Workforce Management
- Ensure High Watermark Patch Bundles Were Applied
- Remove the Contents of the patch_stage Directory (Optional)

6.1 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.
6.2 Review the Post RUP Installer Report

Review the Post RUP Installer report to check for any errors or warnings that require attention. The Post RUP Installer report provides an overview of the tasks that Upgrade Orchestrator ran when it called RUP Installer. It is generated in HTML and XML files and includes links to log files.

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 8, the Post RUP Installer report files are located here:

```
APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/RUP:
```

- PostRUPInstallerReport_timestamp.html
- PostRUPInstallerReport_timestamp.log
- PostRUPInstallerReport_timestamp.xml

For information about resolving errors, see Chapter 7, "Monitoring and Troubleshooting the Upgrade".

6.3 Review the Orchestrator Upgrade Report

Review the Oracle Fusion Applications Orchestrator Upgrade Report to check for any errors or warnings that require attention, to confirm whether the upgrade completed successfully. If there were previous failures during the upgrade, this report would have been generated each time there was a failure. The report name is

```
FAOrchestrationUpgradeReport_release_hosttype_hostname_timestamp.html
```

The Upgrade Orchestrator report is generated for each pod and its location is defined in the mandatory ORCH_REPORT_LOCATION property in the pod.properties file. Previous reports are archived and available for troubleshooting purposes. For more information, see Section A.1.3, "Oracle Fusion Applications Orchestrator Upgrade Report".

6.4 Run the Post Validation Check on Oracle Identity Manager Hosts

Perform the steps in this section only if your Oracle Fusion Applications environment meets the following criteria:

- You run on a SINGLE, 3-NODE, or 4-NODE IDM configuration
- You are on a Solaris or AIX platform
- Your environment is a Release 7 IDM provisioned environment
- You upgraded Oracle Identity Manager using idmupgrade.pl

1. Perform the steps to set the environment variables on each node, as required for your platform. For more information, see Section 4.2.2, "Set Environment Variables."

2. Run postvalidate.pl on each node as follows:
reload custom templates for bi publisher reports

on the oid node:
```bash
cd SHARE_LOCATION/11.1.8.0.0/idmUpgrade
perl postvalidate.pl OID patchAutomation.properties
```

on the oim node:
```bash
cd SHARE_LOCATION/11.1.8.0.0/idmUpgrade
perl postvalidate.pl OIM patchAutomation.properties
```

on the authohs node:
```bash
cd SHARE_LOCATION/11.1.8.0.0/idmUpgrade
perl postvalidate.pl OHS patchAutomation.properties
```

6.5 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/11.1.8.0.0/fapatch/JAZN/stripe/delta/report.txt
```

The stripe is crm, fscm, hcm, obi, soa, ucm or bpm.

Review the Modification section of the report to see the roles that were not updated during the upgrade. For each conflict that displays in this report, you must evaluate and manually patch the role by using Oracle Authorization Policy Manager (APM). For more information, see "Upgrading Oracle Fusion Applications Policies" in the Oracle Fusion Applications Administrator’s Guide.

The following example shows a typical Application Role conflict that has been modified by both the patch and production, therefore it is not applied during the upgrade.

**Modification Conflicts**

Artifact type: Application Role  
Artifact Name: OBIA_PARTNER_CHANNEL_ADMINISTRATIVE_ANALYSIS_DUTY  
Description: This artifact is modified at attribute level in patch version and also in production.

Note the location of the following files for reference when using APM:

- Location of baseline files, where stripe is crm, fscm, hcm, obi, soa, ucm or bpm:
  ```
  FA_ORACLE_HOME/admin/JAZN/stripe/baseline
  ```

- Location of patch files for fscm, crm, and hcm stripes:
  ```
  FA_ORACLE_HOME/stripe/deploy/system-jazn-data.xml
  ```

- Location of patch files for the obi, soa, ucm or bpm stripes:
  ```
  FA_ORACLE_HOME/com/acr/security/jazn/bip_jazn-data.xml
  ```

6.6 Reload Custom Templates for BI Publisher Reports

Perform this step if you have customized BI Publisher reports.
Reload custom templates for BI Publisher reports on Oracle-delivered BI Publisher reports by following the steps in “Upload the Template File to the Report Definition” in the “Customizing Reports and Analytics” chapter of the Oracle Fusion Applications Extensibility Guide.

6.7 Add Administration Servers to the Machine Created During Scale Out

Perform the steps in this section only if the steps in Section 2.6.6, “Validate Domain Directories” required you to temporarily add any Administration Servers back to the originally provisioned machine.

1. Log in to the WebLogic console for the domain.
2. Navigate to Environment, then Machines.
3. Find the machine that was created manually for the purposes of AdminServer high availability scaleout.
4. Click on the machine and go to the Servers tab.
5. Click Lock & Edit to make changes.
6. Click Add.
7. Select the AdminServer and click Finish.
8. Click Activate Changes to apply the changes.

6.8 Stop and Start Servers to Remove WebChat Connections

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

Stop and start the servers on the Common Domain and the CRM Managed Server to remove WebChat connections that were disabled by the DisableWebchatConnections plug-in when you ran RUP Lite for OVM. For more information, see “Starting and Stopping the Administration Servers and Managed Servers” in the Oracle Fusion Applications Administrator’s Guide.

6.9 Confirm the IIR Server is Running

Confirm the IIR server is running. If it is not running, follow the steps in "Troubleshooting Oracle Fusion Data Quality Services and IIR Servers” in the Oracle Fusion Applications Installation Guide to manually check for files that need to be cleaned up and to retry the steps to start the server.

6.10 Perform Steps in Release Notes

Follow any post-upgrade steps mentioned in the Post-Upgrade Known Issues section of Release Notes for Oracle Fusion Applications 11g Release 8 (11.1.8.0.0).
6.11 Resolve Conflicts That Occurred During Oracle BI Metadata Updates

Upgrade Orchestrator updates the applications policies for Oracle Business Intelligence during the Apply Offline BI Metadata and Configuration Updates configuration assistant. When Upgrade Orchestrator runs this configuration assistant, it updates the Oracle BI Applications metadata in the Oracle BI repository and the Oracle BI Presentation Catalog for Oracle Fusion Transactional Business Intelligence and Oracle Business Intelligence Applications.

---

**Note:** This section refers to different Oracle BI directory paths. The BI Oracle home contains the binary and library files necessary for Oracle BI. `BI_ORACLE_HOME` represents the BI Oracle home in path names.

---

This section contains the following topics:

- Resolve Conflicts in the Oracle BI Presentation Catalog
- Resolve Conflicts in the Oracle Business Intelligence Policy Store

### 6.11.1 Resolve Conflicts in the Oracle BI Presentation Catalog

When you run Upgrade Orchestrator, the Oracle BI Metadata Update Tool overwrites all customizations to catalog objects in the Presentation Catalog with the new Oracle-supplied content and logs conflicts in a conflict report.

After Upgrade Orchestrator completes, you must review the conflict report and decide whether you want to retain the new content or re-apply your customizations using a manual process.

**Points to Consider**

- The folders, `/shared/backup/shared` and `/shared/backup/system`, are created in the updated Presentation Catalog during the Upgrade Orchestrator and the Metadata Update Tool process. You access these folders through the Folders pane of the Catalog page in the Oracle BI Enterprise Edition user interface, as described in the following procedure.

  **Note:** The `/shared/backup` folder should not exist before Upgrade Orchestrator runs, because the updated Presentation Catalog file will not be copied to this folder if it already exists.

  As a precaution, to ensure the `/shared/backup` folder does not exist before Upgrade Orchestrator runs, you can optionally create an environment variable called `webcat.force.restore`, which will overwrite the contents of an existing `/shared/backup` folder. This environment variable must be set in the shell prompt from where the orchestrator is going to be invoked, using the command, `setenv webcat.force.restore true`.

- Conflicts that arise during Upgrade Orchestrator and the Metadata Update Tool process are stored in the `/shared/backup/shared` folder in the updated Presentation Catalog. Object references that have conflicts are also stored in `/shared/backup/shared`.

**To resolve conflicts in the Presentation Catalog:**

1. Locate the conflict report named `update-conflict-report.txt`, which is stored in the folder `BI_SHARED_DIR/biapppps_patch_storage/update/Run_ID`.
2. Sign in to Oracle Business Intelligence Enterprise Edition (Oracle BI EE).
3. Click **Catalog** in the global header.

4. In the Folders pane, navigate to **Shared Folders**, backup, and then **shared folder**.

5. Open an object that has a conflict. This object depicts the state of the object before Upgrade Orchestrator and the Metadata Update Tool were run.

6. Open a second instance of Oracle BI EE and the Presentation Catalog.

7. Navigate to the **Shared Folders** folder.

8. Open the same object you opened in step 5. This object depicts the state of the object after Upgrade Orchestrator and the Metadata Update Tool were run (and after the metadata updates were applied).

9. Compare the two objects and decide whether you want to retain the Oracle-supplied updated content or re-apply your customization from the previous version of the Presentation Catalog.

10. To re-apply your customization to an updated object, manually edit the object.

11. Repeat steps 5 through 10 for all objects that have conflicts.

### 6.11.2 Resolve Conflicts in the Oracle Business Intelligence Policy Store

When you run Upgrade Orchestrator, the Oracle BI Metadata Update Tool performs a safe upgrade on the Oracle Business Intelligence policy store, which means it updates only the metadata content that does **not** conflict with your customizations. Updated content that conflicts with your customizations is not applied. Conflicts are listed in the Oracle BI Metadata Tool update report, located at `BI_SHARED_DIR/BI_SHARED_DIR/ .biapps_patch_storage/update/Timestamp/policystore_delta/report.txt`.

This procedure provides instructions for overriding the customizations of the previous Oracle Business Intelligence policy store by applying the Oracle-supplied updated content. This procedure uses Oracle Authorization Policy Manager.

**Note:** You do not need to back up your existing policy store file, because the Metadata Update Tool process does not overwrite your customizations.

**To resolve conflicts in the policy store:**

1. Log in to the Authorization Policy Manager Administration Console.

2. Navigate to the **Home** tab of the Policy Upgrade Management page.

3. Click **Patch Application** in the upper-left corner of the page to display the Patch Application dialog.

4. Select the appropriate application from the **Application** list.

5. In the **Patch File** field, specify the new patch file name and location, for example, `BI_ORACLE_HOME/bifoundation/admin/provisioning/biapps-policystore.xml`.

6. In the **Baseline** field, specify the previous policy store that was backed up by the Oracle BI Metadata Update Tool, for example, `BI_ORACLE_HOME/ .biapps_patch_storage_UPGRADE_from_VERSION/OH_BACKUP/bifoundation/admin/provisioning/biapps-policystore.xml`.

7. Navigate to the **Patch Details** tab to view the policy store conflicts.

**Related Links**

The following documents provide additional information related to subjects discussed in this section:
Allocate Memory for HCM Workforce Management

- For more information about the Fusion Middleware directory structure, see “Understanding Oracle Fusion Middleware Concepts” in Oracle Fusion Middleware Administrator’s Guide.


- For more information about logging in to the Authorization Policy Manager Administration Console, see “Managing Authorization Policies” in Oracle Fusion Applications Administrator’s Guide for instructions.

- For more information about taking the appropriate action regarding conflicts, see the sections titled "Analyzing Patch Differences" and "Resolving Changes and Conflicts" in the Oracle Fusion Applications Administrator’s Guide.

- For detailed information about upgrading Oracle Fusion Applications policies using Oracle Authorization Policy Manager, see "Upgrading Oracle Fusion Applications Policies" in the Oracle Fusion Applications Administrator’s Guide.

6.12 Perform Upgrade Steps for Oracle BI Applications

If you are deploying Oracle Business Intelligence Applications, then you must perform the steps described in "Setting Up Oracle BI Applications" in the Oracle Business Intelligence Applications Installation Guide.

6.13 Upgrade Oracle Fusion Project Portfolio Management Integration with Primavera P6 or Later

If you have installed Oracle Fusion Project Portfolio Management and configured it to integrate with Primavera P6 Enterprise Project Portfolio Management, then you must upgrade the Fusion PPM Bridge and other related configurations in Primavera P6 or later version.

Related Links
The following document provides additional information related to subject discussed in this section:

- For information on upgrading and working with Oracle Fusion Project Portfolio Management, see "Updating Fusion PPM Bridge in WebLogic" in the Primavera P6 EPPM Administrator’s Guide for an Oracle Database.

6.14 Allocate Memory for HCM Workforce Management

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

1. The physical machine hosting HCM Workforce Reputation Management (WorkforceReputationServer_1) managed server must have a minimum of 24 GB of memory. You need to allocate 8 GB of memory to the HCM Workforce Reputation Management (WorkforceReputationServer_1) managed server. The HCM Workforce Reputation Management externalization process may use up to 16 GB of memory.
Perform the following steps to specify memory allocation for HCM Workforce Reputation Management (WorkforceReputationServer_1) managed server:

- **Edit the** `fusionapps_start_params.properties` **file located under** `APPLICATIONS_CONFIG/domains/host_name/HCMDomain/config`.

- **Locate the** # HCMDomain: Main Settings **section in the file. Replace the line**:
  
  ```
  fusion.HCMDomain.WorkforceReputationCluster.default.minmaxmemory.main=-Xms12m -Xmx2048
  ```

  **with**:

  ```
  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 "Starting and Stopping" in the *Oracle Fusion Applications Administrator’s Guide*.

### 6.15 Ensure High Watermark Patch Bundles Were Applied

Ensure you have applied the following high water mark patch bundles on your current environment prior to upgrading to next release:

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

To get more information about high watermark patch bundles, contact Oracle Support.

### 6.16 Remove the Contents of the `patch_stage` Directory (Optional)

To increase free disk space, you can remove the contents of the `APPLICATIONS_BASE/../.patch_stage` directory. This step is optional.
This chapter provides information to assist you in troubleshooting upgrade issues. This chapter contains the following topics:

- General Troubleshooting for Upgrade Orchestrator Failures
- Log Locations
- Monitoring Upgrade Orchestration Progress
- Terminating Upgrade Orchestration
- Canceling the Upgrade and Restoring From Backup
- Troubleshooting Upgrade Orchestrator Failures
- Troubleshooting Failures During the Installation Phase
- Troubleshooting RUP Installer Failures
- Troubleshooting Node Manager and OPMN failures
- Troubleshooting RUP Lite for OHS Failures
- Troubleshooting IDM Upgrade Failures
- Troubleshooting Applying Middleware Patches
- Applying Downloaded Patches Fails
- Troubleshooting Loading Database Components
- Troubleshooting Deployment of Applications Policies
- Troubleshooting Server Start and Stop Failures
- Troubleshooting SOA Composite Deployment Failures
- Troubleshooting RUP Lite for OVM Failures
- Troubleshooting Other Issues During the Upgrade
- Platform Specific Troubleshooting Issues

### 7.1 General Troubleshooting for Upgrade Orchestrator Failures

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 Upgrade Report as an attachment. The report file name is `FAOrchestrationUpgradeReport_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 \texttt{APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/host_name-rel8_hosttype_timestamp.log}.

The following figure depicts the high level flow for troubleshooting Upgrade Orchestrator failures.

\textbf{Figure 7–1  Troubleshooting Flow}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{troubleshooting_flow.png}
\end{figure}

Previous reports are archived whenever a new report is generated, as described in Section 7.6.3, "Unable to Find the Orchestrator Upgrade Report After Failure". For more information about the report, see Section A.1.3, "Oracle Fusion Applications Orchestrator Upgrade 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 \texttt{exitOrchestration} command, its status is "Terminated".

\section*{7.2 Log Locations}

The following types of log files are described in this section:

- Upgrade Orchestrator Log File Directories
- RUP Installer Log File Directories
  - Log Files for Configuration Assistants
  - Log Files for the Database Upload Configuration Assistant

\subsection*{7.2.1 Upgrade Orchestrator Log File Directories}

The following table contains a list of log directories for Upgrade Orchestrator activities. For IDM and OHS log files, the location can be configured using the \texttt{LOG\_LOCATION} property, in the \texttt{IDM.properties} and \texttt{OHS.properties} files. For more information, see Section 2.4.4, "Update Orchestrator Properties Files".

\begin{table}[h]
\centering
\caption{Upgrade Tasks and Related Log Files}
\begin{tabular}{|l|l|}
\hline
Task Display Name and ID & Log File Location \\
\hline
Stopping Index Schedules and Deactivating Index Optimization (StopIndexSchedules) & \texttt{APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/host_name-rel8_primordial_timestamp.log} \\
\hline
\end{tabular}
\end{table}
Table 7–1 (Cont.) Upgrade Tasks and Related Log Files

<table>
<thead>
<tr>
<th>Task Display Name and ID</th>
<th>Log File Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stopping All Servers</td>
<td>Orchestration log files:</td>
</tr>
<tr>
<td>(StopAllServers)</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-re18_primordial_timestamp.log</td>
</tr>
<tr>
<td></td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-re18_midtier_timestamp.log</td>
</tr>
<tr>
<td></td>
<td>Control log file:</td>
</tr>
<tr>
<td></td>
<td>APPLICATIONS_CONFIG/lcm/logs/startstop/STOP_date_time_hostname.log</td>
</tr>
<tr>
<td>Setting CrashRecoveryEnabled Property to False</td>
<td>Orchestration log files:</td>
</tr>
<tr>
<td>(Disable CrashRecoveryEnabled)</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-re18_primordial_timestamp.log</td>
</tr>
<tr>
<td></td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-re18_midtier_timestamp.log</td>
</tr>
<tr>
<td>Stopping OPMN Control Processes</td>
<td>Orchestration log files:</td>
</tr>
<tr>
<td>(StopOPMNProcesses)</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-re18_primordial_timestamp.log</td>
</tr>
<tr>
<td></td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-re18_midtier_timestamp.log</td>
</tr>
<tr>
<td></td>
<td>OPMN log file:</td>
</tr>
<tr>
<td></td>
<td>APPLICATIONS_CONFIG/DOMAIN_CONFIG</td>
</tr>
<tr>
<td></td>
<td>Example: BIInstance&gt;/diagnostics/logs/OPMN/opmn/</td>
</tr>
<tr>
<td>Stopping Node Managers</td>
<td>Orchestration log files:</td>
</tr>
<tr>
<td>(StopNodeManager)</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-re18_primordial_timestamp.log</td>
</tr>
<tr>
<td></td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-re18_midtier_timestamp.log</td>
</tr>
<tr>
<td>Stopping Oracle Identity Management - AUTHOHS (StopOHS)</td>
<td>Orchestration log files:</td>
</tr>
<tr>
<td></td>
<td>/u01/logs/IDM/11.1.8.0.0/orchestration/hostame-rel8_i dm_timestamp.log</td>
</tr>
<tr>
<td>This log file is generated only for automated IDM upgrades.</td>
<td>IDM log file:</td>
</tr>
<tr>
<td></td>
<td>/u01/logs/IDM/logs_node_type/stopIDM_hostname_timestamp.log</td>
</tr>
<tr>
<td>Stopping Oracle Identity Management - OIM (StopOIM)</td>
<td>Orchestration log files:</td>
</tr>
<tr>
<td></td>
<td>/u01/logs/IDM/11.1.8.0.0/orchestration/hostame-rel8_i dm_timestamp.log</td>
</tr>
<tr>
<td>This log file is generated only for automated IDM upgrades.</td>
<td>IDM log file:</td>
</tr>
<tr>
<td></td>
<td>/u01/logs/IDM/logs_node_type/stopIDM_hostname_timestamp.log</td>
</tr>
<tr>
<td>Task Display Name and ID</td>
<td>Log File Location</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------</td>
</tr>
</tbody>
</table>
| **Stopping Oracle Identity Management - OID**<br>(StopOID) | Orchestration log files:  
  - /u01/logs/IDM/11.1.8.0.0/orchestration/hostname-rel8_idm_timestamp.log  
IDM log file:  
  - /u01/logs/IDM/logs_node_type/stopIDM_hostname_timestamp.log |
| **Backing up OPSS Security Store**<br>(BackupOPSS) | Orchestration log file:  
  - APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_IDM_timestamp.log  
IDM log file:  
  - /u01/logs/IDM/logs_ALL/idmUpgrade_hostname_timestamp.log |
| **Upgrading Oracle Identity Management - OID**<br>(OIDApplyPatches) | Orchestration log files:  
  - /u01/logs/IDM/11.1.8.0.0/orchestration/hostname-rel8_idm_timestamp.log  
IDM log file:  
  - /u01/logs/IDM/logs_node_type/IDMupgrade_hostname_timestamp.log |
| **Upgrading Oracle Identity Management - OIM**<br>(OIMApplyPatches) | Orchestration log files:  
  - /u01/logs/IDM/11.1.8.0.0/orchestration/hostname-rel8_idm_timestamp.log  
IDM log file:  
  - /u01/logs/IDM/logs_node_type/IDMupgrade_hostname_timestamp.log |
| **Upgrading Oracle Identity Management - AUTHOHS**<br>(OHSApplyPatches) | Orchestration log files:  
  - /u01/logs/IDM/11.1.8.0.0/orchestration/hostname-rel8_idm_timestamp.log  
IDM log file:  
  - /u01/logs/IDM/logs_node_type/IDMupgrade_hostname_timestamp.log |
| **Validating Oracle Identity Management Setup & Configuration**<br>(IDMPostValidate) | Orchestration log files:  
  - /u01/logs/IDM/11.1.8.0.0/orchestration/hostname-rel8_idm_timestamp.log  
IDM log file:  
  - /u01/logs/IDM/logs_node_type/postValidate_hostname_timestamp.log |
Table 7–1 (Cont.) Upgrade Tasks and Related Log Files

<table>
<thead>
<tr>
<th>Task Display Name and ID</th>
<th>Log File Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running Upgrade Readiness (During Downtime) Checks (DuringDowntimeChecks)</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/healthchecker/PRIMORDIAL_hostname-DuringDowntimeUpgradeReadinessHealthChecks_timestamp.log</td>
</tr>
<tr>
<td></td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/healthchecker/MIDTIER_hostname-DuringDowntimeUpgradeReadinessHealthChecks_timestamp.log</td>
</tr>
<tr>
<td></td>
<td>/u01/logs/OHS/logs/healthchecker/OHS_hostname-DuringDowntimeUpgradeReadinessHealthChecks_timestamp.log</td>
</tr>
<tr>
<td></td>
<td>/u01/logs/IDM/logs/healthchecker/IDM_hostname-PreDowntimeUpgradeReadinessHealthChecks_timestamp.log</td>
</tr>
<tr>
<td>Removing Conflicting Patches for Oracle Fusion Middleware Component Oracle Homes (RemoveConflictingPatches)</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_primordial_timestamp.log</td>
</tr>
<tr>
<td>Installing Oracle Fusion Applications LCM Tools for Oracle VM (InstallFaSaasLcmTools)</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_primordial_timestamp.log</td>
</tr>
<tr>
<td>Preparing for Oracle Fusion Applications LCM Tools for Oracle VM Upgrade (PrepareLCMToolsForOVMUpgrade)</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_primordial_timestamp.log</td>
</tr>
<tr>
<td>Applying Oracle Fusion Applications LCM Tools for Oracle VM Patches (ApplyLCMToolsForOVMPatches)</td>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_primordial_timestamp.log</td>
</tr>
<tr>
<td>Running RUP Lite for OVM in Offline Mode as Application User (RupLiteOvmOffline)</td>
<td>/u01/lcm/rupliteovm/output/logs/11.1.8.0.0/hostname/rupliteoffline.log</td>
</tr>
<tr>
<td>Running Oracle Fusion Applications RUP Installation Part 1 of 2 (RunFirstRUPInstaller)</td>
<td>Orchestration log file: APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_primordial_timestamp.log</td>
</tr>
<tr>
<td></td>
<td>Oracle Fusion Applications Patch Manager log file: APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/RUP/fapatch_timestamp.log</td>
</tr>
</tbody>
</table>
Table 7–1  (Cont.) Upgrade Tasks and Related Log Files

<table>
<thead>
<tr>
<th>Task Display Name and ID</th>
<th>Log File Location</th>
</tr>
</thead>
</table>
| Running RUP Lite for Domain Configuration (RunRUPLiteForDomainsConfig) | Orchestration log file
  ■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_midtier_timestamp.log |
|                                        | RUPLite for Domain Config log file:
  ■ APPLICATIONS_CONFIG/lcm/admin/11.1.8.0.0/fapatch/ruplitedomain/output/logs |
| Starting Node Managers (StartNodeManager) | Orchestration log file:
  ■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_primordial_timestamp.log |
|                                        | ■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_midtier_timestamp.log |
|                                        | Oracle Fusion Applications Control log file:
  ■ APPLICATIONS_CONFIG/lcm/logs/startstop_saas/STOP_timestamp_hostname.log |
| Starting OPMN Control Processes (StartOPMNProcesses) | Orchestration log files:
  ■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_primordial_timestamp.log |
|                                        | ■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_midtier_timestamp.log |
|                                        | ■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_ohs_timestamp.log |
| Running Oracle Fusion Applications RUP Installation Part 2 of 2 (RunSecondRUPInstaller) | Orchestration log file:
  ■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_primordial_timestamp.log |
|                                        | Oracle Fusion Applications Patch Manager log file:
  ■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/RUP/fapatch_timestamp.log |
| Running Vital Signs Checks (VitalSignsChecks) | ■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/healthchecker/PRIMORDIAL_hostname-VitalSignsChecks_timestamp.log |
| Invoking an Instance of UpdateSOAMDS SOA Composite (UpdateMDSSOAComposite) | ■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_primordial_timestamp.log |
| Preparing for Oracle Fusion Applications WebTier Upgrade (CopyWebtierUpgradeToCentralLoc) | ■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_primordial_timestamp.log |
### Table 7–1 (Cont.) Upgrade Tasks and Related Log Files

<table>
<thead>
<tr>
<th>Task Display Name and ID</th>
<th>Log File Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stopping Oracle Fusion Applications - APPOHS (StopOPMNProcesses)</td>
<td>Orchestration log files:</td>
</tr>
<tr>
<td></td>
<td>■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_primordial_timestamp.log</td>
</tr>
<tr>
<td></td>
<td>■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_midtier_timestamp.log</td>
</tr>
<tr>
<td></td>
<td>■ /u01/logs/OHS/11.1.8.0.0/orchestration/hostname-rel8_o hs_timestamp.log</td>
</tr>
<tr>
<td></td>
<td>OPMN logs:</td>
</tr>
<tr>
<td></td>
<td>■ APPLICATIONS_CONFIG/DOMAIN_CONFIG</td>
</tr>
<tr>
<td></td>
<td>Example: BIInstance&gt;/diagnostics/logs/OPMN/opmn/</td>
</tr>
<tr>
<td>Removing Conflicting Patches for Oracle Fusion Applications WebTier Oracle Homes (RemoveConflictingPatches)</td>
<td>Orchestration log files:</td>
</tr>
<tr>
<td></td>
<td>■ /u01/logs/OHS/11.1.8.0.0/orchestration/hostname-rel8_o hs_timestamp.log</td>
</tr>
<tr>
<td>Upgrading Oracle Fusion Applications OHS binaries (UpgradeOHSBinary)</td>
<td>Orchestration log files:</td>
</tr>
<tr>
<td></td>
<td>■ /u01/logs/OHS/11.1.8.0.0/orchestration/hostname-rel8_o hs_timestamp.log</td>
</tr>
<tr>
<td></td>
<td>Web Gate log file:</td>
</tr>
<tr>
<td></td>
<td>■ /u01/webgate/hostname/webgate_installer_REL8/output/logs/hostname/rupliteohsupgradeohsbinary_timestamp.log</td>
</tr>
<tr>
<td>Upgrading Oracle Fusion Applications OHS Configuration (UpgradeOHSCfg)</td>
<td>Orchestration log files:</td>
</tr>
<tr>
<td></td>
<td>■ /u01/logs/OHS/11.1.8.0.0/orchestration/hostname-rel8_o hs_timestamp.log</td>
</tr>
<tr>
<td></td>
<td>RUPLite log file:</td>
</tr>
<tr>
<td></td>
<td>■ /u01/webgate/hostname/webgate_installer_REL8/output/logs/hostname/backupupgradeohsconfig/ru piliteohsupgradeohsconfig_timestamp.log</td>
</tr>
<tr>
<td>Running RUP Lite for BI (RunRUPLiteForBI)</td>
<td>Orchestration log files:</td>
</tr>
<tr>
<td></td>
<td>■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_midtier_timestamp.log</td>
</tr>
<tr>
<td>Running RUP Lite for OVM in Online Mode as Application User (RupLiteOvmOnline)</td>
<td>Orchestration log files:</td>
</tr>
<tr>
<td></td>
<td>■ /u01/rcm/rupliteovm/output/logs/11.1.8.0.0/hostname/rupliteonline.log</td>
</tr>
<tr>
<td>Starting IIR (StartIIRPlugin)</td>
<td>Orchestration log files:</td>
</tr>
<tr>
<td></td>
<td>■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_midtier_timestamp.log</td>
</tr>
<tr>
<td>Setting CrashRecoveryEnabled Property to True (EnableCrashRecoveryEnabled)</td>
<td>Orchestration log files:</td>
</tr>
<tr>
<td></td>
<td>■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_primordial_timestamp.log</td>
</tr>
<tr>
<td></td>
<td>■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_midtier_timestamp.log</td>
</tr>
</tbody>
</table>
### Table 7–1 (Cont.) Upgrade Tasks and Related Log Files

<table>
<thead>
<tr>
<th>Task Display Name and ID</th>
<th>Log File Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running Post Upgrade Health Checks (PostUpgradeChecks)</td>
<td></td>
</tr>
<tr>
<td>■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/healthchecker/PRIMORDIAL_hostname-PostUpgradeHealthChecks_timestamp.log</td>
<td></td>
</tr>
<tr>
<td>■ /u01/logs/OHS/logs/healthchecker/OHS_hostname-PostUpgradeHealthChecks_timestamp.log</td>
<td></td>
</tr>
<tr>
<td>■ midtier_hostname-manifest_name_worker/DowntimePostFA/midtier_hostname-manifest_name_PostUpgradeChecks_timestamp.log</td>
<td></td>
</tr>
<tr>
<td>Running Data Quality Checks (DataQualityChecks)</td>
<td></td>
</tr>
<tr>
<td>■ PRIMORDIAL_hostname-DataQualityChecks_timestamp.log</td>
<td></td>
</tr>
<tr>
<td>Running Post Upgrade Cleanup Tasks (PostUpgradeCleanup)</td>
<td></td>
</tr>
<tr>
<td>■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_primordial_timestamp.log</td>
<td></td>
</tr>
<tr>
<td>Upgrading All Installed Languages (LanguagePackInstall)</td>
<td></td>
</tr>
<tr>
<td>■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_primordial_timestamp.log</td>
<td></td>
</tr>
<tr>
<td>■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_midtier_timestamp.log</td>
<td></td>
</tr>
<tr>
<td>Stopping All Servers (StopServersAfterLP)</td>
<td></td>
</tr>
<tr>
<td>■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_primordial_timestamp.log</td>
<td></td>
</tr>
<tr>
<td>■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_midtier_timestamp.log</td>
<td></td>
</tr>
<tr>
<td>Starting All Servers (StartSeversAfterLP)</td>
<td></td>
</tr>
<tr>
<td>■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_primordial_timestamp.log</td>
<td></td>
</tr>
<tr>
<td>■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/orchestration/hostname-rel8_midtier_timestamp.log</td>
<td></td>
</tr>
<tr>
<td>Running Post Language Pack Health Checks (PostLangPackChecks) - This must call both general system and post LP upgrade checks</td>
<td></td>
</tr>
<tr>
<td>■ APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/healthchecker/PRIMORDIAL_hostname-PostLanguagePackHealthChecks_timestamp.log</td>
<td></td>
</tr>
</tbody>
</table>

### 7.2.2 RUP Installer Log File Directories

The following table contains a list of log directories for RUP Installer activities.

<table>
<thead>
<tr>
<th>Log directory name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>oracle_inventory/logs</td>
<td>Installation phase and Oracle Fusion Middleware patch set installation logs.</td>
</tr>
<tr>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/RUP</td>
<td>Top level directory for RUP Installer logs.</td>
</tr>
<tr>
<td>APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/RUP/ARCHIVE/timestamp</td>
<td>Top level log directory where log files are moved when you retry the installation session.</td>
</tr>
</tbody>
</table>
### 7.2.2.1 Log Files for Configuration Assistants

During the configuration phase of the upgrade, each configuration assistant creates its own log file under the `APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/RUP/configlogs` directory. All messages that are generated during the configuration assistant processing are written to this log file. The only information related to configuration assistants that is written to the main log file, `APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/RUP`, are those messages that indicate that a configuration assistant started and the result of its processing, such as success or error.

### 7.2.2.2 Log Files for the Database Upload Configuration Assistant

During the execution of the `Load Database Components` configuration assistant, log files are created under the `/lcm/logs` directory. Upon completion or failure of the database upload, the log files move to the `APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/RUP/PatchManager_DBPatch` directory.

### 7.3 Monitoring Upgrade Orchestration Progress

You can monitor the progress of the upgrade by monitoring the console output or by running the `getStatus` command. You can run this command on any host, to get the upgrade status for that host or for other hosts. The command follows:
cd ORCH_LOCATION
./orchestration.sh getStatus -pod POD_NAME -hosttype host_type -hostname host_name
-release release_version [-phase phase_name] [-taskid task_id] [-taskstatus task_status]

Example 7–1  Retrieve the overall status of the upgrade
./orchestration.sh getStatus -pod fcsm -hosttype PRIMORDIAL -hostname host_name
-release REL8

Example 7–2  Retrieve all tasks in a phase
./orchestration.sh getStatus -pod fcsm -hosttype PRIMORDIAL -hostname host_name
-release REL8 -phase predontime

Example 7–3  Retrieve all tasks with a specific status
./orchestration.sh getStatus -pod fcsm -hosttype PRIMORDIAL -hostname host_name
-release REL8 -taskstatus success

Example 7–4  Retrieve the status of a specific task
./orchestration.sh getStatus -pod fcsm -hosttype PRIMORDIAL -hostname host_name
-release REL8 -taskid HostTypeValidatePlugin

Table A–3, "Options for orchestration.sh getStatus command" displays a complete list
of options for the orchestration.sh getStatus command.

If any upgrade tasks fail, the Fusion Applications Orchestrator Upgrade Report is
generated and mailed as an attachment to the user specified in the EMAIL_TO_<
RECIPIENT property in the pod.properties file. For more information, see
Section A.1.3, "Oracle Fusion Applications Orchestrator Upgrade Report". For
information about troubleshooting failures, refer to the appropriate section in this
chapter to resolve the issue. After a failure, restart Orchestrator on the host where it
failed, using the same commands you used in Section 5.1.1, "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 step in RUP Installer fails, you receive an email
notification only when all workers are in a FAILED or IDLE (no tasks assigned to it)
state. To resolve this type of issue, follow the steps in Section 7.13.2, "Workers Fail
While Loading Database Components".

7.4 Terminating Upgrade Orchestration

Orchestration can be terminated on all hosts under scenarios that require you to issue
an exit command across the entire environment. This section describes the commands
to use to terminate orchestration on all hosts.
7.4.1 Terminate an Orchestration Session

When you need to terminate an orchestration session on a pod for reasons such as, not being able to complete the upgrade within a certain time, or unexpected issues that may require significant time to resolve, run the following command:

```
cd /ORCH_LOCATION/bin
./orchestration.sh exitOrchestration -pod POD_NAME -hosttype host_type
```

This command terminates the orchestration session on all hosts across all host types in the specified pod. This command can be run from any individual host for the entire environment and/or pods. The `hosttype` argument must match the host from which you issue this command. Upgrade Orchestration sends a notification after all hosts exit from orchestration. After you receive this notification, you must run the command to clear the exit status on all hosts, as described in Section 7.4.2, "Clear the Exit Status on All Hosts." If you do not receive this notification on a timely basis, you can find the status of your request by running the command described in Section 7.4.3, "Get the ExitOrchestration Status."

**Note:** From the time `exitOrchestration` is issued, until `clearExitOrchestration` is issued, no other command, other than `getExitOrchestrationStatus`, can be issued on the pod. Also, `exitOrchestration` can be issued from any host but is applicable for all the hosts under a pod.

7.4.2 Clear the Exit Status on All Hosts

Run the following command to clear the exit status on all hosts, after you receive the notification that confirms all hosts exited from orchestration:

```
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.

7.4.3 Get the ExitOrchestration Status

While the `exitOrchestration` command is running, you can run the `getExitOrchestrationStatus` command to retrieve the status of the `exitOrchestration` command.

```
cd /ORCH_LOCATION/bin
./orchestration.sh getExitOrchestrationStatus -pod POD_NAME
```

7.5 Canceling the Upgrade and Restoring From Backup

To cancel the upgrade and to restore the system, first terminate orchestration by following the steps in Section 7.4, "Terminating Upgrade Orchestration". After orchestration terminates successfully, restore the system from the backup that was taken before starting the upgrade. In addition to restoring the environment from the backups, perform the following steps to restore and clean up the orchestration files.

1. Directories configured for the following properties in `pod.properties` are used by Upgrade Orchestration to store checkpoint files and to archive older versions of checkpoint files.
7.6 Troubleshooting Upgrade Orchestrator Failures

The following specific troubleshooting scenarios are described in this section:

- Unable to Upload Orchestration Checkpoints
- Safely Exit Upgrade Orchestrator
- Unable to Find the Orchestrator Upgrade Report After Failure
- Upgrade Orchestrator Report Fails to Generate Due to Out Of Memory Error
- Property Validation Fails Due to Invalid Property Error
- Unable to Update Task Status From Running to Success
- Emails Are Not Being Sent Upon Failure
- Upgrade Orchestrator Does Not Use a Value in the Properties File
- Stale NFS File Handle Error
- Error in Creating_Middleware_Schemas Log
- Cannot Remove Snapshot File Error
- Informatica Identity Resolution (IIR) Does Not Come Up After the Upgrade
- Unable to Initialize the Checkpoint System
- Stop Index Schedule and Deactivate Index Optimization Fails on Primordial Host

7.6.1 Unable to Upload Orchestration Checkpoints

**Problem**
When orchestration is relaunched for any reason, there could be an error loading checkpoint files to the appropriate location. In this case, Upgrade Orchestrator exits with the following errors.

Unable to upload orchestration checkpoints under /fsnadmin/upgrade/fusionChangeOps/11.1.8.0.0/orchestration/bin/../checkpoint.

**Corrective Action:** Remove any existing files from older Orchestration run in /fsnadmin/upgrade/fusionChangeOps/11.1.8.0.0/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.
7.6.2 Safely Exit Upgrade Orchestrator

**Problem**
Orchestration hangs during the preDowntime or downtimeFA phase, or you need to exit Upgrade Orchestrator in the middle of an upgrade for any valid reason.

**Solution**
Run the exitOrchestration command from another console, on any host in the pod, to gracefully exit orchestration. Then run clearExitOrchestration. Refer to Section 7.4, "Terminating Upgrade Orchestration".

The exitOrchestration command terminates the upgrade on all hosts. Therefore, after you resolve the issue, rerun orchestration on all hosts where orchestration was previously running.

7.6.3 Unable to Find the Orchestrator Upgrade Report After Failure

**Problem**
After Upgrade Orchestrator fails, the console reports the following example information:

Fusion Applications Orchestrator Upgrade Report:
/u01/orchestration/orchreports/FAOrchestrationUpgradeReport_release_hosttype_hostname_timestamp.html

This html file does not exist in the /u01/orchestration/orchreports directory.

**Solution**
As the upgrade progresses, the Orchestrator Upgrade report is archived after the failure or completion of each task. You can find the output in the following directory, based on the example.


7.6.4 Upgrade Orchestrator Report Fails to Generate Due to Out Of Memory Error

**Problem**
Upgrade Orchestrator fails while generating the Upgrade Orchestrator report with the following error:

*Java.lang.OutOfMemoryError: PermGen space

**Solution**
Increase the ORCH_JVM_OPTION value in pod.properties to allocate more memory for both the startup of JVM and the total size of permgen, as shown in the following example:

ORCH_JVM_OPTION=-Xmx2048m -XX:PermSize=256M -XX:MaxPermSize=512M

7.6.5 Property Validation Fails Due to Invalid Property Error

**Problem**
Property validation fails during the PreDowntime phase with the following error:
Invalid property: must specify ORCHESTRATION_CHECKPOINT_LOCATION in orchestration properties file ./../config/pod/pod_properties.

No log file or HTML file is generated.

Solution
Populate the ORCHESTRATION_CHECKPOINT_LOCATION mandatory property in the pod.properties file. Note that no logs are generated for this type of failure by design.

7.6.6 Wait for Peer Phase Error After Setting Task to Success Status

Problem
You ran the updateStatus command to manually set the status of a failed task_id on the primordial host to "success" for the PreDowntime phase. After you resume orchestration on the IDM host, it fails with the following error:

Wait for peer phase: PRIMORDIAL:PreDowntime on host.mycompany.com
Found peer phase: PRIMORDIAL:PreDowntime on host.mycompany.com Error.

The results of getStatus on the pod shows that all tasks were successful but the PreDownTime phase was in error status.

Solution
Setting a task status to "success" does not resolve a "Wait for peer phase" error, because a phase level status cannot be updated by the updateStatus command. The only way to resolve a "Wait for peer phase" issue is to resume orchestration so that it can verify that all tasks in the phase were successful.

7.6.7 Unable to Update Task Status From Running to Success

Problem
An orchestration task is no longer running and the following error is reported:

Orchestration step: DowntimePreFA DeploySoaShared Running
Unable to update task status from Running to Success

Oracle Fusion Applications Release Upgrade Orchestration failed.

Solution
Before performing the step in this solution, confirm that there are no orchestration processes running. Then run the updateStatus command to change the status of the task specified in the error message to error and then resume Upgrade Or orchestrator.

Upgrade Or orchestrator supports only the following status transitions:

- Error to Success
- Running to Error
- ManualStep to Success
- Success to Error
7.6.8 Emails Are Not Being Sent Upon Failure

**Problem**
The emails that Upgrade Orchestrator sends upon failure are not being received.

**Solution**
Perform the following steps to check if your mail server is configured properly:

1. You can check if your mail server is configured properly by running the following command:
   
   
   ```
   echo hello | /usr/sbin/sendmail <email_addr>
   ```

2. If emails are not being sent, restart the mail server and test again.
   
   ```
   /etc/init.d/sendmail restart
   ```

3. Ensure that all properties related to email are populated with the correct values in the `pod.properties` file. For more information, see Table B-1, "pod.properties".

7.6.9 Upgrade Orchestrator Does Not Use a Value in the Properties File

**Problem**
Upgrade Orchestrator is not using a value that was recently added to one of the properties files.

**Solution**
If you updated the properties file after launching Upgrade Orchestrator, follow the steps to safely exit orchestration in Section 7.6.2, "Safely Exit Upgrade Orchestrator" and then relaunch orchestration.

7.6.10 Stale NFS File Handle Error

**Problem**
While running various commands for Upgrade Orchestrator, the following error is reported:

Stale NFS file handle

**Solution**
If the Stale NFS file handle error is reported while running any of the plug-ins in orchestration or the `getStatus` or `updateStatus` commands, verify that all mount points provided in the various property files are actually accessible. For more information, see Appendix B, "Upgrade Orchestrator Properties Files".

7.6.11 Error in Creating_Middleware_Schemas Log

**Problem**
The following error is reported:

7.6.12 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 Orchestrator failed.

Solution
Remove the file that is causing the error and restart Upgrade Orchestrator.

7.6.13 Informatica Identity Resolution (IIR) Does Not Come Up After the Upgrade

Problem
IIR does not come up after following the steps to start IIR as part of the Start External Servers Pause Point Post Upgrade step.

Solution
Follow the steps in "Troubleshooting Informatica Identity Resolution and Data Quality Setup" in the Oracle Fusion Applications Installation Guide to manually check for files that need to be cleaned up and to retry the steps to start the server.

7.6.14 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.

7.6.15 Stop Index Schedule and Deactivate Index Optimization Fails on Primordial Host

Problem
SES crawler processes in the LAUNCHING state cannot be stopped. The following errors messages are reported in the primordial orchestration log. The schedule names listed in the snippet below are the schedules that could not be stopped.
Troubleshooting Failures During the Installation Phase

Perform the following steps when an error occurs during the RUP Installer or Language Pack Installer installation phase:

1. Click Cancel to exit out of the installer.
2. Review the log files to determine the cause of the failure. The log files reside in oracle_inventory/logs/installtimestamp.log.
3. Resolve the cause of the failure.
4. Start the installer using the same command syntax that you used for the previous incomplete installation. After canceling the previous installation and starting again, you must choose to continue with the previously failed installation by clicking Yes on the Checkpoint Dialog. If the error is not recoverable, you can restore and restart from backup.
5. If you choose to continue with the failed installation, the installer opens at the screen where it was canceled. When canceled during the copy action, it relaunches in the Installation Summary screen. Click Next to navigate through the Installation Summary screen. When the Installation Progress screen displays, click Install to start the installation again.

Troubleshooting steps are described for the following specific failures that may occur during the installation phase:

- CFGLOG-00056: Exception caught while getting node-manager homes
- Invalid Oracle Home
- Error in Writing to File, Text File Busy
- Inventory Pointer File is Empty

7.7.1 CFGLOG-00056: Exception caught while getting node-manager homes

Problem
Within a few seconds of starting the installer, you receive the following messages:

In the log file:
SEVERE: CFGLOG-00056 : Exception caught while getting node-manager homes

In the user interface:
CFGLOG-00052 : Error occurred while moving instance specific files

**Solution**
This failure is the result of having an incompatible version of OPatch in FA_ORACLE_HOME. To resolve the issue, download and apply patch 14044793, which contains the compatible version of OPatch.

### 7.7.2 Invalid Oracle Home

**Problem**
In the Installation Location page, you receive a message about entering an invalid Oracle home, even though the location displayed on the page is correct. The installer reads /etc/oraInst.loc to determine the location of the central inventory.

**Solution**
To resolve this problem:

- Ensure that the /etc/oraInst.loc file on the machine where you are running the installer is pointing to the correct central inventory location.
- Ensure that the FA_ORACLE_HOME matches the values provided during provisioning. If a /net/location was provided as the Oracle home location during provisioning, the same /net/location that corresponds to FA_ORACLE_HOME should be provided during the installation. You can find this location by following these steps:
  - Open /etc/oraInst.loc and find the path to oraInventory, which is the central inventory, for example, server01/appmgr/APPTOP/oraInventory.
  - Change directory to the ContentsXML directory under the central inventory, for example, server01/appmgr/APPTOP/oraInventory/ContentsXML.
  - Open the inventory.xml file to find the correct directory path to FA_ORACLE_HOME.

### 7.7.3 Error in Writing to File, Text File Busy

**Problem**
During the installation phase of RUP Installer, you receive the following message on a UNIX platform.

Error in writing to file
'#/server01/APPLICATIONS_BASE/fusionapps/applications/lcm/ad/bin/adctrl'
(Text file busy)

**Solution**
To resolve this issue, perform the following steps.

1. Run the lsof command using the full directory path of the file that is busy.
   
   /usr/bin/lsof full_path_to_file
2. You should receive a list of process ids that are using the file. Kill each process using the appropriate command for your operating system.

3. After all processes are no longer running, resume orchestration.

### 7.7.4 Inventory Pointer File is Empty

**Problem**
After running the installer, the contents of `oraInst.loc` were removed.

**Solution**
The installer always tries to copy the inventory pointer file specified by the `-invPtrLoc` option to the Oracle home on which the release is to be installed. If you specify an incorrect path for the `-invPtrLoc` file, the inventory pointer file could result in being an empty file. Review the following possible solutions for this issue:

- For best results, if you are using the `-invPtrLoc` option, use it with this value: `FA_ORACLE_HOME/oraInst.loc`. This avoids a situation where you may inadvertently exclude part of the directory path to the file, as in the case of using a mapped drive. For example, if Oracle home is registered in inventory with a `/net` path, such as `/net/home/oraInst.loc`, and you provide `/home/oraInst.loc` to the `-invPtrLoc` option, the installer interprets the two paths as different. The end result is an empty inventory pointer file.

- If `FA_ORACLE_HOME` is registered in central inventory with a `/net` path, then you must include `/net` when specifying the location of the inventory pointer file with the `-invPtrLoc` option, for example, `-invPtrLoc /net/directory_path/oraInst.loc`.

- Restore from a backup copy of your `oraInst.loc` file in case the original file is damaged. You can find this in `/etc/oraInst.loc`.

- You can recover from this error by creating a new `oraInst.loc`. See the “Creating the oraInst.loc File” section in the relevant Oracle Database installation guide, for example, *Oracle Database Installation Guide, 11g Release 2 (11.2) for Linux*. Then resume orchestration.

### 7.8 Troubleshooting RUP Installer Failures

This section provides information about the following RUP Installer failures:

- **RUP Installer Fails**
- **Installer Requirement Checks Fail**
- **Failure During Apply Pre-PSA Due to Smart Patch Conflict (Oracle VM Only)**
- **RUP Installer Fails Due To Thread Calls**
- **Recover From an Installer Session That Was Shut Down**
- **Deploying New Application Configuration Fails with a "NumberFormatException"**
- **Importing of Group Space Templates Fails During RUP Installer Part 2**
- **GST Validation Fails During Import of Group Space Template**
Troubleshooting RUP Installer Failures

- **Configuration Assistant Fails Due to "Could not create credential store instance" Error**
- **First Installer Fails on Primordial Host During Applying Middleware Patchsets**

### 7.8.1 RUP Installer Fails

RUP Installer is one of the tasks performed by Upgrade Orchestrator. In the case of a failure, information in Section 7.1, "General Troubleshooting for Upgrade Orchestrator Failures" applies. In addition to the Upgrade Report and log location, the RUP Installer Report location is also included as part of the notification that is sent. For more information, see Section 6.2, "Review the Post RUP Installer Report".

### 7.8.2 Installer Requirement Checks Fail

**Problem**
The installer fails with the following type of errors:

Starting Oracle Universal Installer...
Checking if CPU speed is above 300 MHz.
Checking Temp space: must be greater than 4096 MB. Actual 9177 MB Passed

Checking swap space: 3915 MB available, 4000 MB required. Failed <<<<
Some requirement checks failed. You must fulfill these requirements before continuing with the installation,

**Solution**
Manually increase the requirement check that failed, in this example, the swap space. Then resume orchestration.

### 7.8.3 Failure During Apply Pre-PSA Due to Smart Patch Conflict (Oracle VM Only)

**Problem**
For the CRM stripe on an Oracle VM environment, RUP Installer fails during the **Apply Pre-PSA Middleware Patches** configuration assistant, due to a smart patch conflict. The following exception is reported:

"Conflict(s) detected - resolve conflict condition and execute patch installation again.

Conflict condition details follow:

SEVERE: Conflict(s) detected - resolve conflict condition and execute patch installation again

Patch HYKC is mutually exclusive and cannot coexist with patch(es):
3BBT, SZXM, 7YZB, 6D9T, 56MM, F89C, 9264, 9887, S39F, 7AAZ, JZED, E9FL, IH4D, YJTB

SEVERE: Patch HYKC is mutually exclusive and cannot coexist with patch(es):
3BBT, SZXM, 7YZB, 6D9T, 56MM, F89C, 9264, 9887, S39F, 7AAZ, JZED, E9FL, IH4D, YJTB"

**Solution**
Manually roll back all conflicting WLS patches and rerun orchestration.
7.8.4 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 restarting Upgrade Orchestrator.

7.8.5 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 your backup of `APPLICATIONS_BASE` and start from the beginning of the upgrade.

7.8.6 Deploying New Application Configuration Fails with a "NumberFormatException"

**Problem**
A `NumberFormatException` is reported when retrying the Deploy New Applications configuration assistant due to an incorrect value for `numCompletedDeployments` variable in the `checkpoint.xml` file.

**Solution**
To resolve this issue, convert the float value to an integer value for the "NumberOfSuccessfulArtifacts" attribute in the checkpoint file located at `central_inventory_location/checkpoint/11.1.8.0.0/farup/checkpoint.xml`.

The following example shows the value to be updated in bold:

```xml
<aggregate name="Deploying New Applications" status="fail">
  <property name="NumberOfSuccessfulArtifacts" value="2.0"/>
  ...
</aggregate>
```

The following example shows the updated value in bold.

```xml
<aggregate name="Deploying New Applications" status="fail">
  <property name="NumberOfSuccessfulArtifacts" value="2"/>
  ...
</aggregate>
```
7.8.7 Importing of Group Space Templates Fails During RUP Installer Part 2

Problem
The import of Group Space Templates fails with the following error:

Another application named 'webcenter' exists. Specify the Server on which your application is deployed. Use: server= 'YourServerName '.

Solution
There are multiple applications with the same name in the domain in which you are trying to register your application. This usually happens in a cluster environment, where the same application is deployed to multiple managed servers. If this is the case, specify the name of the server in which you are trying to register this application. For example, run the registerWSRPProducer WLST command with the server argument:

```
registerWSRPProducer(appName='myApp', name='MyWSRPSamples', url='http://host:port/application_name/portlets/wsrp2?WSDL', server=server_name)
```

Related Links
The following document provides additional information related to the subject discussed in this section:

- For command syntax and examples, see "registerWSRPProducer" in the Oracle Fusion Middleware WebLogic Scripting Tool Command Reference.

7.8.8 GST Validation Fails During Import of Group Space Template

Problem
The import of Group Space Templates fails with the following error:

```
[oracle.apps.ad.rupconfig.Online_Preverfication] [tid: 5] [ecid: 0000KJNbPbF8Hv_LTQ9Dic1JA0m300006,0] CFGLOG-00169 : Step "Group Space Template" failed.[]
```

Solution
If you use Oracle Web Center Collaboration Server, you must resolve the issues that resulted in these errors. Otherwise, perform the following steps to skip the GST validation.

1. `cd $Inventory_Loc/checkpoint/farup/11.1.8.0.0`
2. Back up the checkpoint.xml file.
4. Resume orchestration. The Online Preverification proceeds by skipping GST validation and completes the rest of the checks in the configuration assistant. The runSecondRUPInstaller plug-in will then fail due to the GST failure. Review all logs to confirm the configuration assistant was successful,
5. Update the runSecondRUPInstaller plug-in to success.
7.8.9 Configuration Assistant Fails Due to "Could not create credential store instance"

**Error**

**Problem**
A configuration assistant fails with the following error:

JPS-01055: Could not create credential store instance.
Reason: java.io.IO Exception: PKI-02002: Unable to open the wallet. Check password.

**Solution**
Restart Upgrade Orchestrator.

7.8.10 First Installer Fails on Primordial Host During Applying Middleware Patchsets

**Problem**
The first installer fails on the primordial host with the following exception reported in /u01/instance/lcm/log/11.1.8.0.0/RUP/fapatch_Applying_Middleware_Patchsets_timestamp.log.

((Internal Error: File Copy failed. Aborting Install
ERROR: Failed Job ID 12
ERROR: jobs failed during Applying Middleware Patchsets))


The following error is also reported in the Installer logs using the timestamp in the previous log file, under /u01/inventory/admin-apps.oracleoutsourcing.com/oraInventory/logs.

OUI exception. oracle.sysman.oii.oic.OicInstallAPIException: OUI-10022: The target area /u01/oim/oraInventory cannot be used because it is in an invalid state.

**Solution**
Resume Upgrade Orchestrator on the primordial nodes to proceed with the upgrade.

7.8.11 Importing Oracle Data Integrator Repositories Fails

**Problem**
The second installer fails while running the Import Oracle Data Integrator Repositories configuration assistant when it is run in checkpointing mode, and when the 'Offline Preverification' step was run in a previous session of the installer. The following message is reported.
odi.core.security.internal.ODIJpsHelper.createSubject Get exception.
User:FUSION_APPS_PROV_PATCH_APPID. Exception msg is:
java.lang.NoClassDefFoundError: javax/security/jacc/PolicyContext

Solution
1. Back up the existing checkpoint file at
   /u01/inventory/hostname/oraInventory/checkpoint/farup/11.1.8.0.0/checkpoint.xml
   to a different location.
2. In the checkpoint.xml file, look for <aggregate name="Offline Preverification" status="success"/>
3. Update the line to set the status to "fail" and then save the file.
4. Resume orchestration.

7.8.12 Creating Middleware Schema Fails

Problem
The Create Middleware Schema configuration assistant fails.

Solution
You cannot retry the Create Middleware Schema configuration assistant after a failure. You must restore your environment from a backup and then restart the upgrade.

7.9 Troubleshooting Node Manager and OPMN failures

- Verifying Node Manager and OPMN Status Fails Due to Bad Certificate Issue
- Stopping OPMN Processes Fails
- Verifying Node Manager and OPMN Status Fails
- Node Manager Does Not Start Between First and Second Installer

7.9.1 Verifying Node Manager and OPMN Status Fails Due to Bad Certificate Issue

Problem
Verifying Node Manager and OPMS Status fails with the following error:
WLSTException: Error occured while performing nmConnect :
Cannot connect to Node Manager. :
[Security:090542]Certificate chain received from <hostname> - <host IP address>
was not trusted causing SSL handshake failure.

Solution
The issue can occur when the host associated with a node manager is explicitly bounced in the middle of the upgrade, and if Upgrade Orchestrator expects the node manager to be in a shutdown state at that time. Node manager on the host may be configured to automatically start up as part of the system boot process and could cause various issues depending on which upgrade step was being performed when the host was restarted. To resolve this issue, stop and restart node manager on the host where the issue was reported.
7.9.2 Stopping OPMN Processes Fails

**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


7.9.3 Verifying Node Manager and OPMN Status Fails

**Problem**
The Verifying Node Manager and OPMN Status configuration assistant fails.

**Solution**
Do not exit out of Upgrade Orchestrator in response to this configuration assistant failure. Perform the following steps to recover:

1. Review the node manager log files to determine the cause of the failure:
   APPLICATIONS_CONFIG/nodemanager/host_name/
   Note that the APPLICATIONS_CONFIG value can be obtained from the APPLICATIONS_BASE/fusionapps/faInst.loc file.

2. After you resolve the issue that caused the failure, start the Node Manager on all hosts that are part of the Oracle Fusion Applications provisioned system. For more information, see "Task 3: Start Node Manager" in the Oracle Fusion Applications Administrator’s Guide.

3. Restart the OPMN server for BI, GOP (if GOP is installed), and Web Tier. If you run the Web Tier (OHS) installed with the Oracle Fusion Applications middle tier, you can start it using the following steps. If you run the Web Tier on a separate machine, you may be able to run the steps below on the other machine. In either case, ensure that Web Tier (OHS) is up at this point.
   
   Example for BI: (note the usage of start instead of startall)
   
   cd APPLICATIONS_CONFIG/BIInstance/bin
   ./opmnctl start
Example for GOP: (note the usage of `start` instead of `startall`) Note that the OPMN server for GOP should be started from the machine that hosts the Supply Chain Management Administration Server domain. Start the OPMN server for GOP only if you have GOP installed.

```bash
cd APPLICATIONS_CONFIG/gop_1/bin
./opmnctl start
```

Example for Web Tier: (note the usage of `start` instead of `startall`)

```bash
cd APPLICATIONS_CONFIG/CommonDomain_webtier/bin
./opmnctl start
```

For more information about the location of `APPLICATIONS_BASE` and `APPLICATIONS_CONFIG`, see Section 2.1, "Before You Begin".

The BI and Web Tier processes managed by OPMN are started by RUP Installer in the Starting All Servers configuration assistant. The GOP processes managed by OPMN must be started using Fusion Applications Control, as described in Section 5.2.6, "Start External Servers", after RUP Installer completes.

4. Fix any other environment issues before resuming the upgrade. If RUP Installer exits for any reason, make sure that all node managers and OPMN processes are running. Contact Oracle Support Services to proceed out of this step if you have unresolved environment issues.

5. After you start the services, resume orchestration to proceed to the Starting All Servers configuration assistant. If the starting of servers times out, see Section 7.15, "Troubleshooting Server Start and Stop Failures".

---

**Note:** If GOP is not installed, the user interface reports "Success" for GOP OPMN status, but the log file reports: GOP is not provisioned. Skipping check for OPMN status.

---

### 7.9.4 Node Manager Does Not Start Between First and Second Installer

This section describes two scenarios that can prevent the node manager from starting between the first and second installer.

#### Problem

The node manager was manually started before or during the Extending Certification Validity configuration assistant. The node manager caches the previous keystore certificates so the updated certificates are not validated and the node manager fails to start.

#### Solution

Check the node manager logs to determine if it is running and when it was last started. If the time stamp is earlier than the Extending Certification Validity configuration assistant execution time stamp, you must restart the node manager so that it reads the updated keystore certificates.

1. To find out if the node manager is running for a specific host, connect to the host and run the following command. If any results are returned, the node manager is running.

   ```bash
   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_Viability_XXXX file in one of the following directories.
   APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/RUP/configlogs
   APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/RUP/ARCHIVE/timestamp/configlogs

   The last time stamp entry is the execution timestamp.

**Problem**
The administration servers in one or more domains are running before the **Extending Certification Validity** configuration assistant runs. This prevents validation of the updated keystore certificates and fails to provide the correct status to orchestration.

**Solution**
Perform the following steps:

1. Verify whether the administration server of the domain is running by launching the administration console of the domain. If the console comes up, then the administration server is running.

2. Verify the last time the administration server was started. Go to the APPLICATIONS_CONFIG/domains/logical_host_name/domain_name/servers/AdminServer/logs directory. Using the command, ls -lrt, find the most recent the AdminServer.log file. In this file, find the time of 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.>

### 7.10 Troubleshooting RUP Lite for OHS Failures

The following RUP Lite for OHS failures are described:

- RUP Lite for OHS Fails With Missing JDK exception
- RUP Lite for OHS Fails With ReassociateCommonDomain Plug-in
- RUP Lite for OHS Fails With Security Mode Errors

#### 7.10.1 RUP Lite for OHS Fails With Missing JDK exception

**Problem**
RUP Lite for OHS fails during the ohs.plugin.UpgradeWebtier step due to missing the jdk directory.

**Solution**
Verify if there is a jdk_backup_existing_version directory under WT_ORACLE_HOME. If this directory exists, rename it to jdk and resume Orchestration.
Also, if the missing jdk directory is from \texttt{WT_MW_HOME/oracle_common}, check to see if there is a \texttt{jdk_backup_existing_version} directory under this directory. If so, rename it to jdk and resume Orchestration.

### 7.10.2 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 \texttt{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.

### 7.10.3 RUP Lite for OHS Fails With Security Mode Errors

**Problem**
RUP Lite for OHS reports a server side error with an error message such as:

Server instance is not running for the security mode specified: “simple”. Try again using a different security mode. The remote registration process did not succeed! Please find the specific error message below.

**Solution**
Perform the following steps to resolve the issue.

1. Log in to the OAM administration console.
2. From the System Configuration tab, click Server Instances, and double click the OAM server instance, such as, oam_server1.
3. Select "simple" from the Mode field in the right panel.
4. Click Apply to submit the changes.
5. Restart the OAM Server.
6. Restart all OHS servers in the environment.
7. Resume Upgrade Orchestrator.

---

**Note:** Check the Oracle Fusion Applications OHS to ensure that SSO still works after the change. If it does not, you must upgrade Webgate manually for the Oracle Fusion Applications OHS.

### 7.11 Troubleshooting IDM Upgrade Failures

This section provides the following troubleshooting information related to upgrading Oracle Identity Management:

- Communication Exceptions on Primordial Console While Waiting for IDMOHS
- WLS Exception - ESS Server Does Not Respond During Start all Servers
Troubleshooting IDM Upgrade Failures

- OAM Configuration Step Fails Due to Special Characters in Password
- Location of GRC Policies in the OAM Applications Domain
- Oracle Identity Federation Application Does Not Start and config.xml is Empty

7.11.1 Communication Exceptions on Primordial Console While Waiting for IDMOHS

**Problem**
While PRIMORDIAL is waiting for IDMOHS:IDMUpgradeDone, there are communication exceptions on the PRIMORDIAL console.

**Solution**
These errors can be ignored and Orchestration can be resumed.

7.11.2 WLS Exception - ESS Server Does Not Respond During Start all Servers

**Problem**
The Starting All Servers configuration assistant in RUP Installer fails to start ess_server1 and reports the following error in the ess_server1.log:

```
weblogic.rmi.extensions.DisconnectMonitorUnavailableException: Could not register a DisconnectListener
```

**Solution**
Perform the following steps to resolve this issue:

1. Open the Oracle Enterprise Manager console for the domain.
2. Navigate to following location:
   - From the console, expand the WebLogic Domain
   - Go to ESSCluster, then ess_server1
   - Right click and open System MBean browser
   - Go to ess_server1, ServerStart, select ess_server1, and click Arguments
3. Verify if `-Doracle.ess.initialProcessorState=stopped` is present. If it is, remove `-Doracle.ess.initialProcessorState=stopped` and click Apply. If it is not present, there is no action to take.

7.11.3 OAM Configuration Step Fails Due to Special Characters in Password

If the OAM administrator password contains special characters, such as '#' or '&', the OAM Configuration step will fail. To work around this issue, you can manually validate that the OAM Administration Server host/port and surname/password are correct. After you manually validate this information, you can proceed with the upgrade by resuming orchestration.

Perform the following steps to validate.

1. Get the OAM administrator user name and password from the credential store.
2. Run `APPLICATIONS_BASE/fusionapps/oracle_common/common/bin/wlst.sh`. 

---

Monitoring and Troubleshooting the Upgrade  7-29
3. Run the following commands to connect to the Common Domain Administration Server and get the OAM administrator surname and password:

   ```
   connect()
   listCred(map='oracle.patching', key='FUSION_APPS_PATCH_OAM_ADMIN-KEY')
   ```

4. Get the OAM Administration Server host and port from the following properties in `APPLICATIONS_CONFIG/fapatch/FUSION_prov.properties`:
   - `OAM_ADMIN_SERVER_HOST`
   - `OAM_ADMIN_SERVER_PORT`

5. Use `oamcfgtool.jar` to confirm whether the OAM server can be invoked using the values found in the previous steps.

   ```
   cd APPLICATIONS_BASE/fusionapps/oracle_common/modules/oracle.oamprovider_11.1.1
   java -jar oamcfgtool.jar app_domain=crm web_domain=OraFusionApp
   uris_file=APPLICATIONS_BASE/fusionapps/applications/crm/security/oam.conf
   oam_aaa_mode=open_or_simple app_agent_password=password_for_ map="oracle.patching"
   key='FUSION_APPS_PATCH_OAM_ADMIN-KEY' in_credential_store
   primary_oam_servers=oam_server1 oam_admin_server=http://OAM_admin_server_
   host:port
   oam_admin_username=username_for_FUSION_APPS_PATCH_OAM_ADMIN-KEY
   oam_admin_password=password_for_FUSION_APPS_PATCH_OAM_ADMIN-KEY
   oam_version=11 default_authn_scheme=FAAuthScheme
   ```

6. If the previous command is successful, the validation is successful and you can resume orchestration.

**7.11.4 Location of GRC Policies in the OAM Applications Domain**

The location of your Governance, Risk, and Compliance (GRC) policies varies, depending on your upgrade path to Release 8. GRC policies are located in the grc OAM application domain if your Oracle Fusion Applications environment was originally provisioned with either version 11.1.1.5 or 11.1.2, then upgraded to version 11.1.3, and then upgraded to version 11.1.4. If your environment was originally provisioned with version 11.1.3 and upgraded to version 11.1.4, your GRC policies are located in the fs OAM application domain.

**7.11.5 Oracle Identity Federation Application Does Not Start and config.xml is Empty**

**Problem**

The IDM upgrade fails with an error on Oracle Identity Federation (OIF) that it did not start successfully and the OIF `config.xml` file is empty. An error is reported in the IDM upgrade logs, as shown in the following example.

```
```

An error is also reported in the WLS logs, as shown in the following example.

```
'<Jan 8, 2014 2:06:09 AM UTC> <Error> <Default> <J2EE JMX-46030> <failure to register MBean> "com.oracle.security.fed:name=ServerConfig,type=OIFConfigMBean,Application=OIF,App'
Solution
Perform the following steps to resolve this failure:

1. Shut down OIF.
2. Delete config.xml from the following directory: u01/oim/user_projects/domains/oim_domain/config/fmwconfig/servers/wls_oif1/applications/OIF_11.1.1.2.0/configuration.
3. Copy config.xml.bak to config.xml, in the same directory used in Step 2.
4. Make a backup copy of config.xml.bak.
5. Start OIF.
6. Resume orchestration to restart the IDM upgrade.

7.12 Troubleshooting Applying Middleware Patches

This section provides the following troubleshooting information related to the Applying Pre-PSA Middleware Patches or Applying Post-PSA Middleware Patches configuration assistants:

- Log Files for Applying Middleware Patches
- Applying 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

7.12.1 Log Files for Applying Middleware Patches

Problem
An error occurred during the Applying Pre-PSA Middleware Patches or Applying Post-PSA Middleware Patches configuration assistant.

Solution
Review the log file in the relevant location to find the cause of the error:

APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/RUP/ApplyPrePSAMiddlewarePatchestimestamp.log

APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/RUP/ApplyPostPSAMiddlewarePatchestimestamp.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.
7.12.2 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: 0000JaNml6AxG0pIww0yiHRacu000006,0] 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.

7.12.3 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. You can resolve this issue by following the steps in Section 7.13, "Troubleshooting Loading Database Components". Run the commands from ATGPF_ORACLE_HOME instead of FA_ORACLE_HOME.

7.12.4 Applying Database Client Patches Fails

**Problem**
The following error occurs:

```
OPatch cannot continue because it can't load library from the directory '
```

**Solution**
This error may occur if the OUI version in the database client Oracle home is 11.2 while the OUI version in Oracle Fusion Applications Oracle home (FA_ORACLE_HOME) is 11.1.

Perform the following steps to resolve this issue:

1. Go to the DB Client home.
2. Set the ORACLE_HOME environment variable to point to the database client Oracle home.
3. Apply the database client patches using the following command:
```
$ORACLE_HOME/OPatch/opatch apply patch_location
```
4. Because the patches have now been manually applied, perform the following steps to continue with the upgrade:
   a. Go to the FA_ORACLE_HOME/fusionapps/applications/lcm/tp/config/RUP/FMW directory.
b. Open the pre-psa-jobs.xml file for editing.

c. Comment out the job with the name dbclient. An example of this job follows.

```
<!-- <job>
  <id>10</id>
  <target>FAMW</target>
  <component>
    <name>dbclient</name>
    <version>11.1.1.5</version>
    <component>
      <utility_name>opatch</utility_name>
      <patch_number>NA</patch_number>
      <command>%opatch% napply -silent -skip_duplicate -skip_subset
      -oh %dbclient_home% -phBaseDir %dbclient_patch% -jre %jre_loc% -invPtrLoc
      %oraInstLocFile%</command>
      <patch_location>NA</patch_location>
    </component>
  </component>
</job>
```

d. Save the pre-psa-jobs.xml.

e. Resume orchestration or retry RUP Installer.

f. Modify the custom reports per the new folder structure and attribute names.

### 7.12.5 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.

### 7.12.6 Upgrading Middleware Schema Fails

**Problem**
An error occurred during the Upgrading Middleware Schema configuration assistant.

**Solution**
Review the log file in this location to find the cause of the error:

fusionapps/oracle_common/upgrade/logs/psatimestamp.log

**Problem**
The Upgrading Middleware Schema configuration assistant fails because JAVA_HOME cannot be found.
Solution
Set the JAVA_HOME and then manually run the upgrade for the failed schema, as shown in the following example:

```
export JAVA_HOME=/u01/APPLTOP/fusionapps/jdk6
/u01/APPLTOP/fusionapps/oracle_common/bin/psa -response
/u01/APPLTOP/fusionapps/applications/admin/FUSION/oui_resp/psa_response_crm.txt
```

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: 0000K8DIf519xWR5IZL6if1ISVu^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
Perform the following steps to resolve this issue.

1. Connect as searchsys.
2. DROP INDEX "SEARCHSYS"."EQ$DOC_PATH_IDX" force;
3. exec eq_adm.use_instance(1)
4. exec eq_ddl.create_index()
5. Resume orchestration.

7.12.7 Applying Downloaded Patches Fails

Problem
The Applying Downloaded Patches configuration assistant failed with the following error:

```
Stack Description: java.lang.RuntimeException:
PatchObject constructor: Input file */net/server01/Downloaded_Patches/atgpf/patch/1234567/etc
/config/inventory* does not exist.
```

Solution
This type of error occurs when you do not download the patches to the appropriate directory. To resolve this issue, copy the patches to the correct directory and resume orchestration.

7.13 Troubleshooting Loading Database Components

This section contains information about troubleshooting issues that may occur during the Loading Database Components configuration assistant. Depending on the type of failure, you may need to review one or more of the log files in the following locations:

- `APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/RUP/PatchManager_DBPatch/`
The following troubleshooting issues are described in this section:

- Failure During Granting Privileges
- Workers Fail While Loading Database Components
- Database Failure While Loading Database Components
- AutoPatch Validation Fails
- Flexfield Seed Data Upload Fails
- Applying Downloaded Patches Fails
- Loading Database Components Fails When JDBC URL is Null
- Active FAPatchMgr Sessions Are Found
- Patch Manager Fails Due to Unique Constraint While Running Abort

### 7.13.1 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**
You can find the cause of the failure by running the script manually as the sysdba user, using SQL*Plus or SQL*Developer. After you resolve the issue, resume orchestration.

### 7.13.2 Workers Fail While Loading Database Components

**Problem**
You receive an email notification stating that one or more database workers failed during the Loading Database Components configuration assistant.

**Solution**
You receive this email notification only when the upgrade cannot progress any further and requires user intervention. In this scenario, all the workers are in a FAILED or IDLE status. The configuration assistant remains in a RUNNING status until all tasks in Loading Database Components have run. To resolve this issue, you must start AD Controller to manage the failed workers. For additional information, see "Troubleshooting Patching Sessions for Database Content" in the Oracle Fusion Applications Patching Guide. After you resolve the issue that caused the workers to fail, and restart the workers, Upgrade Orchestrator continues processing. No further intervention is required.

Note that the messages are displayed on the console for database component failures if you run orchestration with the -DlogLevel option set to FINEST.
There might be corner cases when you might receive an alert email indicating failed workers although the workers are still running. In such cases, you can ignore the email alert after ensuring the workers are running with no failures.

7.13.3 Database Failure While Loading Database Components

**Problem**

Your database goes down while RUP Installer is running the **Loading Database Components** configuration assistant. If you simply bring the database up and then resume orchestration, you may encounter the following error:

Failed to connect to the database as fusion with error:
No more data to read from socket

**Solution**

Perform the following steps to recover from this error:

1. Force the database patching session to fail.
   
   (UNIX) `FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh forcefail`
   
   (Windows) `FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd forcefail`
   
2. Start AD Controller.
   
   (UNIX) `FA_ORACLE_HOME/lcm/ad/bin/adctrl.sh`
   
   (Windows) `FA_ORACLE_HOME\lcm\ad\bin\adctrl.cmd`
   
   For more information, see "Starting AD Controller" in the [Oracle Fusion Applications Patching Guide](#).

3. Follow this sequence of steps in AD Controller to manage the workers:

   a. Select **Tell manager that a worker failed its job** and enter **All** for all workers.
   
   b. Select **Tell worker to quit** and enter **All** for all workers. Note that this does not kill the workers. It sends a command to the worker to shutdown after it completes the current task.
   
   c. Wait for all workers to complete their tasks and shut down normally.
   
   d. If there are still some worker processes that do not shut down, kill those processes manually by selecting **Tell manager that a worker failed its job**. Then select **Tell manager that a worker acknowledges quit** and enter **All** for all workers.
   
   e. From your operating system, check for processes that are running `fapmgr`, `javaworker`, `adpatch`, `adadmin`, `sqlplus`, and `adworker`. If any exist, terminate them from your operating system.
   
   f. Select **Tell worker to restart a failed job** and enter **All** for all workers.

4. Resume orchestration.

7.13.4 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.
   (UNIX) `FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh forcefail [-logfile log file name] [-loglevel level]`
   (Windows) `FA_ORACLE_HOME/lcm/ad/bin/fapmgr.cmd forcefail [-logfile log file name] [-loglevel level]`

2. Run the `fapmgr abort` command from `FA_ORACLE_HOME` to find out if an Oracle Fusion Applications Patch Manager session must be cleaned up.
   (UNIX) `FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh abort [-logfile log file name] [-logLevel level]`
   (Windows) `FA_ORACLE_HOME/lcm/ad/bin/fapmgr.cmd abort [-logfile log file name] [-logLevel level]`

   If this command finds no failed session, proceed to Step 3.

3. Run the following commands from `ATGPF_ORACLE_HOME` to abandon any Applications Core patching sessions or AD Administration sessions that may be running:
   (UNIX) `ATGPF_ORACLE_HOME/lcm/ad/bin/adpatch.sh abandon=y interactive=n defaultsfile=APPLICATIONS_CONFIG/atgpf/admin/defaults.txt`
   (UNIX) `ATGPF_ORACLE_HOME/lcm/ad/bin/adadmin.sh abandon=y interactive=n defaultsfile=APPLICATIONS_CONFIG/atgpf/admin/defaults.txt`
   (Windows) `ATGPF_ORACLE_HOME\lcm\ad\bin\adpatch.exe abandon=y interactive=n defaultsfile=APPLICATIONS_CONFIG\atgpf\admin\defaults.txt`
   (Windows) `ATGPF_ORACLE_HOME\lcm\ad\bin\adadmin.cmd abandon=y interactive=n defaultsfile=APPLICATIONS_CONFIG\atgpf\admin\defaults.txt`

7.13.5 Flexfield Seed Data Upload Fails

Problem
When multiple seed data files are uploaded for the same flexfield but for different flexfield contexts, the upload tasks can fail due to locking issues. The failed tasks appear in the log file as the following error:

```
Loading failed with a JboException: JBO-25014: Another user has changed the row with primary key oracle.jbo.Key ...
```

Solution
AutoPatch defers any failed tasks to the end of the phase and reattempts the failed tasks only after attempting all tasks in the phase at least once. Usually the flexfield seed data tasks that failed due to the locking issue succeed on subsequent attempts. You can ignore these errors if the flexfield seed data task succeeds on the retry. If the task remains in a failed state, you must use the AD Controller utility to retry the failed task.
For more information, see "Restarting a Failed Worker" in the *Oracle Fusion Applications Patching Guide*. 

### 7.13.6 Loading Database Components Fails When JDBC URL is Null

**Problem**
The *Loading Database Components* configuration assistant fails with the following exception:

```java
[2013-11-20T06:01:53.280+00:00] [] [ERROR] [] [] [tid: 34]
[ecid:0000K9o6OHX6gI25RrtilZ4P100000d,0] java.lang.NullPointerException: Schema @ name/password/ jdbc url cannot be null[

at oracle.apps.ad.common.db.ADDatabaseConnection.createConnection(ADDatabaseConnection.java:529)

at oracle.apps.ad.common.db.ADDatabaseConnection.getConnectionWithCluster(ADDatabaseConnection.java:444)

at oracle.apps.ad.common.db.ADDatabaseConnection.getConnectionWithCluster(ADDatabaseConnection.java:446)

.................................

[2013-11-20T06:15:58+00:00] [apps] [ERROR] []
[oracle.apps.ad.rupconfig.Loading_Database_Components] [tid: 34]
[ecid:0000K9o6OHX6gI25RrtilZ4P100000d,0] [[java.lang.StackOverflowError]]
```

**Solution**
From the command line, run `FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh forcefail`. Then resume orchestration.

### 7.13.7 Active FAPatchMgr Sessions Are Found

**Problem**
In a scenario where fapmgr applies patches using the multi-apply feature, and any patch validation fails, the status is set to 'SUCCESS'. This new status is treated as an active session by Health Checker and it fails, causing an orchestration failure with the error message as shown in the following example:

```
[ERROR]: Plugin 'PatchSessionsAndProcessesCheck': HC-PATCHSP-00004 : Check

#1: Found active FAPMgr sessions. Review log files for details on which Sessions exist. (Pre-Upgrade Checks)
```

**Solution**
Run the following SQL*Plus command in the fusion schema:

```
update AD_PATCH_UTIL_SESSIONS set status='COMPLETED_WITH_WARNINGS' where status='SUCCESS';
```
Resume orchestration.
7.13.8  Patch Manager Fails Due to Unique Constraint While Running Abort

**Problem**
Oracle Fusion Applications Patch Manager fails with the following error:

Failed to run Fusion Applications Patch Manager.
Reason: Failed to create a task in AD_PATCH_UTIL_TASKS.
Reason: Error while querying the database. ORA-00001: unique constraint (FUSION_AD_PATCH_UTIL_TASKS_U2) violated

**Solution**
This error indicates that a patch validation session was incomplete. To resolve the issue, an attempt was made to abandon the session by using the 'abort' option, which failed.

Run the following SQL*Plus statement to fix the data:

Update AD_PATCH_UTIL_SESSIONS set STATUS = 'ABORTED' where STATUS = 'FAILED';

7.14  Troubleshooting 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
- Applications Policies Analysis Fails
- Deploying Applications Policies Fails
- Deploying Applications Policies Reports a Warning
- Deploying Applications Policies Reports a Warning during Migrate Security Store
- IDM Server Fails During Deployment of Applications Policies

7.14.1  Log Files for Deploying Application Policies

Log files for this configuration assistant may be found in this location:

APPLICATIONS_CONFIG/1cm/logs/11.1.8.0.0/RUP/configLogs/fapatch_Deploying_Applications_Policies_(jazn-data.xml)_timestamp.log

7.14.2  Applications Policies Analysis 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/1cm/logs/11.1.8.0.0/RUP and are named as follows:

- fapatch_CRMJaznAnalysis_timestamp.log
- fapatch_FSCMJaznAnalysis_timestamp.log
- fapatch_HCJMaznAnalysis_timestamp.log
- fapatch_OBJJaznAnalysis_timestamp.log
7.14.3 Deploying Applications Policies Fails

**Problem**
A failure occurs during Deploying Application Policies.

**Solution**
When a failure occurs during Deploying Application Policies, you must restore only the stripe or system policy that has failed, from your backup. Use the OPSS migrateSecurityStore command with the appropriate source and destination arguments to perform the restore. Do not restore a stripe that has not failed. Review the JAZN deployment log file to determine the cause of the failure, fapatch_Deploying_Applications_Policies_(jazn-data.xml)_timestamp.log.

After you resolve the issue, resume orchestration.

**Related Link**
The following document provides additional information related to subjects discussed in this section:
- For more information, see "Migrating with the Script migrateSecurityStore" in the Oracle Fusion Middleware Application Security Guide.

7.14.4 Deploying Applications Policies Reports a Warning

**Problem**
The following warning occurs during Deploying Application Policies:


WLS ManagedService is not up running. Fall back to use system properties for configuration.

**Solution**
You can safely ignore this message as there is no functional impact of this warning and the deployment is successful.
7.14.5 Deploying Applications Policies Reports a Warning during Migrate Security Store

**Problem**
The following warning occurs during **Deploying Application Policies**:

```
FINE: Application policies already exists for application: fscm
oracle.security.jps.service.policystore.PolicyObjectAlreadyExistsException:
Cannot create application policy context "fscm".
    at oracle.security.jps.internal.policystore.ldap.LdapPolicyStore.unsync_createApplicationPolicy(LdapPolicyStore.java:933)
    at oracle.security.jps.internal.policystore.ldap.LdapPolicyStore.createApplicationPolicy(LdapPolicyStore.java:753)
    at oracle.security.jps.internal.tools.utility.destination.apibased.JpsDstPolicy.clone(JpsDstPolicy.java:805)
```

**Solution**
You can safely ignore this message as there is no functional impact of this warning and the deployment is successful.

7.14.6 IDM Server Fails During Deployment of Applications Policies

**Problem**
The IDM Server goes down during **Deploying Application Policies** and the deployment fails.

**Solution**
Upgrade Orchestrator does not allow a retry after this type of failure. You must instead exit orchestration and restore from your IDM backup. Then resume orchestration.

7.15 Troubleshooting Server Start and Stop Failures

This section includes the following troubleshooting topics:

- Starting All Servers Fails Due to Time Outs
- Starting All Servers Fails to Start BIServer
- Startup Fails for CommonDomain: OHSComponent (Oracle VM Only)
- Online Preverification Reports EditTimedOutException Error
- Server Startup Reports WLS SocketTimeoutException
- The SOA-infra Application is in a Warning State
- The SOA-infra Application is in a Warning State on All Domains
- Custom Domains Fail to Start or Stop
- StartAllServers Task Fails After Language Pack Upgrade on CRM
7.15.1 Starting All Servers Fails Due to Time Outs

**Problem**
A failure during the Starting All Servers configuration assistant typically happens when one of the servers times out and fails to start due to resource issues or application specific issues.

**Solution**
Various platforms and environment configurations can impact how long it will take all servers to actually start during the Starting All Servers configuration assistant. Although RUP Installer waits an average amount of time for this configuration assistant to complete before it is marked as Failed, different platforms may require more time. It is not unusual to receive timeout errors in the log files if the starting of all servers for your environment requires more time than RUP Installer allows. If this configuration assistant fails, follow these steps:

1. Monitor the status of the servers by reviewing the messages in the server log files or on the console. The log file, APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/RUP/StartStop/fastartstop_timestamp.log, indicates which server started and failed to start.

   An example of messages for a server that timed out follows.

   Time out while performing Start for domain SCMDomain. Waited for 2400 seconds
   [2011-10-21T03:57:52.052-8:00] [fastartstop] [NOTIFICATION:1] [UTIL]
   [oracle.apps.startstop.util.MbeanUtil: runSSCommandOnDomain.868] [tid:37] Start
   operation is completed for domain SCMDomain. Please see SCMDomain.log for
   details.

   [2011-10-21T03:57:52.052-8:00] [fastartstop] [NOTIFICATION:1] [UTIL]
   [oracle.apps.startstop.invoke.StartStopTask: call.221] [tid:37] StartStopTask
   over for domain SCMDomain

   [2011-10-21T03:57:52.052-8:00] [fastartstop] [NOTIFICATION:1] [SST]
   [oracle.apps.startstop.invoke.StartStopTask: call.223] [tid:37] Finished the
   task for the Domain SCMDomain

2. Review the log files at the domain level to see a summary of the server status for that domain: APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/RUP/StartStop/domain name_timestamp.log.

3. Review the corresponding server logs for the failed servers under the following directory: APPLICATIONS_CONFIG/domains/hostname/domain name/servers/server name/logs.

4. After you determine and resolve the cause of the failure, restart Upgrade Orchestrator.

7.15.2 Starting All Servers Fails to Start BIServer

**Problem**
The following exception during the Starting all Servers configuration action indicates a failure in starting the BIServer:

Start all servers fails to start
Start operation on the component :coreapplication_obips1:, for the instance
:BIInstance: - FAILED
The coreapplication_obips1 server log file reports the following error:

```
ecid:]
[2012-04-10T00:22:20.000-07:00] [OBIPS] [ERROR:16] []
saw.security.odbcuserpopulationimpl.initialize [ecid: ] [tid: ] Unable to create a system user connection to BI Server during start up. Trying again.[]
File:odbcuserpoploaderimpl.cpp
Line:325
Location:
saw.security.odbcuserpopulationimpl.initialize
saw.catalog.local.loadCatalog
saw.subsystems.catalogbootstrapper.loadcatalog
saw.webextensionbase.init
saw.sawserver
ecid:]
```

```
[2012-04-10T00:22:25.000-07:00] [OBIPS] [NOTIFICATION:1] []
saw.sawserver
ecid:]
```

**Solution**

Perform the following steps to work around this issue.

1. Resume orchestration, which shuts down and starts bi_server1.
2. Monitor the faststartstop log files and the state of bi_server1(BIDomain).
3. As soon as bi_server1 restarts, as indicated by a RUNNING status, start the component coreapplication_obiccs1 or all the components of type OracleBIClusterControllerComponent using opmnctl.

Example syntax follows:

```
*/BIInstance/bin/opmnctl startproc ias-component=coreapplication_obiccs1
```

### 7.15.3 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.config, for example:

   ```
   LockFile "/u101/ohs_inst1/diagnostics/logs/OHS/ohs1/http_lock"
   ```
2. Confirm whether the directory that contains the lock file exists.
3. Assuming this directory does not exist, create the directory.
7.15.4 Online Preverification Reports EditTimedOutException Error

**Problem**
The following error is reported during Online Preverification:
weblogic.management.mbeanservers.edit.EditTimedOutException

**Solution**
You may have to manually release the edit session. For more information, see "Resolving an EditTimedOutException Error" in the Oracle Fusion Applications Patching Guide.

7.15.5 Server Startup Reports WLS SocketTimeoutException

**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.

7.15.6 The SOA-infra Application is in a Warning State

**Problem**
After the upgrade, the following error displays after you log in to the WLS Console of CommonDomain and navigate to Deployments:
soa-infra application is in WARNING state.

**Solution**
You can ignore this error as there is no functional impact for SOA users due to this error.

7.15.7 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.
7.15.8 Custom Domains Fail to Start or Stop

**Problem**
Your 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 you resume orchestration.

7.15.9 StartAllServers Task Fails After Language Pack Upgrade on CRM

**Problem**
Orchestration tries to restart all servers after a Language Pack upgrade. On CRM PODs, there may be failures in starting the IIR server, which may be reported as the following error:

`ORCH-DOWNTIME-SS-00005 : Failed to start all servers. Review log file /u01/APPLTOP/instance/lcm/logs/11.1.8.0.0/orchestration/host_name-rel8_midtier_timestamp.log for details on the failures to take appropriate corrective action. (Bounce All Servers).`

**Solution**
Perform the following steps.

1. Review the orchestration log file at `/u01/APPLTOP/instance/lcm/logs/11.1.8.n.n/orchestration/hostname-rel8_midtier_timestamp.log, and check for any failures.
2. Review all fa_control logs on the failed host and look for details on the server that failed.
3. If the IIR server is the only server that failed to start, update the status of the task to Success using the following `updateStatus` command, and resume Upgrade Orchestrator. You can restart the IIR server manually after the upgrade.

   `/orchestration.sh updateStatus -pod POD_NAME -hosttype host_type -hostname host_name -release 11.1.8.n.n -phase DowntimePostLP -taskid StartSeversAfterLP -taskstatus success`

7.16 Troubleshooting SOA Composite Deployment Failures

This section describes how to recover from failures during the Deploying SOA Composites configuration assistant. The following topics are described:

- SOA Composite Log Files
- SOA Composite Failure Does Not Recover
- Wsm-pm Application is not Running in Domain (Solaris Only)
- Manually Deploying SOA Composites
- Invoking an Instance of SOA Composite
- Merging SOA Composite JDeveloper Customizations During SOA Preverification
7.16.1 SOA Composite Log Files

The following log files are generated by the deployment of SOA composites:

- Client side log files where individual domain logs reside: APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/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

7.16.2 SOA Composite Failure Does Not Recover

Problem

Normally, a failed SOA composite is undeployed by RUP Installer. However, if the failure of the deployment is due to an issue such as SOA servers running out of memory, then RUP Installer does not recover until you resume orchestration.

Examples of error messages related to SOA Composite failures follow:

CFGLOG-00380: SOA composite "composite_name" patch failed for server "server_name". Recovery process also failed with an unknown reason. If the SOA composite patch exists on the server, it will be automatically undeployed during retry or a checkpoint run. Also if the base composite is not the default composite, it will be automatically set as default.

CFGLOG-00327: SOA composite "composite_name" patch failed for server "server_name". Recovery process also failed, and the composite patch is not undeployed. The patch will be automatically undeployed during retry or a checkpoint run.

CFGLOG-00328: SOA composite "composite_name" patch failed for server "server_name". Recovery process also failed, and the base composite is not set as the default composite. The base composite will be automatically set as default during retry or a checkpoint run.

Examples of report exceptions follow:

CFGEX-00087: SOA composite "composite_name" patch failed for server "server_name". Recovery process also failed. Recovery will be done automatically during retry or a checkpoint run.
Action : No action required.

CFGEX-00073: SOA composite "composite_name" patch failed for server "server_name".
Action : See logs for details.
Solution
When patching existing SOA composites, RUP Installer automatically recovers any partially deployed SOA composites after failure when you restart Upgrade Orchestrator. The following actions can be performed by Upgrade Orchestrator:

- Undeploy the partially deployed SOA composite revision if it is still present.
- Set as default the same SOA composite revision that was default before the patching was attempted, if it’s not already set as default.

If the failure was caused by an environment issue, such as running out of memory, resolve the cause of the failure before you restart RUP Installer.

7.16.3 Wsm-pm Application is not Running in Domain (Solaris Only)

Problem
The following error is reported during SOA Composite deployment on a Solaris platform:

CFGEX-00079 : Wsm-pm application is not running in domain "domain name"

You have already confirmed that the wsm-pm application is running on this domain.

Solution
Perform the following steps:

1. Log in to the failed domain and check the health of all managed servers and deployed applications.
2. Bounce all managed servers of the failed domains.
3. Exit Upgrade Orchestrator.
4. Restart Upgrade Orchestrator.

7.16.4 Manually Deploying SOA Composites

If a customized SOA composite deployment fails during the upgrade, you must manually deploy this composite using WLST commands.

To apply a SOA composite manually after a deployment failure
In the following steps, the example composite, FinAp, is patched from revision 1.0 to revision 2.0 and the SAR file of revision 2.0 is in $FA_ORACLE_HOME/crm/deploy/sca_FinAp_rev2.0.jar.

Note that the parameters are for illustration purposes only.

1. Refer to the Diagnostics report to find the name and location of the sca_*.jar file that was copied to $FA_ORACLE_HOME by Oracle Fusion Applications Patch Manager. For more information, see "Diagnostics Report" in the Oracle Fusion Applications Patching Guide.
2. If the previous revision contained JDeveloper customizations, ensure that you deploy the patched revision with the merged JDeveloper customizations. Using the sca_*.jar file from Step 1, follow the JDeveloper customization merge instructions that are described in Section 7.16.6, "Merging SOA Composite JDeveloper Customizations During SOA Preverification". Then use the merged sca_*.jar for Step 3.
3. Deploy the patched composite using the single patch composite command.
sca_patchComposite('SOA-Infra URL', user, password, '/FA_ORACLE_HOME/crm/deploy/sca_FinAprev2.0.jar', mergeLogFile='/tmp/merge-log.txt')

7.16.5 Invoking an Instance of SOA Composite
You must run the UpdateSOAMDS SOA composite on every domain if you made any flexfield changes, by following the steps described in "Task: Synchronizing Customized Flexfields in the MDS Repository for SOA" in the Oracle Fusion Applications Extensibility Guide for Developers.

7.16.6 Merging SOA Composite JDeveloper Customizations During SOA Preverification
If you performed JDeveloper customizations to a SOA composite and you deployed the composite to the SOA runtime, RUP Installer reports an error during SOA Preverification, which instructs you to take the newer version of the composite that is in the release. You must then merge your customizations by performing the following steps.

1. If any customizations are detected, the SOA Preverification results display the SOA composite name, its location in the FA_ORACLE_HOME/stripe/deploy directory, and the requirement for you to merge JDeveloper customizations into the sca_*.jar file in FA_ORACLE_HOME before proceeding with RUP Installer. The stripe in the directory path refers to crm, hcm, fscm, and so on.

2. Open the custom SOA workshops and the customized version of the Fusion Applications SOA composite in JDeveloper using "Oracle Fusion Applications Developer".

3. Import the composite sca_*.jar file from FA_ORACLE_HOME/stripe/deploy into the project, for example revision 11.1.8.0.0, in JDeveloper. Make note of this revision number in the deployment window because you will need it in Step 8.

4. Restart JDeveloper in the Oracle Fusion Applications Administrator Customization role.

5. Verify that there are no errors in JDeveloper.

6. Verify that the changes introduced in both the customized version and the patched version are present.

7. Right-click the composite project in the Application Navigator, select Deploy, select the composite, click Deploy to SAR, and click Next.

8. Manually change the value in New Revision ID to the revision from Step 3, for example, 11.1.8.0.0, and click Finish.

9. If the deployment folder is set to a location different from that of the FA_ORACLE_HOME/stripe/deploy directory, copy and replace the JAR in the location mentioned in the error message of this SOA Composite. If your file name is different, rename it to the original name. You must copy the jar in the correct format to FA_ORACLE_HOME/stripe/deploy. For example if you have sca_ContractsDeliverablePurchaseDocAttrReadComposite_rev11.1.8.0.0.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.
Related Links

The following documents provide additional information related to subjects discussed in this section:

- For more information about working with SOA composites, see "Customizing SOA Composite Applications with JDeveloper" 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.

7.17 Troubleshooting RUP Lite for OVM Failures

This section contains the following topics:

- Troubleshooting RUP Lite for OVM Plug-in Failures
- RUP Lite for OVM Hangs During Domain Configuration

7.17.1 Troubleshooting RUP Lite for OVM Plug-in Failures

Review the `/u01/lcm/rupliteovm/output/logs/ruplite.log` file to confirm there are no errors. You can also check rehydration framework logs under `/assemblybuilder/logs` or `/var/log` for any errors.

Review the following troubleshooting information for specific plug-ins:

- **DeployECSF**: This plug-in is re-runnable. If your environment was originally provisioned before Release 5, you can verify that this plug-in was successful by confirming that the help object, schedule and group being deployed are reported in the log file. You can also use Fusion Applications Control to connect to the Administration Server that hosts the search application and confirm that the Help instance artifacts are deployed.

- **ValidateEnvironment**: If this plug-in fails, RUP Lite for OVM stops. You must resolve any errors reported in the log file and then run RUP Lite for OVM again.

- **SetupCredentials**: If this plug-in fails, RUP Lite for OVM stops. Typical causes of failure are an incorrect key for an existing wallet, or specifying a key for a new wallet that does not meet Oracle's minimum standards. You must resolve any errors reported in the log file and then run RUP Lite for OVM again.

  Note that you are prompted for the password twice and that both responses must be identical. If you need to change the password in the wallet, set the `ovm.plugin.SetupCredentials.enable_password_update` property to true. If this property is enabled, when the `SetupCredentials` plug-in reruns, you are given the option to overwrite the existing password for a particular plug-in, in the wallet. By default this feature is disabled.

- **ApplyMemorySettings**: Check the `fusionapps_start_params.properties` files in the environment, which are located under the `bin` directory of each domain. Ensure that the `minmaxmemory` settings in the files are at least as high as the settings in the template under the `ovm/metadata` directory that corresponds to the environment's topology.

- **GenerateOptimizedQueryPlans**: This plug-in is re-runnable. Verify this plug-in was successful by connecting to the database as `fusion_mds` and running the following command:

    ```sql
    SELECT TO_CHAR(last_analyzed, 'yyyy/mm/dd hh:mm:ss am') as last_analyzed FROM`
user_tables;

The results should show that the tables were just analyzed.

- **UpdateODIUnicastConfiguration**: This plug-in is re-runnable. Verify this plug-in was successful by confirming that the config.xml for each domain under the admin-apps directory of the FA node that contains odi_server1 and odi_serverHA, such as CRMDomain, contains the correct coherence start properties.

- **UpdateFusionIIRScripts**: This plug-in is re-runnable. Check the /u01/APPLTOP/InformaticaIR/bin directory to make sure that the updated versions of fusioniirDiag.sh and fusiondqhealthcheck.sh are available.

### 7.17.2 RUP Lite for OVM Hangs During Domain Configuration

**Problem**
RUP Lite for OVM runs for a long time during domain configuration.

**Solution**
Perform the following steps to resolve this issue:

1. Ensure that the IDM host is accessible and responding.
2. Ensure that the database is accessible and responding.
3. If either the IDM host or the database is not responding, update the status of the orchestration task that runs RUP Lite for OVM to "Error", using the following command:
   ```bash
cd ORCH_LOCATION/bin
./orchestration.sh updateStatus -pod POD_NAME -hosttype host_type -hostname host_name -release release_number -phase phase_name -taskid plugin_name -taskstatus Error
```

Fix the issue with the IDM host or the database and resume Upgrade Orchestrator.

4. If none of the above steps solve the problem, contact Oracle Support with detailed log information.

### 7.18 Troubleshooting Health Checker Failures and Errors

This section contains the following topics:

- **Upgrade Readiness Checks Fail During Pre-Downtime**
- **DomainsFileOwnership Health Check Fails With Permissions Issues**
- **Context Root Check Health Check Fails**
- **Resolve JAZN Conflicts Found by Health Checker**
- **Failure Due to oracle.sysman.oii.oiit.OiitTargetLockNotAvailable Exception**

#### 7.18.1 Upgrade Readiness Checks Fail During Pre-Downtime

**Problem**
Health Checker fails while running upgrade readiness checks during pre-downtime checks. This problem might occur if OFMN and server components are not registered...
properly with the Administration Server of the common domain. The following error is an example error message:

```
ORCH-DOWNTIME-HCT-00002: Executing HealthChecker in task Running Upgrade Readiness (PreDowntime) Checks-GeneralSystem failed. Refer to the logs in /u01/APPLTOP/instance/1cm/logs/11.1.5.0.0/healthchecker for details to take an appropriate corrective action.(Pre-Downtime Checks)
```

**Solution**

Verify that OPMN and server components are registered with the Administration Server of the Common Domain. You can verify this by reviewing the `<ias-instance>` element in the `topology.xml` file. There should be an entry for the server instance with `<ias-instance>` in this file. You can view the `topology.xml` file at this location: `COMMON_DOMAIN_HOME/opmn/topology.xml`. Registration is typically done when setting up the environment.

The entry should be similar to the following example:

```
<topology xmlns='http://www.oracle.com/fmw-nonj2ee-topology'>
   <ias-instance id="CommonDomain_webtier" oracle-home="APPLICATIONS_BASE\webtier_mwhome\webtier" instance-home="APPLICATIONS_CONFIG\CommonDomain_webtier" host="<hostname>" port="<port_number>">
      <ias-component id="ohs1" type="OHS" mbean-class-name="oracle.ohs.OHSGlobalConfig" mbean-interface-name="oracle.ohs.OHSGlobalConfigMXBean" port="<port_number>">
         <properties>
            <property name="ORACLE_HOME" value="APPLICATIONS_BASE\webtier_mwhome\webtier"/>
            <property name="INSTANCE_HOME" value="APPLICATIONS_CONFIG\CommonDomain_webtier"/>
            <property name="ComponentType" value="ohs"/>
         </properties>
         <em-properties>
            <property name="EMTargetType" value="oracle_apache"/>
            <property name="ProxyMBeanObjectName" value="oracle.as.management.mbeans.register:type=component,name=ohs1,instance=CommonDomain_webtier"/> 
            <property name="version" value="11.1.1.6.0"/>
         </em-properties>
      </ias-component>
   </ias-instance>
</topology>
```

If this entry is not present in your file or opmn/topology.xml is not available, run the following command to register the OHS Instance:

```
APPLICATIONS_CONFIG/CommonDomain_webtier/bin/opmnctl registerinstance -adminHost admin_host_name -adminPort admin_port -adminUsername admin_username
```

### 7.18.2 DomainsFileOwnership Health Check Fails With Permissions Issues

**Problem**

Health Checker fails during the DomainsFileOwnership check. The following error is reported, followed by one or more files or directories:

```
[ERROR]: Plugin ‘DomainsFileOwnership’: HC-DOmans-FILE_OwNERSHIP-0002 : Following files and directories have ownership or permission issues.
```
Solution
Change the permission of the files or directories to be at least 600, using the `chmod 600` command.

7.18.3 Context Root Check Health Check Fails

Problem
Health Checker takes an hour or more to complete the Context Root health check. This plugin checks for context root once for redirect=true, and also for redirect=false. The timeout for the plugin is set to 30 minutes by default, causing the check to run for more than an hour.

Solution
Add the following entry to the `ALL_overrides.xml` file, located in the `SHARED_LOCATION/11.1.8.0.0/orchestration/tmp_upgrade_work_area/healthchecker/POD_NAME` directory.

```xml
<checks category="timeout_seconds">
    <check name="ContextRootCheckPlugin" value="500"/>
</checks>
```

7.18.4 Resolve JAZN Conflicts Found by Health Checker

Health Checker checks the JAZN Analysis reports for potential conflicts and deletions that are not patched automatically by the installer. The reports are located in this directory:

`APPLICATIONS_CONFIG/lcm/admin/11.1.8.0.0/fapatch/JAZN/stripe/delta/report.txt`

The `stripe` is crm, fscm, hcm, obi, soa, ucm or bpm.

Review the Modification section of the report to see the roles that the installer did not update. For each conflict that displays in this report, you must evaluate and manually patch the role by using Oracle Authorization Policy Manager (APM).

The following example shows a typical Application Role conflict that has been modified by both the patch and production, therefore it is not applied by the installer.

**MODIFICATION CONFLICTS**
Artifact type: Application Role
Artifact Name: OBIA_PARTNER_CHANNEL_ADMINISTRATIVE_ANALYSIS_DUTY
Description: This artifact is modified at attribute level in patch version and also in production.

Note the location of the following files for reference when using APM:

- Location of baseline files, where `stripe` is crm, fscm, hcm, obi, soa, ucm or bpm:
  `FA_ORACLE_HOME/admin/JAZN/stripe/baseline`

- Location of patch files for fscm, crm, and hcm stripes:
  `FA_ORACLE_HOME/stripedeploy/system-jazn-data.xml`

- Location of patch files for the obi, soa, ucm or bpm stripes:
  `FA_ORACLE_HOME/com/acr/security/jazn/bip_jazn-data.xml`
Related Link
The following document provides additional information related to subjects discussed in this section:
- For more information, see "Upgrading Oracle Fusion Applications Policies" in the Oracle Fusion Applications Administrator’s Guide.

7.18.5 Failure Due to oracle.sysman.oii.oit.OiitTargetLockNotAvailable Exception

Problem
The oracle.sysman.oii.oit.OiitTargetLockNotAvailable exception causes various plug-in failures. The failure messages may or may not contain this exception. Therefore, reviewing the log file is necessary. The following error message is reported in the log file for the failed plugin:

oracle.sysman.oii.oit.OiitTargetLockNotAvailableException: The inventory inventory_path cannot be read since it is being written to by another session.

Solution
This is an intermittent issue and you can resume orchestration when it occurs.

7.19 Troubleshooting Other Issues During the Upgrade

This section contains the following troubleshooting scenarios:
- Perl lib Version is not Compatible
- Policy Store and Oracle Platform Security Services Versions Are Not Compatible
- Bootstrapping Patch Manager Fails
- Propagating Domain Configuration Fails
- Upgrade Failures on Non-Oracle VM Configuration Using OVM Templates
- RUP Lite for Domain Configuration Takes Too Long to Complete
- Deployment of BI Publisher Artifacts Fails
- Importing IPM Artifacts Fails
- Extending Certificate Validation Fails on non-Oracle VM Environment
- Multiple Warnings in Data Security Grants Logs
- Ignorable Errors Reported by catbundle.sql
- Ignorable Errors During Applying Online BI Metadata and Configuration Updates

7.19.1 Perl lib Version is not Compatible

Problem
While downloading patches, as described in Section 2.3.5.3, "Download and Unzip Mandatory Post-Release 8 Patches", you are setting environment variables to run the adCreateMosPlan.pl script. After you issue the setenv command for PERLLIB5, the following error occurs: Perl lib version (v5.8.3) does not match the executable version (v5.8.8).
Solution
Run the following commands:

```bash
export PERL_HOME=/u01/APPLTOP/dbclient/perl
export PATH=/u01/APPLTOP/dbclient/perl/bin:$PATH
```

Then retry the `setenv` command.

7.19.2 Policy Store and Oracle Platform Security Services Versions Are Not Compatible

Problem
After upgrading to Release 11.1.1.8.0, you receive the following error while connecting to ODI Studio:

```java
oracle.security.jps.service.policystore.PolicyStoreIncompatibleVersionException
JPS-06100: Policy Store version 11.1.1.8.0 and Oracle Platform Security Services Version 11.1.1.7.0 are not compatible.
```

Solution
Upgrade or reinstall the ODI studio component from Release 11.1.8.0.

Related Link
The following document provides additional information related to subjects discussed in this section:

- For more information, see "Installing Oracle Data Integrator" in the Oracle Fusion Middleware Installation Guide for Oracle Data Integrator.

7.19.3 Bootstrapping Patch Manager Fails

Problem
An error occurred during the Bootstrapping Patch Manager configuration assistant.

Solution
An error during Bootstrapping Patch Manager normally occurs only when the database is down. Ensure that the database is up and running. You can review the related log files in this location:

```
APPLICATIONS_CONFIG/lcm/logs/11.1.8.0.0/RUP/RUPatchManager_bootstrap_timestamp.log
```

7.19.4 Propagating Domain Configuration Fails

This section contains information about troubleshooting issues that may occur during the Propagating Domain Configuration configuration assistant. The following topics are discussed:

- Propagating Domain Configuration Assistant Takes Too Long to Complete
- Confirm the Configuration Assistant Was Successful
- WARs or EARs Are Not Accessible From The Primordial Host
7.19.4.1 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.

You can monitor the progress of this configuration assistant by reviewing log files in this location:

```
APPLICATIONS_CONFIG/lcm/admin/version/fapatch//ruplitedomain/output/logs
```

7.19.4.2 Confirm the Configuration Assistant Was Successful

To confirm this configuration assistant was successful, verify that the `config/fusionapps_start_params.properties` file exists under each local or non-admin split domain. Also ensure that the `bin/setDomainEnv.sh` file under each local or non-admin split domain contains the following row:

```
POST_CLASSPATH="${COMMON_COMPONENTS_HOME}/modules/oracle.appstrace_11.1.1/appstrace.jar${CLASSPATHSEP}${POST_CLASSPATH}"
```

7.19.4.3 WARs or EARs Are Not Accessible From The Primordial Host

**Problem**
The Propagating Domain Configuration configuration assistant fails if there are WARs or EARs installed or deployed that are not accessible from the primordial host where RUP Installer is running. An example of the error caused by this condition follows:

```
<< read domain from APPTOP/instance/domains/server.company.com/SCMDomain
<< write template to APPLICATIONS_CONFIG/lcm/admin/11.1.8.0.0/fapatch/ruplitedomain/output/templates/SCMDomain.jar
>> fail: Unable to locate file: /fusionapps/localdomain/domains/server.company.com/SCMDomain/datalens/datalens.war
>> fail: write template to "APPLICATIONS_CONFIG/lcm/admin/11.1.8.0.0/fapatch/ruplitedomain/output/templates/SCMDomain.jar"
```

CFGFWK-60550: Script execution aborted. The script may contain an error. Unable to locate file: /fusionapps/localdomain/domains/server.company.com/SCMDomain/datalens/datalens.war

**Solution**
To resolve this issue, you must undeploy or uninstall the WAR or EAR, which is `datalens.war` in this example. Then resume orchestration. After the upgrade has completed successfully, you can install or deploy the WAR or EAR.
7.19.5 Upgrade Failures on Non-Oracle VM Configuration Using OVM Templates

**Problem**
You are running Oracle Fusion Applications on a non-Oracle VM configuration and are using an Oracle VM template, and the upgrade fails.

**Problem**
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.

7.19.6 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.

7.19.7 Deployment of BI Publisher Artifacts Fails

**Problem**
The following error occurs if the BI Presentation servers are running during the deployment of BI Publisher artifacts:

```
java.lang.RuntimeException: Webcat patch file creation failed!
```

**Solution**
If you upgrade to a release that contains BI Publisher artifacts, the BI Presentation servers must not be running. To resolve this issue, shut down the BI Presentation servers to release locks on the Oracle BI Presentation Catalog. For more information, see "faststartstop Syntax" in the Oracle Fusion Applications Administrator’s Guide.

7.19.8 Importing IPM Artifacts Fails

**Problem**
The Importing IPM artifacts configuration assistant fails with the following error:

```
importIPMApplication() & importIPMInput() WLST commands have not run successfully
```

**Solution**
Follow the instructions in Steps 1 through 7 in "Prerequisites for the Deployment of IPM Artifacts" in the Oracle Fusion Applications Patching Guide. Then resume Upgrade Orchestrator.
7.19.9 Extending Certificate Validation Fails on non-Oracle VM Environment

**Problem**
If you have Incentive Compensation, Enterprise Contracts, and Oracle Fusion Accounting Hub offerings on your environment, then Extending Certificate Validation fails with exception reporting:

```
APPTOP/instance/domains/CommonDomain_host/CommonDomain/config/fmwconfig/owc_discussions.jks (No such file or directory).
```

**Solution**
If you don’t find the missing file in APPTOP/instance/domains/CommonDomain_host/CommonDomain/config/fmwconfig, perform the following steps.

1. Copy `default_keystore.jks` to `owc_discussions.jks` in APPTOP/instance/domains/CommonDomain_host/CommonDomain/config/fmwconfig.
2. Resume orchestration.

7.19.10 Multiple Warnings in Data Security Grants Logs

**Problem**
After the Release 8 upgrade step called "Deploying Data Security Grants", the `apatch_Deploying_Data_Security_Grants_timestamp.log` file contains entries as shown in the following example:

- Number of records processed : 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: 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: F9C89E5D04C2322629EB642337695FC. 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.
7.19.11 Ignorable Errors Reported by catbundle.sql

The following ignorable errors may be encountered while running the catbundle.sql script or its rollback script:

ORA-29809: cannot drop an operator with dependent objects
ORA-29931: specified association does not exist
ORA-29830: operator does not exist
ORA-00942: table or view does not exist
ORA-00955: name is already used by an existing object
ORA-01430: column being added already exists in table
ORA-01432: public synonym to be dropped does not exist
ORA-01434: private synonym to be dropped does not exist
ORA-01435: user does not exist
ORA-01917: user or role 'XDB' does not exist
ORA-01920: user name '<user-name>' conflicts with another user or role name
ORA-01921: role name '<role name>' conflicts with another user or role name
ORA-01952: system privileges not granted to 'WKSYS'
ORA-02303: cannot drop or replace a type with type or table dependents
ORA-02443: Cannot drop constraint - nonexistent constraint
ORA-04043: object <object-name> does not exist
ORA-29832: cannot drop or replace an indextype with dependent indexes
ORA-29844: duplicate operator name specified
ORA-14452: attempt to create, alter or drop an index on temporary table already in use
ORA-06512: at line <line number>. If this error follow any of above errors, then can be safely ignored.
ORA-01927: cannot REVOKE privileges you did not grant

7.19.12 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, you can resume the upgrade

7.20 Platform Specific Troubleshooting Issues

This section contains troubleshooting information for platform specific issues.

- Windows Troubleshooting Issues
7.20.1 Windows Troubleshooting Issues

This section contains troubleshooting information for the following issues on Windows.

- DowntimePostFA Phase Fails in RemoveConflictingPatches Task
- Upgrade JDK Fails
- Update Impersonation Configuration Fails on Windows

7.20.1.1 DowntimePostFA Phase Fails in RemoveConflictingPatches Task

**Problem**
The DowntimePostFA phase of orchestration fails during the RemoveConflictingPatches task on Windows with the following error:

RollbackSession rolling back interim patch '16569379' from OH 'c:\AT\webtier_mwhome\webtier'
Prerequisite check 'CheckActiveFilesAndExecutables' failed. The details are:

Following files are active:
c:\AT\webtier_mwhome\webtier\bin\yod.dll

**Solution**
This failure is caused by the OPMN processes running from the BI and GOP homes using this dll. When this failure occurs, shut down the OPMN and the OPMN-managed processes using the respective services. After making sure that the OPMN processes are down, restart orchestration. After orchestration succeeds, bring up the OPMN processes by using the respective services.

7.20.1.2 Upgrade JDK Fails

**Problem**
Upgrade JDK fails with the following error:

Upgrade JDK plugin command:
C:\R\installers\farup\Disk1\upgrade\bin\upgradeJDK.bat
--apptop C:\AT --repo
C:\R
[2013-07-02T14:24:34.566-06:00] [orchestration] [NOTIFICATION] []
[oracle.orchestration] [tid: 12]
[ecid: 0000JyWzVIIFW7HpIsDCif1HonA^000003,0]

Tue 07/02/2013 14:24:34.57 Output logged to file
C:\AT\fusionapps\applications\admin\FUSION\log\upgradeJDK\upgradeJDK_14243455.log
Solution
Set the following environment variables:

```
set APPLICATIONS_BASE=APPLICATIONS_BASE LOCATION>
set REPOSITORY_LOCATION=C:\SHARED\11.1.8.0.0\Repository
```

Then in the same command prompt, start orchestration on the primordial node.

### 7.20.1.3 Update Impersonation Configuration Fails on Windows

**Problem**
The Update Impersonation Configuration configuration assistant fails on Windows.

**Solution**
Relaunch Upgrade Orchestrator to rerun the configuration assistant for Update Impersonation Configuration.

### 7.20.2 Solaris Troubleshooting Issues

This section contains troubleshooting information for Solaris.

#### 7.20.2.1 OutOfMemoryError Due to PermGen Space

**Problem**
An OutOfMemoryError due to PermGen space is reported on the WebLogic managed server for the Solaris x64 or Solaris Sparc platform.

**Solution for Solaris x64**
Perform the following steps to resolve this issue on the Solaris x64 platform.

1. Check the cluster name for the managed server where the PermGen exception is reported. The cluster name can be found from the Administration Server console.
2. Edit the `$DOMAIN_HOME/config/fusionapps_start_params.properties` file by performing the following steps.
   a. Identify the key, value pair which is `fusion.default.SunOS-i386.memoryargs` in `fusionapps_start_params.properties`.
   b. Copy the key, value pair of `fusion.default.SunOS-i386.memoryargs` and add this as a new entry in `fusionapps_start_params.properties`.
   c. For the entry added in the previous step, change the default in `fusion.default.SunOS-i386.memoryargs` to the cluster name and change the argument for `-XX:MaxPermSize` from 512m to 756m.
   d. Bounce the Managed Server.

An example for `SCMCommonServer_1` for Solaris x64 follows.

1. `SCMCommonCluster` is the cluster name for `SCMCommonServer_1`.
2. Add the following entry:

```
fusion.SCMCommonCluster.SunOS-i386.memoryargs=-XX:PermSize=256m
-XX:MaxPermSize=756m -XX:+UseParallelGC -XX:+HeapDumpOnOutOfMemoryError
-XX:HeapDumpPath=path_for_heap_dump -XX:+ParallelGCVerbose
-XX:ReservedCodeCacheSize=128m -XX:+UseParallelOldGC
-XX:ParallelGCThreads=4
```
3. In this example, the entry for `fusion.default.SunOS-i386.memoryargs` is already correct.

**Solution for Solaris Sparc**

Perform the following steps to resolve this issue on the Solaris Sparc platform.

1. Check the cluster name for the managed server where the PermGen exception is reported. The cluster name can be found from the Administration Server console.

2. Edit the `$DOMAIN_HOME/config/fusionapps_start_params.properties` file by performing the following steps.
   
a. Identify the key, value pair which is  
   `fusion.default.SunOS-sparc.memoryargs` in `fusionapps_start_params.properties`.

b. Copy the key, value pair of `fusion.default.SunOS-sparc.memoryargs` and add as a new entry in `fusionapps_start_params.properties`.

c. For the entry added in the previous step, change the default in `fusion.default.SunOS-sparc.memoryargs` to the cluster name and change the argument for `-XX:MaxPermSize` from 512m to 756m.

d. Bounce the Managed Server.

An example for `SCMCommonServer_1` for Solaris Sparc follows.

1. `SCMCommonCluster` is the cluster name for `SCMCommonServer_1`.

2. Add the following entry:

3. In this example, the entry for `fusion.default.SunOS-sparc.memoryargs` is already correct.

7.20.3 AIX Troubleshooting Issues

This section contains troubleshooting information for the following issues on AIX.

- `preValidate.pl` or `postvalidate.pl` Fail for "SSO Keystore Check Test"
- Errors Reported in Oracle Identity Management Upgrade Log

7.20.3.1 preValidate.pl or postvalidate.pl Fail for "SSO Keystore Check Test"

**Problem**

When running `preValidate.pl` or `postvalidate.pl` for the IDM upgrade, the following errors are reported in the `idmUpgrade` logs.

Test Results for "SSO Keystore Check Test"

SSO Keystore required for OIM OAM communication over NAP channel in simple mode is not present.

Test Status: FAILED
**Solution**
If the OAM console is accessible before or after the Oracle Identity Management upgrade is complete, this validation error can be ignored.

### 7.20.3.2 Errors Reported in Oracle Identity Management Upgrade Log

**Problem**
After the Oracle Identity Management upgrade is complete, using idmUpgrade.pl, the following errors are reported in the idmUpgrade logs.

```bash
/bin/bash: <IDMTOP>/products/ohs/ohs/jdk/bin/jps: A file or directory in the path name does not exist.
10:29:34 : Server: AdminServer is not running
```

Similar messages can be reported for other IDM servers also.

**Solution**
If all IDM server instances are stopped before running idmUpgrade.pl, these messages can be ignored.
This appendix provides additional information about Upgrade Orchestrator.

This appendix includes the following topics:

- Upgrade Orchestrator Features
- Additional Information About Upgrade Orchestrator Commands
- Utilities Run by Upgrade Orchestrator

**A.1 Upgrade Orchestrator Features**

Upgrade Orchestrator provides the following features:

- Upgrade Phases
- Pause Points
- Oracle Fusion Applications Orchestrator Upgrade Report
- Language Upgrade

**A.1.1 Upgrade Phases**

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

**A.1.2 Pause Points**

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

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

- Perform required backups.
- Upgrade the Oracle Identity Management domain, if you are not running Oracle Fusion Applications on a SINGLE, 3-NODE, or 4-NODE IDM configuration that is running on Linux and a Release 7 IDM provisioned environment.

- Start external servers.

You cannot edit or remove default pause points. For more information, see Section 5.2, "Pause Point Steps".

### A.1.3 Oracle Fusion Applications Orchestrator Upgrade Report

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

The report displays the task that failed, including the phase and host type. The Fusion Applications Orchestrator Upgrade report also displays the following information:

- **Upgrade from Release**: The starting release on the pod, which is release 11.1.7.0.0.

- **Upgrade to Release**: The ending release, which in this case is "FA version 11.1.8.0.0".

- **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.
A.1.4 Language Upgrade

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

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

A.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

A.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 Section A.2.3, "Options for the Orchestration updateStatus Command."

- Use getStatus to retrieve the status of a specific task as well as the summary of the upgrade on a specific POD_NAME and host_type while Upgrade Orchestrator is running. For more information, see Section A.2.4, "Options for the Orchestration getStatus Command" and Section 7.3, "Monitoring Upgrade Orchestration Progress."

- Use exitOrchestration to terminate orchestration gracefully on all hosts on a specific pod. For more information, see Section 7.4, "Terminating Upgrade Orchestration".

- Use clearExitOrchestration to clear the exit status on all hosts. For more information, see Section 7.4, "Terminating Upgrade Orchestration".

- Use getExitOrchestrationStatus to retrieve the status of the exitOrchestration command. For more information, see Section 7.4.3, "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 Section A.2.5, "The validatesetup Argument."
A.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 A–1 Options for the orchestration.sh command

<table>
<thead>
<tr>
<th>Name</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-pod</td>
<td>Yes</td>
<td>The value of POD_NAME refers to the directory you created in Step 3, Section 2.4.1, &quot;Set Up Upgrade Orchestrator on a Shared Location&quot;.</td>
</tr>
<tr>
<td>-hosttype</td>
<td>Yes</td>
<td>The host type. Valid values are PRIMORDIAL, MIDTIER, OHS, and IDM. For more information see Section 1.2.1, &quot;Host Types.&quot;</td>
</tr>
<tr>
<td>-release</td>
<td>No</td>
<td>The release name, for example, REL8.</td>
</tr>
<tr>
<td>-phase</td>
<td>No</td>
<td>Only the PreDowntime phase can be specified in the command line when running orchestration.</td>
</tr>
<tr>
<td>-checkpoint</td>
<td>No</td>
<td>Valid values are true or false. If set to false, ignore the checkpoint results and rerun. The default value is true.</td>
</tr>
<tr>
<td>-DlogLevel</td>
<td>No</td>
<td>The log level. Valid values are SEVERE, WARNING, INFO, CONFIG, FINE, FINER and FINEST. The default value is INFO. Note that error messages are displayed on the console for database component failures if you set the -DlogLevel option to FINEST.</td>
</tr>
<tr>
<td>-v</td>
<td>No</td>
<td>Displays the product version and exits.</td>
</tr>
<tr>
<td>-h</td>
<td>No</td>
<td>Displays help information and exits.</td>
</tr>
</tbody>
</table>

A.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 A–2 Options for orchestration.sh updateStatus command

<table>
<thead>
<tr>
<th>Name</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>updateStatus</td>
<td>Do not use with getStatus</td>
<td>Updates the status of the selected task.</td>
</tr>
<tr>
<td>-pod</td>
<td>Yes</td>
<td>The name of the pod to be searched.</td>
</tr>
<tr>
<td>-hosttype</td>
<td>Yes</td>
<td>The host type. Valid values are: PRIMORDIAL, MIDTIER, OHS, and IDM.</td>
</tr>
<tr>
<td>-hostname</td>
<td>Yes</td>
<td>Host name, including domain details.</td>
</tr>
<tr>
<td>-release</td>
<td>Yes</td>
<td>The release name, for example, REL8. If this option is not used, all releases defined in the manifest file are executed.</td>
</tr>
<tr>
<td>-phase</td>
<td>Yes</td>
<td>The phase name. Valid values are: PreDowntime, DowntimePreFA, DowntimeDuringFA, DowntimePostFA, DowntimeDuringLP, DowntimePostLP.</td>
</tr>
<tr>
<td>-taskid</td>
<td>Yes</td>
<td>Orchestration task_id that is to be updated.</td>
</tr>
<tr>
<td>-taskstatus</td>
<td>Yes</td>
<td>Orchestration task status. Valid values are success and error.</td>
</tr>
<tr>
<td>-v</td>
<td>No</td>
<td>Displays the product version and exits.</td>
</tr>
<tr>
<td>-h</td>
<td>No</td>
<td>Displays help information and exits.</td>
</tr>
</tbody>
</table>
A.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>
<thead>
<tr>
<th>Name</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>getStatus</td>
<td>Do not use with updateStatus</td>
<td>Retrieves the checkpoint status from the selected orchestration task.</td>
</tr>
<tr>
<td>-pod</td>
<td>Yes</td>
<td>The name of the pod to be searched.</td>
</tr>
<tr>
<td>-hosttype</td>
<td>Yes</td>
<td>The host type. Valid values are: PRIMORDIAL, MIDTIER, OHS, and IDM.</td>
</tr>
<tr>
<td>-hostname</td>
<td>Yes</td>
<td>Host name, including domain details.</td>
</tr>
<tr>
<td>-release</td>
<td>Yes</td>
<td>The release name, for example, REL8. If this option is not used, all releases defined in the manifest file are queried.</td>
</tr>
<tr>
<td>-phase</td>
<td>No</td>
<td>You can specify the following phase names to see the status for the specific phase: PreDowntime, DowntimePreFA, DowntimeDuringFA, DowntimePostFA, DowntimeDuringLP, DowntimePostLP.</td>
</tr>
<tr>
<td>-taskid</td>
<td>No</td>
<td>The Orchestration task_id that is to be searched. If this option is used, the status for the specific task is returned.</td>
</tr>
<tr>
<td>-taskstatus</td>
<td>No</td>
<td>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.</td>
</tr>
<tr>
<td>-v</td>
<td>No</td>
<td>Displays the product version and exits.</td>
</tr>
<tr>
<td>-h</td>
<td>No</td>
<td>Displays help information and exits.</td>
</tr>
</tbody>
</table>

A.2.5 The validatesetup Argument

If you run the orchestration.sh command with the validatesetup argument, the following validations occur:

- Validating SHARED_UPGRADE_LOCATION
  Successfully validated permissions of shared folder.
- Validating ORCHESTRATION_CHECKPOINT_LOCATION
  Successfully validated permissions of shared folder.
- Validating ORCHESTRATION_CHECKPOINT_ARCHIVE_LOCATION
  Successfully validated permissions of shared folder.

These options run implicitly when any of the orchestration commands run.

A.3 Utilities Run by Upgrade Orchestrator

This section describes the utilities that are run by Upgrade Orchestrator. This is for your information only and no action is needed. The following utilities are included:

- RUP Installer
- Health Checker Utility
- RUP Lite for OVM Utility
A.3.1 RUP Installer

During the installation phase, RUP Installer copies all files for 11g Release 8 (11.1.8) to the appropriate locations, such as Oracle Fusion Middleware home and Oracle Fusion Applications Oracle home. After the file copy completes, RUP Installer calls its first installer to update Oracle Fusion Applications Patch Manager and apply Oracle Fusion Middleware patches. When the first installer completes successfully, RUP Installer calls the second installer, which performs the Policy Store Analysis. Upon successful completion of the Policy Store Analysis, RUP Installer calls Configuration Assistants to perform the remaining tasks required to update and deploy artifacts to Oracle Fusion Applications. Depending on the contents of 11g Release 8 (11.1.8), not all configuration assistants may run.

A.3.1.1 RUP Installer Configuration Assistants

All mandatory configuration assistants must complete successfully before proceeding to the next configuration assistant.

If any tasks fail during the installation phase, refer to Section 7.7, "Troubleshooting Failures During the Installation Phase" for more information.

The following table provides a list of configuration assistants that the first installer runs. The Retry Behavior and Troubleshooting column describes what RUP Installer does after a configuration assistant fails, you resolve the cause of the failure, and then resume orchestration. If available, links are provided to relevant troubleshooting sections.

<table>
<thead>
<tr>
<th>Name</th>
<th>Mand atory</th>
<th>Description</th>
<th>Retry Behavior and Troubleshooting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Patch Manager</td>
<td>Yes</td>
<td>Configures Oracle Fusion Applications Patch Manager.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Consolidate Repository And Downloaded Patches</td>
<td>Yes</td>
<td>Consolidates patches in the repository and the patches you download in Section 2.3.5.3, &quot;Download and Unzip Mandatory Post-Release 8 Patches&quot;.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Update Patch Manager</td>
<td>Yes</td>
<td>Applies Patch Manager Patches</td>
<td>Applies failed patches.</td>
</tr>
<tr>
<td>Reconfigure Patch Manager</td>
<td>Yes</td>
<td>Reconfigures Oracle Fusion Applications Patch Manager.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Bootstrap Patch Manager</td>
<td>Yes</td>
<td>Updates the data model for Oracle Fusion Applications Patch Manager by running the fapmgr bootstrap command.</td>
<td>Starts from the beginning of the task. See Section 7.19.3, &quot;Bootstrapping Patch Manager Fails&quot;.</td>
</tr>
<tr>
<td>Create Middleware Schemas</td>
<td>Yes</td>
<td>Creates Oracle Fusion Middleware schemas</td>
<td>The upgrade fails. See Section 7.8.12, &quot;Creating Middleware Schema Fails&quot;.</td>
</tr>
<tr>
<td>Name</td>
<td>Mandatory</td>
<td>Description</td>
<td>Retry Behavior and Troubleshooting</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Apply Middleware Patch Sets</td>
<td>Yes</td>
<td>Applies Oracle Fusion Middleware patch sets, which can include upgrades, schema changes and installers. For more information, see Section A.3.1.1.1, &quot;Middleware Installers Invoked by the Apply Middleware Patch Sets Configuration Assistant&quot;.</td>
<td>Install failed patch sets.</td>
</tr>
<tr>
<td>Apply Pre-PSA Middleware Patches</td>
<td>Yes</td>
<td>Applies Pre-PSA Middleware Patches For more information, see Section A.3.1.1.2, &quot;Patches Not Supported by the Apply Pre-PSA and Post-PSA Middleware Patches Configuration Assistants&quot;.</td>
<td>Applies the failed patches. See Section 7.12, &quot;Troubleshooting Applying Middleware Patches&quot;.</td>
</tr>
<tr>
<td>Verify Middleware PSA Schema Credentials</td>
<td>Yes</td>
<td>Verifies users and logins for schemas.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Upgrade Middleware Schemas</td>
<td>Yes</td>
<td>Runs Oracle Fusion Middleware patch set assistants (PSA).</td>
<td>Runs failed tasks. See Section 7.12.6, &quot;Upgrading Middleware Schema Fails&quot;.</td>
</tr>
<tr>
<td>Apply Post-PSA Middleware Patches</td>
<td>Yes</td>
<td>Applies Post-PSA Middleware Patches See Section A.3.1.1.2, &quot;Patches Not Supported by the Apply Pre-PSA and Post-PSA Middleware Patches Configuration Assistants&quot;.</td>
<td>Applies the failed patches. See Section 7.12, &quot;Troubleshooting Applying Middleware Patches&quot;.</td>
</tr>
<tr>
<td>Restore Default Context in JPS-CONFIG-JSE.XML Files</td>
<td>Yes</td>
<td>Restores default context.</td>
<td>Checks if file is corrupted and replaces the file with a well formed XML file and retries failed steps.</td>
</tr>
<tr>
<td>Upgrade OPSS</td>
<td>Yes</td>
<td>Upgrades the Policy Store.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Extend Certificate Validity</td>
<td>Yes</td>
<td>Extends certificate validity by three years from the date of the upgrade.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Deploy Middleware Policies (jazn-data.xml)</td>
<td>Yes</td>
<td>Deploys Middleware policies:</td>
<td>Starts from the beginning of the task and includes the clean up required.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Deploys JAZN for ATGPF</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Deploys JAZN for FSM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Deploys JAZN for APPSDIAG</td>
<td></td>
</tr>
<tr>
<td>Apply Offline BI Metadata and Configuration Updates</td>
<td>Yes</td>
<td>Performs the deployment of the updated applications policies for Oracle Business Intelligence.</td>
<td>Retries failed steps.</td>
</tr>
<tr>
<td>Apply ESSAPP Code Source Grant Changes</td>
<td>Yes</td>
<td>Adds code source grants to support auditing.</td>
<td>Starts from the beginning of the task.</td>
</tr>
</tbody>
</table>
The following table provides a list of configuration assistants that the second installer runs. The Retry Behavior and Troubleshooting column describes what RUP Installer does after a configuration assistant fails, you resolve the failure, and then resume orchestration. If available, links are provided to relevant troubleshooting sections. The second installer supports parallel processing of certain configuration assistants, which run in groups.

### Table A–5  Configuration Assistants Run by Oracle Fusion Applications 11g Release 8 (11.1.8) RUP Installer Part 2 of 2

<table>
<thead>
<tr>
<th>Name</th>
<th>Mandatory</th>
<th>Description</th>
<th>Retry Behavior and Troubleshooting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply Domain Configuration</td>
<td>Yes</td>
<td>- Applies startup parameter changes.</td>
<td>Retries failed steps.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Configures datasource for audit service.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updates logging configuration.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Reassigns library targets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Redeploys UMS drivers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updates OWLCS version.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Configures new ODI server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updates domain component versions.</td>
<td></td>
</tr>
<tr>
<td>Propagate Domain Configuration</td>
<td>Yes</td>
<td>Unzips RUP Lite for Domain Configuration into APPLICATIONS_CONFIG/lcm/admin/version/fapatch/ruppliedomain. Updates properties in the RUP Lite env.properties file and prepares RUP Lite so you can run RUP Lite for Domain Configuration.</td>
<td>Starts from the beginning of the task. See Section 7.19.4, “Propagating Domain Configuration Fails”.</td>
</tr>
</tbody>
</table>

The following table provides a list of configuration assistants that the second installer runs. The Retry Behavior and Troubleshooting column describes what RUP Installer does after a configuration assistant fails, you resolve the failure, and then resume orchestration. If available, links are provided to relevant troubleshooting sections. The second installer supports parallel processing of certain configuration assistants, which run in groups.

### Table A–4  Configuration Assistants Run by Oracle Fusion Applications 11g Release 8 (11.1.8) RUP Installer Part 1 of 2

<table>
<thead>
<tr>
<th>Name</th>
<th>Mandatory</th>
<th>Description</th>
<th>Retry Behavior and Troubleshooting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Patch Manager</td>
<td>Yes</td>
<td>Configures Oracle Fusion Applications Patch Manager.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Bootstrap Patch Manager</td>
<td>Yes</td>
<td>Updates the data model for Oracle Fusion Applications Patch Manager by running the fapmng bootstrap command.</td>
<td>Starts from the beginning of the task. See Section 7.19.3, “Bootstrapping Patch Manager Fails”.</td>
</tr>
<tr>
<td>Offline Preverification Pre Database Content Upload</td>
<td>Yes</td>
<td>Performs the following validation checks while all servers are shut down:</td>
<td>Runs failed steps.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Policy Store</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Number of database workers</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Database Content Upload</td>
<td></td>
</tr>
<tr>
<td>Grant Privileges to Application Schemas</td>
<td>Yes</td>
<td>Grants system privileges to database users and creates base object privileges.</td>
<td>Runs the failed script.</td>
</tr>
<tr>
<td>Name</td>
<td>Mandatory</td>
<td>Description</td>
<td>Retry Behavior and Troubleshooting</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>Load Database Components</td>
<td>Yes</td>
<td>Uploads the database content packaged in 11g Release 8 (11.1.8) to the database, such as database objects, seed data, and package headers and bodies.</td>
<td>Runs failed database commands. See Section 7.13, “Troubleshooting Loading Database Components”.</td>
</tr>
<tr>
<td>Deploy Applications Policies (jazn-data.xml)</td>
<td>Yes</td>
<td>Deploys updated applications policies, based on your selections during the Policy Store Analysis configuration assistant.</td>
<td>Deploys the failed stripes. See Section 7.14, “Troubleshooting Deployment of Applications Policies”.</td>
</tr>
<tr>
<td>Deploy BI Publisher Artifacts</td>
<td>Yes</td>
<td>Using Catalog Manager, performs the following steps:</td>
<td>Starts from the beginning of the task. See Section 7.19.7, “Deployment of BI Publisher Artifacts Fails”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Backs up BI Presentation Catalog under APPLICATIONS_CONFIG/lcm/admin/version/fapatch/BIP/language_code for example, APPLICATIONS_CONFIG/lcm/admin/11.1.8.0.0/fapatch/BIP/en_US/webcat.zip.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Backs up captions under APPLICATIONS_CONFIG/lcm/admin/version/fapatch/BIP/language_code/captions.zip.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Copies captions to the Oracle Business Intelligence repository.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Deploys BI Presentation Catalog to the Oracle Business Intelligence repository.</td>
<td></td>
</tr>
<tr>
<td>Import Oracle Data Integrator Repositories</td>
<td>Yes</td>
<td>■ Imports ODI topology.</td>
<td>Imports failed data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Imports ODI model folders.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Imports ODI models.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Imports ODI projects.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Drops ODI error tables.</td>
<td></td>
</tr>
<tr>
<td>Create Grants/Synonyms on Application Database Objects</td>
<td>Yes</td>
<td>Creates synonyms between database objects and grants object privileges to database users.</td>
<td>Runs the failed script.</td>
</tr>
<tr>
<td>Offline Preverification Post Database Content Upload</td>
<td>Yes</td>
<td>Validate host and port for new managed servers.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Deploy Data Security Grants</td>
<td>Yes</td>
<td>Performs GUID reconciliation in LDAP.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Generate SOA Configuration Plan</td>
<td>Yes</td>
<td>Generates the configuration plan to be used for deploying SOA composites.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Name</td>
<td>Mandatory</td>
<td>Description</td>
<td>Retry Behavior and Troubleshooting</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Update Flexfield Configuration</td>
<td>Yes</td>
<td>Updates the FndSetup application for supporting new flexfields, new flexfield usages, and flexfield view links added by Oracle Fusion Application products.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Configure New Managed Servers</td>
<td>Yes</td>
<td>Configures managed servers for new applications to be associated with the first non-admin host by default.</td>
<td>Reapplies failed managed server templates.</td>
</tr>
<tr>
<td>Deploy New Applications</td>
<td>Yes</td>
<td>Deploys new applications using domain extension templates.</td>
<td>Reapplies failed domain extension templates.</td>
</tr>
<tr>
<td>Generate ADF Domain Configuration Plan</td>
<td>Yes</td>
<td>Generates Oracle ADF domain configuration in Metadata Service (MDS) to be used by Expression Language (EL) expressions in connections.xml.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Apply Offline Setting Changes</td>
<td>Yes</td>
<td>Applies Oracle Fusion Applications environment configuration setting changes while all servers are shut down.</td>
<td>Retries failed domains.</td>
</tr>
<tr>
<td>Verify Node Manager and OPMN Status</td>
<td>Yes</td>
<td>Verifies the following processes: ■ Node Managers ■ BI OPMN Processes ■ GOP OPMN Processes ■ Web Tier OPMN Processes You must not exit out of RUP Installer during this configuration assistant.</td>
<td>Runs failed steps. See Section 7.9.3, &quot;Verifying Node Manager and OPMN Status Fails&quot;.</td>
</tr>
<tr>
<td>Start All Admin Servers</td>
<td>No</td>
<td>Starts all Administration Servers.</td>
<td>Restarts failed Administration Servers. See Section 7.15, &quot;Troubleshooting Server Start and Stop Failures&quot;.</td>
</tr>
<tr>
<td>Configure DB Persistence Store for JMS/TLogs</td>
<td>Yes</td>
<td>Configures SOA and UMS to store JMS and TLogs content in the database instead of the file system.</td>
<td>Retries failed plug-ins.</td>
</tr>
<tr>
<td>Configure OPSS Keystore Service</td>
<td>Yes</td>
<td>Configures OPSS to be used for remote task flow Keystore Service.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Deploying LDAP Data (LDIF)</td>
<td>No</td>
<td>Loads new enterprise roles.</td>
<td>Retries to load the failed LDIF files.</td>
</tr>
<tr>
<td>Create Fusion APPIDs</td>
<td>Yes</td>
<td>Creates Fusion APPID users and groups in the LDAP server and credentials for those users in the credential store.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Apply Admin Server Online Setting Changes</td>
<td>Yes</td>
<td>Applies Oracle Fusion Applications environment configuration setting changes that are applicable to the Administration Servers.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Start Minimal Servers for Configuration Updates</td>
<td>Yes</td>
<td>Starts minimal managed servers required to run the necessary configuration assistants successfully.</td>
<td>Starts from the beginning of the task.</td>
</tr>
</tbody>
</table>
### Utilities Run by Upgrade Orchestrator

<table>
<thead>
<tr>
<th>Name</th>
<th>Mandatory</th>
<th>Description</th>
<th>Retry Behavior and Troubleshooting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply UCM Configuration</td>
<td>Yes</td>
<td>Configures UCM to store content in the database instead of the file system.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Apply WebCenter Connection Changes</td>
<td>Yes</td>
<td>■ Replaces WebCenter-UCM Connection with FusionAppsContentRepository Connection</td>
<td>Retries failed plug-ins.</td>
</tr>
<tr>
<td>■ Updates Connection References</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure Trust Asserter</td>
<td>Yes</td>
<td>Configures trust asserter to be used for remote task flow Keystore Service.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Start All Servers</td>
<td>No</td>
<td>Starts all servers in all domains, including the BI servers. Also performs the <code>opmnctl start</code> for Oracle HTTP Server (OHS) and BIInstance.</td>
<td>Restarts failed servers. See Section 7.15, &quot;Troubleshooting Server Start and Stop Failures&quot;.</td>
</tr>
<tr>
<td>Online Preverification</td>
<td>Yes</td>
<td>Performs steps described in see Section A.3.1.1.3, &quot;Steps Performed During Online Preverification&quot;.</td>
<td>Runs failed steps. See Section 7.15.4, &quot;Online Preverification Reports EditTimedOutException Error&quot;.</td>
</tr>
<tr>
<td>Upgrade ADF Metadata</td>
<td>No</td>
<td>Upgrades ADF related metadata.</td>
<td>Retries failed domains.</td>
</tr>
<tr>
<td>Generate OHS Reference Configuration File</td>
<td>No</td>
<td>Generates OHS configuration files for installed product families in the directory, <code>APPLICATIONS_CONFIG/lcm/admin/version/fapatch/OHS/patched_moduleconf</code>.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Apply OWSM Configuration</td>
<td>Yes</td>
<td>Upgrades Oracle Web Services Manager (Oracle WSM) policies after backing up the policies.</td>
<td>Restores the backup of the policies and starts from the beginning of the task.</td>
</tr>
<tr>
<td>Deploy SPE Inline Service Artifacts</td>
<td>No</td>
<td>Deploys SPE Inline Service Artifacts.</td>
<td>Retries the deployment.</td>
</tr>
<tr>
<td>Deploy Data Role (RGX) Templates</td>
<td>No</td>
<td>Deploys RGX Template artifacts to the Common Domain.</td>
<td>Deploys failed templates.</td>
</tr>
<tr>
<td>Apply OAM Configuration</td>
<td>No</td>
<td>Applies changes to the Oracle Access Manager (OAM) configuration.</td>
<td>Starts from the beginning of the task. See Section 7.11.4, &quot;Location of GRC Policies in the OAM Applications Domain&quot;.</td>
</tr>
<tr>
<td>Deploy Flexfields</td>
<td>No</td>
<td>Deploys flexfields to the domain that hosts the FndSetup application.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Name</td>
<td>Mandatory</td>
<td>Description</td>
<td>Retry Behavior and Troubleshooting</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Apply Online BI Metadata and Configuration Updates</td>
<td>Yes</td>
<td>Applies Oracle Business Intelligence Metadata updates.</td>
<td>Starts from the beginning of the task. If you made any customizations to the Oracle BI Repository, the Oracle BI Presentation Catalog, or JAZN settings related to Oracle Business Intelligence, you must merge your changes. See Section 6.11, &quot;Resolve Conflicts That Occurred During Oracle BI Metadata Updates&quot;.</td>
</tr>
<tr>
<td>SOA Preverification</td>
<td>Yes</td>
<td>Performs the steps described in Section A.3.1.4, &quot;Steps Performed During SOA Preverification&quot;. If you have customizations, you must merge them during this configuration assistant.</td>
<td>Retries failed steps. See Section 7.16.6, &quot;Merging SOA Composite JDeveloper Customizations During SOA Preverification&quot;.</td>
</tr>
<tr>
<td>Apply SES Configuration Changes</td>
<td>No</td>
<td>Updates additional configuration updates to Oracle Secure Enterprise Search (SES) running on the Common Domain.</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td>Remove UCM SES Objects</td>
<td>No</td>
<td>Removes the following objects on the SES search administration server:</td>
<td>Starts from the beginning of the task.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Index Schedule with the name &quot;WebCenter UCM Schedule&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Data source with the name &quot;WebCenter UCM&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Data source with the name &quot;WebCenter UCM&quot; from the data source group with the name &quot;Collaboration&quot;</td>
<td></td>
</tr>
<tr>
<td>Deploy BPM Templates</td>
<td>No</td>
<td>Deploys BPM Templates to the MDS repository.</td>
<td>Deploys failed templates.</td>
</tr>
<tr>
<td>Deploy SOA Shared Repository</td>
<td>Yes</td>
<td>Deploys SOA shared repository artifacts to the SOA servers available in the environment.</td>
<td>Deploys failed SOA shared repository artifacts.</td>
</tr>
<tr>
<td>Deploy SOA Composites</td>
<td>No</td>
<td>Deploys SOA composites to the corresponding SOA servers and performs server management steps.</td>
<td>Deploys failed SOA composites. See Section 7.16, &quot;Troubleshooting SOA Composite Deployment Failures&quot;.</td>
</tr>
</tbody>
</table>
### Table A–5 (Cont.) Configuration Assistants Run by Oracle Fusion Applications 11g Release 8 (11.1.8) RUP Installer Part 2 of 2

<table>
<thead>
<tr>
<th>Name</th>
<th>Mandatory</th>
<th>Description</th>
<th>Retry Behavior and Troubleshooting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy SOA Resource Bundles</td>
<td>Yes</td>
<td>Deploys SOA Resource Bundles to the corresponding SOA servers.</td>
<td>Deploys failed SOA resource bundles.</td>
</tr>
<tr>
<td>Import Image Routing (IPM) Artifacts</td>
<td>No</td>
<td>Deploys IPM artifacts to the IPM server.</td>
<td>Retries failed IPM artifacts. See Section 7.19.8, &quot;Importing IPM Artifacts Fails&quot;</td>
</tr>
<tr>
<td>Restart All SOA Servers</td>
<td>Yes</td>
<td>Restarts all SOA servers in the environment.</td>
<td>Starts at the beginning of the task.</td>
</tr>
<tr>
<td>Apply Online Setting Changes</td>
<td>No</td>
<td>Applies Oracle Fusion Applications environment configuration setting changes during the online phase.</td>
<td>Starts from the failed task.</td>
</tr>
<tr>
<td>Generate RUP Lite for OHS</td>
<td>No</td>
<td>Generates the zip file that contains all files needed by RUP Lite for OHS to upgrade OHS.</td>
<td>Starts at the beginning of the task.</td>
</tr>
<tr>
<td>Apply Downloaded Oracle Fusion Applications Patches</td>
<td>Yes</td>
<td>Applies the Oracle Fusion Applications patches that you downloaded in Section 2.3.5.3, &quot;Download and Unzip Mandatory Post-Release 8 Patches&quot;.</td>
<td>Applies failed patches.</td>
</tr>
<tr>
<td>Post Configuration</td>
<td>No</td>
<td>◼ Reactivates SES Index Optimization ◼ Reactivates ESS Server from inactive or quiescent mode ◼ Deletes wallets</td>
<td>Retries failed domains.</td>
</tr>
</tbody>
</table>

### A.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)
A.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: You patch your Database Server using RUP Lite for RDBMS. For more information, see Section 3.2, "Run RUP Lite for RDBMS."
- Oracle Identity Management Server: You patch your IDM server by following the steps in Section 5.2.5, "Upgrade the Oracle Identity Management Domain to 11g Release 8 (11.1.8)."

A.3.1.1.3 Steps Performed During Online Preverification

The following validation steps are performed during the Online Preverification configuration assistant, if Release 8 (11.1.8) contains artifacts related to the validation:

- Taxonomy URL
- Database validation
- Flexfield: Checks for the HelpPortal Managed Server in the Common Domain and for the successful deployment of the FndSetup application.
- OAM Configuration
- SES Admin Server URL
- SPE Inline Service: Checks if the Oracle CRM Performance application is deployed. If it is, the OracleRTD application must be deployed and at least one BI server must be running where the OracleRTD application is deployed.
- Data Role (RGX) Template: Checks if the Administration Server for the Common Domain is up.
- Group Space Template: Checks if the following Managed Servers are up: WC_Spaces, WC_Collaboration, ucm_server1.
- Oracle WSM validation

A.3.1.1.4 Steps Performed During SOA Preverification

The following validation steps are performed during the SOA Preverification configuration assistant:

- Business Process Management (BPM) Template
- B2B Metadata: Checks if the Common Domain, SOA Managed Server, and the LDAP Server are up.
- 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 Section 7.16.6, "Merging SOA Composite JDeveloper Customizations During SOA Preverification".

Image Routing (IPM): Checks if the IPM server is up.

A.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. You run Health Checker during pre-down time, as described in Section 4.1, "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. The validation checks are organized into groups, based on the purpose of the checks and when the checks are performed. When Health Checker runs, it uses a specific manifest file which performs the appropriate checks. Several health checks are called by Upgrade Orchestrator and all health checks can also be run manually. Health Checker provides a list of corrective actions for the checks that fail validation. The suggested corrective actions must be run manually to fix the issue before proceeding with the related activity, such as upgrading or patching activities.

The following topics describe the usage of Health Checker:

■ Health Checker Manifests
■ Health Checker Plug-ins
■ Override Health Checks

A.3.2.1 Health Checker Manifests

When you run Health Checker manually, you specify a manifest file, 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 you upgrade:

\[ FA_{ORACLE\_HOME}/lcm/hc/config \]

■ The manifest files in the following location are from the current release and must be used when running Health Checker before the upgrade:

\[ REPOSITORY\_LOCATION/installers/farup/Disk1/upgrade/config \]
### Table A-6  Health Checker Manifest Files

<table>
<thead>
<tr>
<th>Manifest File</th>
<th>Host Requirements</th>
<th>Typical Usage of the Manifest</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>GeneralSystemHealthChecks.xml</code></td>
<td>Primordial, OHS, Mid tier, DB</td>
<td>Run this manifest any time. See Section A.3.2.2.1, &quot;General System Health Checks.&quot;</td>
</tr>
<tr>
<td><code>PreDowntimeUpgradeReadinessHealthChecks.xml</code></td>
<td>Primordial, OHS, Mid tier, DB</td>
<td>Upgrade Orchestrator runs this manifest before the upgrade downtime. You can run this at any time. See Section A.3.2.2.2, &quot;Pre-Downtime Upgrade Tasks.&quot;</td>
</tr>
<tr>
<td><code>DuringDowntimeUpgradeReadinessHealthChecks.xml</code></td>
<td>Primordial, OHS, Mid tier</td>
<td>Upgrade Orchestrator runs this manifest during downtime and before the upgrade starts. See Section A.3.2.2.3, &quot;Pre-Upgrade Tasks Performed by Health Checker During Downtime.&quot;</td>
</tr>
<tr>
<td><code>VitalSignsChecks.xml</code></td>
<td></td>
<td>Upgrade Orchestrator runs this manifest during the upgrade. See Section A.3.2.2.10, &quot;Vital Signs Check.&quot;</td>
</tr>
<tr>
<td><code>PostUpgradeHealthChecks.xml</code></td>
<td>Primordial, OHS, Mid tier</td>
<td>Upgrade Orchestrator runs this manifest after the upgrade. See Section A.3.2.2.4, &quot;Post-Upgrade Tasks Performed by Health Checker.&quot;</td>
</tr>
<tr>
<td><code>LanguagePackReadinessHealthChecks.xml</code></td>
<td></td>
<td>Run this manifest before installing a language pack. See Section A.3.2.2.5, &quot;Language Pack Readiness Health Checks.&quot;</td>
</tr>
<tr>
<td><code>PostLanguagePackHealthChecks.xml</code></td>
<td></td>
<td>Run this manifest after installing a language pack. See Section A.3.2.2.6, &quot;Post Language Pack Health Checks.&quot;</td>
</tr>
<tr>
<td><code>PatchingReadinessHealthChecks.xml</code></td>
<td></td>
<td>Run this manifest before applying a patch. See Section A.3.2.2.7, &quot;Patching Readiness Health Checks.&quot;</td>
</tr>
<tr>
<td><code>PostPatchingHealthChecks.xml</code></td>
<td></td>
<td>Run this manifest after applying a patch. See Section A.3.2.2.8, &quot;Post Patching Health Checks.&quot;</td>
</tr>
<tr>
<td><code>DataQualityChecks.xml</code></td>
<td></td>
<td>Run this manifest to check the quality of data such as JAZN and seed data. Note that these checks may require significant processing time. See Section A.3.2.2.9, &quot;Data Quality Check.&quot;</td>
</tr>
</tbody>
</table>

#### A.3.2.2 Health Checker Plug-ins

There may be situations in which you want to run health checks manually, outside of orchestration. For example, you may want to run the pre-downtime checks several weeks before you upgrade, so that you have time to fix any issues found by `PreDowntimeUpgradeReadinessHealthChecks.xml`.

Health Checker calls plug-ins to perform its tasks. This section describes which plug-ins run during the following phases of the installer process:

- General System Health Checks
- Pre-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
Utilities Run by Upgrade Orchestrator

A.3.2.2.1 General System Health Checks  The following checks occur when you run Health Checker using the GeneralSystemHealthChecks.xml manifest.

- Administration Servers and Managed Servers are Up
  Confirms that all relevant Administration Servers and Managed Servers have a RUNNING status.

- Certificate Expiry in Trust Keystore
  Checks the expiration date for the certificates in the Trust key store and reports an error if the expiration date has passed or is within the next 90 days.

- Credential Store Connectivity
  Checks if a connection can be established to the credential store.

- Credentials in Oracle Directory Services Manager (ODSM)
  Verifies that a specific user, usually the PolicyRWUser user, is part of the cn=DirectoryAdminGroup.

- Database Instance Connectivity
  Checks if the database instance is up. For RAC databases, checks if all nodes are up.

- DBMS_STATS Collection for MDS Schema in Oracle Fusion Applications Database
  Confirms that DBMS_STATS has recently been run on the MDS schema in the Oracle Fusion Applications database. You must run DBMS_STATS on any schemas that are reported by Health Checker.

- Deployed Applications are Up
  Verifies that all deployed applications are up and running.

- FAPatchManager Configuration
  Checks if Oracle Fusion Applications Patch Manager is correctly configured, including the following validations:
  - Checks to see if FUSION_env.properties and ATGPF_env.properties are correct.
  - Checks for existence of the fapmgr.ini file in the environment.
  - Verifies registered products against the database.

- Flexfields Metadata in the Flex Repository
  Checks if there is a Flexfields metadata violation that indicates that the Extensible Flexfields has a UI Page defined that references a Flexfield Context which has not been associated with the corresponding Category or any of its parent Categories.

- Fusion Applications Certification Matrix
  Confirms the correct versions of installed components, according to the certification matrix.

- Fusion Schema Connectivity
  Validates the database connectivity to all Fusion schemas.

- Hosts Name
Confirms that host names are correctly formatted in the `/etc/hosts` file. The `/etc/hosts` file is a network configuration file that associates IP addresses with host names and host alias names, if used. The following checks are performed by this plug-in:

- The `/etc/hosts` file contains an entry for the IP address `127.0.0.1`, followed by the name `localhost`.
- The format of each host entry in `/etc/hosts` is `IP_address canonical_hostname [aliases]`. If the machine name is a logical host name and is different from the physical host name that is specified in `/etc/sysconfig/network`, the logical host name must be listed before the physical host. Ensure that the first entry in `/etc/hosts`, machine name (host name), and the value used in `pod.properties`, are identical.
- If the machine name is the same as the physical host name, there is no need to check the order of the host names.

- Identity and Policy Store LDAP
  Verifies the connectivity to the identity store and policy store LDAP using identity store credentials.

- Identity Store Connectivity using jps-config-jse.xml
  Verifies that the `idstore.ldap.provider` in `jps-config-jse.xml` can be used to connect to the identity store.

- IIR Configuration
  Verifies that Fusion Informatica IR is set up properly.

- `INBOUND_CONNECT_TIMEOUT` parameter in `sqlnet.ora` and `listener.ora`
  Checks for recommended values in the `INBOUND_CONNECT_TIMEOUT` parameter in `sqlnet.ora` and `listener.ora` files on the database host.

- Index Validity in Fusion Schema of Oracle Fusion Applications Database
  Checks for unusable indexes in the Fusion Schema of the Oracle Fusion Applications database.

- `init.ora` parameters
  Verifies that the `init.ora` parameters are correct.

- Invalid Objects
  Checks for and reports any invalid objects.

- JAZN Version in Oracle_Home Matches LDAP
  Verifies that the JAZN version in `system-jazn-data.xml` is the same as the version in the policy store.

- JVM Architecture, JDK platform Type, JAVA Version, and JDK Vendor
  Verifies that the JDK version is valid. It also validates the JVM architecture, JDK platform type, and JDK vendor.

- Listener Configuration
  Verifies that the database listener configuration runs from the grid home on the DB host and also that no duplicate processes for the listener are running.

- Local Port Range Value
Checks the local port range value in `/proc/sys/net/ipv4/ip_local_port_range`. The recommended value is `32768 61000`. If the range is set to any value below `32768`, a system process could potentially use a port that was assigned to one of the Managed Servers. Since RUP Installer requires all domains to be down, those ports are available for the system to use.

- **Mandatory Patches Have Been Applied**
  Verifies that mandatory patches have been applied.

- **MDS Schema Connectivity**
  Checks database connectivity for schemas that contain `FUSION_MDS` in their name.

- **Middleware Schema Connectivity**
  Checks database connectivity for all schemas except for `FUSION_MDS` schemas.

- **Multi-Tenant set-up in Fusion Schema of Oracle Fusion Applications Database**
  Ensures that only one enterprise is enabled in the database.

- **Node Manager Crash Recovery Is Set To True**
  Verifies the `CrashRecoveryEnabled` entry in `nodemanager.properties` is set for each host.

- **Node Managers are up and accessible**
  Checks if node managers for all hosts are running and are accessible.

- **OAM Configuration**
  Verifies the following information in `Fusion_env.properties`:
  - `OAM_ADMIN_SERVER_HOST`
  - `OAM_ADMIN_SERVER_PORT`
  - `OAM_WEB_DOMAIN`
  - `OAM admin user credential from the credential store`

- **ODI Repository URLs**
  Finds all jdbc connection URLs in the ODI repository and validates that they point to the same database as the database that is referenced in the `DB_CONNECT_STRING` parameter in `Fusion_env.properties`.

- **ODI supervisor credentials**
  Confirms the correct connection URLs exist in the ODI Repository.

- **OHS Instance Registration**
  Verifies that the OHS instance is registered in `topology.xml`.

- **OHS Process Status on OHS Using OPMN**
  Check if the OHS process is up on the OHS host.

- **OPatch Version in FA_ORACLE_HOME**
  Verifies that the version of OPatch is compatible with Oracle Fusion Applications. If an incompatible version of OPatch exists in `FA_ORACLE_HOME`, errors can occur while applying patches and running RUP Installer.

- **Open File Limit**
Utilities Run by Upgrade Orchestrator

Verifies the open file limit. RUP Installer uses multiple workers for uploading database content. The number of workers used dictates the open file limit setting for the machine where you run the RUP Installer. To understand how the number of workers are calculated and the requirement for the open file limit setting for the workers, see "Patching Database Artifacts" in the Oracle Fusion Applications Patching Guide. For more information, see "Increase the Open Files Limit" in the Oracle Fusion Applications Installation Guide.

- Oracle Homes are Registered in the Central Inventory
  Verifies that the Oracle Business Intelligence, Global Order Processing, Web Tier, and Web Tier Common Oracle home directories are registered for use by Oracle Fusion Applications.

- ORACLE_COMMON Inventory Location on OHS
  Verifies that the OH home and the Oracle Common home are pointing to the correct inventory location on OHS in WT_MIDDLEWARE_HOME/oracle_common/oraInst.loc.

- OS Attributes
  Validates the operating system name, architecture and versions.

- Password Expiry For Critical Bind Users in LDAP
  Verifies that the passwords for critical bind users are not locked and will not expire within the next three days.

- Read Write Access to APPLICATIONS_BASE
  Verifies that directory the APPLICATIONS_BASE directory has read-write access.

- Remote OPMN Access
  Verifies that the remote OPMN process is accessible.

- Size and Contents of default-keystore.jks File in All Domains
  Verifies that the size of the default-keystore.jks file for all domains is same as that of CommonDomain.

- Taxonomy URL
  Verifies the TAXONOMY_URL value, which is obtained from FUSION_env.properties.

- User Administrator or Super User Role
  Verifies that the owner of APPLICATIONS_BASE is the same as the user who is running Health Checker.

- Virtual Hosts Wiring
  Verifies that the host and port wirings in the APPLICATIONS_CONFIG/CommonDomain_webtier/config/OHS/ohs1/moduleconf/FusionVirtualHost_app.conf files are correct.

- WSM-PM Application is Active
  Verifies that the WSM-PM application is running on all SOA domains.

A.3.2.2 Pre-Downtime Upgrade Tasks
The following checks occur when Health Checker runs using the PreDowntimeUpgradeReadinessHealthChecks.xml manifest.

- Base SOA Composites Exist
Utilities Run by Upgrade Orchestrator

Verifies that all base SOA composites exist for the versions that are going to be upgraded by a patch.

- Data Guard State
  Checks if Data Recovery is enabled in the environment and that it is stopped before the upgrade.

- Environment Properties on OHS
  This plug-in verifies the properties used by the RUP Lite for OHS utility.

- Free and Total Memory
  Verifies that the primordial host has enough free memory for the upgrade. The required memory is calculated based on which domains and servers are configured to run on the host where the Health Checker is run.

- Free Disk Space
  Checks for free and usable disk space on the primordial and non-primordial Oracle Fusion Applications hosts.

- HCM Workforce Reputation Offerings Shared Mount
  If the environment is provisioned with HCM Workforce offerings, verifies if the environments have the mandatory shared directory and mount point configured.

- Middleware Installer exists in Release Repository
  Verifies that all Middleware installers exist in the repository.

- No Locked ODI Objects or SES Objects Exist
  Verifies that there are no locked objects in the FUSION_ODI and SES schemas.

- No Patch Conflicts Exist
  Runs the PatchConflictManager utility to remove conflicting patches.

- WLS Edit Sessions and Unactivated Changes Exist
  Verifies that no WLS edit sessions or unactivated changes exist.

- OHS Process Status on OHS Using OPMN
  Verifies that the OHS process is up and running on the OHS host.

- Oracle Fusion Applications Release Version:
  To install Release 7, the installed Oracle Fusion Applications version must be Release 6. This plug-in ensures that the installed version of Oracle Fusion Applications is 11g Release 6, (11.1.6.0.0).

- Permissions For Temp Directory
  Verifies that files in the temporary directory that match the pattern, /tmp/*pki*, are owned by the same user that starts servers.

- Availability of ports for new Managed Servers
  Verifies the availability of ports for managed servers that were added. This plug-in is available only in Release 7.

- Properties for DB Host Upgrade
  Verifies that the environment properties to be used for DB Host upgrade are valid.

- Repository Integrity
Checks whether all required files are present in the repository and reports any missing files.

- **Seed Data For Potential Conflicts**
  Performs a set of validations to prevent potential seed data failures.

- **SES Schedules and Index Optimizer are Stopped/Disabled**
  Verifies that SES schedules and the index optimizer are stopped.

- **SOA Platform is Ready**
  Verifies whether the SOA platform is ready for each domain that is impacted by the contents of the upgrade.

- **Sessions holding 'library cache load lock' in Fusion Schema of Oracle Fusion Applications Database**
  Checks whether there are any database sessions that are holding a "library cache load lock" in the Fusion schema of the Oracle Fusion Applications database.

- **Total Memory and Swap**
  Verifies there is sufficient memory for upgrading. The memory requirement calculation is based on the domains and servers that are configured to run where Health Checker runs.

A.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.

- **AD Admin Sessions, AutoPatch and Patch Manager Processes are Complete**
  Checks whether any AD Administration, AutoPatch or Patch Manager processes are running.

- **Credential Store Connectivity**
  Checks if a connection can be established to the credential store.

- **Data Guard State**
  Checks if Data Recovery is enabled in the environment and that it is stopped before the upgrade.

- **Database Instance Connectivity**
  Checks if the database instance is up. For RAC databases, checks if all nodes are up.

- **Database version**
  Checks if Oracle Database version is above the minimum required for Oracle Fusion Applications 11g Release 8 (11.1.8).

- **Database is Running and in Idle State**
  Verifies that no SQL sessions, jobs, or processes are running or are scheduled to be running against the database.

- **Free Memory and Swap**

- **Identity and Policy Store LDAP**
  Verifies the connectivity to the identity store and policy store LDAP using identity store credentials.
Utilities Run by Upgrade Orchestrator

A-23

Additional Information About Upgrade Orchestrator

- **Identity Store Connectivity using jps-config-jse.xml**
  Verifies that the idstore.ldap.provider in jps-config-jse.xml can be used to connect to the identity store.

- **Invalid Objects**
  Checks for and reports any invalid objects.

- **JAZN Version in Oracle_Home Matches LDAP**
  Verifies that the JAZN version in system-jazn-data.xml is the same as the version in the policy store.

- **Mandatory Patches Have Been Applied**
  Verifies that mandatory patches have been applied.

- **MDS Schema Connectivity in RUP1 Env**
  Checks database connectivity for schemas that contain FUSION_MDS in their name.

- **Middleware Schema Connectivity in RUP1 Env**
  Checks database connectivity for all schemas except for FUSION_MDS schemas.

- **Node Managers are down**
  Verifies Node Managers are down.

- **Administration Servers and Managed Servers are Down**
  Confirms that all relevant Administration Servers and Managed Servers are down.

**A.3.2.2.4 Post-Upgrade Tasks Performed by Health Checker** The following checks occur when Health Checker runs the PostUpgradeHealthChecks.xml manifest.

- **AD Admin Sessions, AutoPatch and Patch Manager Processes are Complete**
  Checks whether any AD Administration, AutoPatch or Patch Manager processes are running.

- **Data Guard State**
  Checks if Data Recovery is enabled in the environment and that it is stopped before the upgrade.

- **Database version**
  Checks if Oracle Database version is above the minimum required for Oracle Fusion Applications 11g Release 8 (11.1.8).

- **Installed Languages are Upgraded to Release**
  Checks if a language pack has been upgraded to the current release or needs to be upgraded to the current release.

- **JAZN Conflicts**
  Validates the results of the JAZN analysis reports for each stripe to find any potential conflicts or deletions that were not patched automatically by the installer.

- **Locked ODI Objects or SES Objects**
  Verifies that there are no locked objects in the FUSION_ODI and SES schema.

- **Permissions For Temp Directory**
Utilities Run by Upgrade Orchestrator

Verifies that files in the temporary directory that match the pattern, /tmp/*pki*, are owned by the same user that starts servers.

- SOA Composites in the Repository are Deployed
  Verifies that the SOA composites in the repository were deployed by the upgrade.

- SOA Platform is Ready
  Verifies whether the SOA platform is ready for each domain that is impacted by the contents of the upgrade.

- WLS Edit Sessions and Unactivated Changes
  Verifies that no WLS edit sessions or unactivated changes exist.

A.3.2.2.5 Language Pack Readiness Health Checks The following checks occur when Health Checker runs the LanguagePackReadinessHealthChecks.xml manifest. You typically run this manifest before you install a language pack. For more information, see "Installing and Maintaining Oracle Fusion Applications Languages" in Oracle Fusion Applications Administrator’s Guide.

- AD Admin Sessions, AutoPatch and Patch Manager Processes are complete
  Checks whether any AD Administration, AutoPatch or Patch Manager processes are running.

- All Installed Languages are Upgraded to Release
  Checks if a language pack has been upgraded to the current release or needs to be upgraded to the current release.

- Database is Running and in Idle State
  Verifies that no SQL sessions, jobs, or processes are running or are scheduled to be running against the database.

- Repository Integrity
  Checks whether all required files are present in the repository and reports any missing files.

- SOA Platform is Ready
  Verifies whether the SOA platform is ready for each domain that is impacted by the contents of the upgrade.

A.3.2.2.6 Post Language Pack Health Checks The following checks occur when Health Checker runs the PostLanguagePackHealthChecks.xml manifest. You typically run this manifest after you install a language pack. For more information, see "Installing and Maintaining Oracle Fusion Applications Languages" in the Oracle Fusion Applications Administrator’s Guide.

- JAZN Conflicts
  Validates the results of the JAZN analysis reports for each stripe to find any potential conflicts or deletions that were not patched automatically by the installer.

A.3.2.2.7 Patching Readiness Health Checks The following checks occur when Health Checker runs the PatchingReadinessHealthChecks.xml manifest. You typically run this manifest before applying a patch. For more information, see "Step 7 Prepare the System" in the Oracle Fusion Applications Patching Guide.

- AD Admin Sessions, AutoPatch and Patch Manager Processes are complete
Checks whether any AD Administration, AutoPatch or Patch Manager processes are running.

- **Base SOA Composites Exist**
  Verifies that all base SOA composites exist for the versions that are going to be upgraded by a patch.

- **Database version**
  Checks if Oracle Database version is above the minimum required for Oracle Fusion Applications 11g Release 8 (11.1.8).

- **Database is Running and in Idle State**
  Verifies that no SQL sessions, jobs, or processes are running or are scheduled to be running against the database.

- **IPM server status**

- **No Locked ODI Objects or SES Objects Exist**
  Verifies that there are no locked objects in the FUSION_ODI or SES schema.

- **WLS Edit Sessions and Unactivated Changes Exist**
  Verifies that no WLS edit sessions or unactivated changes exist.

- **SOA Platform is Ready**
  Verifies whether the SOA platform is ready for each domain that is impacted by the contents of the upgrade.

**A.3.2.2.8 Post Patching Health Checks** The following checks occur when Health Checker runs the PostPatchingHealthChecks.xml manifest. You typically run this manifest after applying a patch. For more information, see "Step 11 Run Health Checker for Post Patching Health Checks" in the Oracle Fusion Applications Patching Guide

- **AD Admin Sessions, AutoPatch and Patch Manager Processes are complete**
  Checks whether any AD Administration, AutoPatch or Patch Manager processes are running.

- **JAZN Conflicts**
  Validates the results of the JAZN analysis reports for each stripe to find any potential conflicts or deletions that were not patched automatically by the installer.

- **No Locked ODI Objects or SES Objects Exist**
  Verifies that there are no locked objects in the FUSION_ODI schema.

- **WLS Edit Sessions and Unactivated Changes Exist**
  Verifies that no WLS edit sessions or unactivated changes exist.

**A.3.2.2.9 Data Quality Check** The Validating JAZN Policy Data check occurs when Health Checker runs the DataQualityChecks.xml manifest.

**A.3.2.2.10 Vital Signs Check** The following checks occur when Health Checker runs the VitalSignsChecks.xml manifest.

- **Database Instance Connectivity**
  Checks if the database instance is up. For RAC databases, checks if all nodes are up.
Utilities Run by Upgrade Orchestrator

- Fusion Schema Connectivity
  Validates the database connectivity to all Fusion schemas.
- Identity and Policy Store LDAP
  Verifies the connectivity to the identity store and policy store LDAP using identity store credentials.
- Identity Store Connectivity using jps-config-jse.xml
  Verifies that the idstore.ldap.provider in jps-config-jse.xml can be used to connect to the identity store.
- MDS Schema Connectivity
  Checks database connectivity for schemas that contain FUSION_MDS in their name.
- Middleware Schema Connectivity
  Checks database connectivity for all schemas except for FUSION_MDS schemas.
- Verify All Admin Servers and Managed Servers are Up
  Verifies that all Administration and Managed Servers are up.

A.3.2.3 Override Health Checks
The Health Checker utility offers a method for you to manage which health checks run on your environment. For example, you may want to exclude a health check that is related to a known issue in an environment. You can also add a new check to an existing Health Checker plug-in, if needed. The configuration parameters for Health Checker are stored in the REPOSITORY_LOCATION/installers/farup/Disk1/upgrade/config/healthchecks.xml file. You are not allowed to edit this file. If you want to override any configuration parameters or exclude certain plug-ins from running, you can create configuration override files.

Health Checker first loads the configuration parameters that are stored in healthchecks.xml and then it considers the configuration override files.

This section describes the following topics related to managing Health Checker sessions:

- Create Override Files
- Override Health Checker Configuration Parameters
- Example For Overriding Health Checks
- Disable a Plug-in
- Customize Plug-in Timeouts

A.3.2.3.1 Create Override Files
The first step in overriding the standard checks run by Health Checker is to create one or more override files. To create an override file, copy the appropriate override template to the override directory, which defaults to location SHARED_UPGRADE_LOCATION/healthchecker/POD_NAME and rename this file to eliminate the .template extension. The following templates are located in the ORCH_LOCATION/fusionapps/applications/lcm/hc/config directory. ORCH_LOCATION is where orchestration.zip is unzipped, as described in Section 2.3.7, "Unzip Orchestration.zip".

- ALL_overrides.xml.template
- DB_overrides.xml.template
- MIDTIER_overrides.xml.template
- OHS_overrides.xml.template
- PRIMORDIAL_overrides.xml.template

Select the template that corresponds to the host type for which you want to create the overrides. For example, if you want to create overrides for the primordial host, use PRIMORDIAL_overrides.xml. If the override applies to all hosts, use ALL_overrides.xml.

The default location for override files is SHARED_UPGRADE_LOCATION/healthchecker/POD_NAME.

A.3.2.3.2 Override Health Checker Configuration Parameters To override configuration parameters within an override file, uncomment the XML portion of the override file, and customize the override file to meet your requirements. Remove all values from the override file except for the values that you want to exclude. To disable a check, add disabled=true to the check. To add a check, add the value to the override file.

A.3.2.3.3 Example For Overriding Health Checks This example shows how to customize the list of URIs that are verified by Health Checker. The following steps describe this customization:

1. Copy the template for the override file.

   ```bash
cp REPOSITORY_LOCATION/installers/farup/Disk1/upgrade/config/ALL_overrides.xml.template SHARED_UPGRADE_LOCATION/healthchecker/POD_NAME/ALL_overrides.xml
   ```

2. Uncomment the XML portion of the override file.

   The original override file looks like this:
   ```xml
   <!--
   <checks category="context_root_locations">
   <check value="/console"/>
   <check value="/soa-infra"/>
   <check value="/wsm-pm"/>
   <check value="/apm"/>
   <check value="/setup"/>
   <check value="/helpPortal"/>
   <check value="/fndSetup"/>
   <check value="/homePage"/>
   </checks>
   -->
   ```
   After removing the XML comment lines, <!--, the -->, the override file now looks like this:
   ```xml
   <checks category="context_root_locations">
   <check value="/console"/>
   <check value="/soa-infra"/>
   <check value="/wsm-pm"/>
   <check value="/apm"/>
   <check value="/setup"/>
   <check value="/helpPortal"/>
   <check value="/fndSetup"/>
   <check value="/homePage"/>
   </checks>
   ```

3. Remove all rows except those that you want to exclude. In this example, you do not want Health Checker to validate the URI for soa-infra and you want to add a
validation for myuri. To disable a check, add disabled="true" to the check. To add a URI to be checked, add the URI to the override file. The override file now looks like this:

```xml
<checks category="context_root_locations">
  <check value="/soa-infra" disabled="true"/>
  <check value="/myuri"/>
</checks>
```

**A.3.2.3.4 Disable a Plug-in** To disable a plug-in, you must first find its display name (from the HTML report), its class name (from the log file), or its ID (from the manifest). The following example displays how a plug-in is defined in a Health Checker manifest file:

```xml
<plugin id="TotalMemoryCheck" description="Verifying Total Memory and Swap" invoke=""
plugin.class="oracle.check.sys.TotalMemCheckPlugin"
```

The following example depicts how you can override the plug-in in the override file. This example shows the display name, class name, and ID for the plug-in, but only one of these is required. Note that excluded plug-ins must be listed under the 'exclude' category.

```xml
<checks category="exclude">
  <check name="TotalMemoryCheck"/>
</checks>

Or:

```xml
<checks category="exclude">
  <check name="Verifying Total Memory and Swap"/>
</checks>

Or:

```xml
<checks category="exclude">
  <check name="oracle.check.sys.TotalMemCheckPlugin"/>
</checks>

Or:

```xml
<checks category="exclude">
  <check name="TotalMemCheckPlugin"/>
</checks>
```

**A.3.2.3.5 Customize Plug-in Timeouts** To prevent a plug-in timeout while Health Checker runs, you can create an override file to specify a longer timeout. You must know the plug-in class name, and the timeout value in seconds to modify the value. You can find the plug-in class name in the Health Checker manifest. In the following example, the plug-in class name for the Verify DataSource connectivity check is oracle.check.apps.VerifyDSConnectivity.

```xml
<GeneralSystemHealthChecks.xml plugin id="DSStatusPlugin"
GeneralSystemHealthChecks.xml description="Verify DataSource connectivity"
GeneralSystemHealthChecks.xml invoke=""
GeneralSystemHealthChecks.xml plugin.class="oracle.check.apps.VerifyDSConnectivity"
GeneralSystemHealthChecks.xml class.path="$HC_LOCATION/lib/precheckplugin.jar;
GeneralSystemHealthChecks.xml $HC_LOCATION/lib/hccommon.jar"
GeneralSystemHealthChecks.xml stoponerror="false"/>
```
To find the current timeout value, open the healthchecker log file and find the portion of the log that was produced by the plug-in. The log includes the current timeout value, as shown in the following examples:

```
[2013-08-08T22:35:42.791+00:00] [healthcheckplug] [NOTIFICATION] []
[oracle.healthcheckplug] [tid: 10] [ecid: 0000K1W4R2R3v1G5IzXBif111oQ000000,0]
Using default timeout of 120 seconds
```

```
[2013-08-08T22:35:17.877+00:00] [healthcheckplug] [NOTIFICATION] []
[oracle.healthcheckplug] [tid: 10] [ecid: 0000K1W4R2R3v1G5IzXBif111oQ000000,0]
[SRC_CLASS: oracle.check.common.util.Utils] [SRC_METHOD: getTimeout] Timeout for VerifyDSConnectivity is 901 seconds
```

Perform the following steps to modify the timeout value.

1. Create the override file as described in Section A.3.2.3.1, "Create Override Files".
2. Go to the timeout_seconds section as shown in the following example.

   ```
   <!-- Timeout, used by plugins for running external commands or wlst scripts or ...
   ... -->
   <checks category="timeout_seconds">
   <check name="VerifyDSConnectivity" value="600"/>
   <check name="LdapDataQualityCheckPlugin" value="1800"/>
   <check name="ContextRootCheckPlugin" value="1800"/>
   </checks>
   ```

3. If the plug-in is already listed in this section, set the new timeout value in seconds. If the plug-in is not listed, add it.

   In the following example, the timeout for `Verify DataSource connectivity` (oracle.check.apps.VerifyDSConnectivity) is set to 45 minutes (2700 seconds).

   ```
   <!-- Either of the two lines below changes the timeout to 2700 -->
   <check name="VerifyDSConnectivity" value="600"/>
   <check name="oracle.check.apps.VerifyDSConnectivity" value="2700"/>
   ```

A.3.3 RUP Lite for OVM Utility

The RUP Lite for OVM utility addresses the differences between a newly provisioned Oracle VM environment on the latest release and an Oracle VM environment provisioned in a previous release. You run RUP Lite for OVM only if you are running Oracle Fusion Applications in an Oracle VM environment that was created from the official releases of Oracle VM templates for Oracle Fusion Applications Release 2 (11.1.2) and higher. This utility is not applicable for any Oracle VM environments that are created using other methods.

The following steps provide an overview of how Upgrade Orchestrator supports RUP Lite for OVM when upgrading from Release 7 to Release 8.

Note that log files for RUP Lite for OVM are located under the location from where you are running RUP Lite for OVM. An example location for running RUP Lite for OVM in offline mode follows:

```
/u01/lcm/rupliteovm/output/logs/11.1.8.0.0/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 offline mode.

<table>
<thead>
<tr>
<th>Table A–7 Offline Plug-ins for RUP Lite for OVM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plug-in Name</strong></td>
</tr>
<tr>
<td>ValidateEnvironment</td>
</tr>
<tr>
<td>SetupCredentials</td>
</tr>
<tr>
<td>ApplyMemorySettings</td>
</tr>
<tr>
<td>GenerateOptimizedQueryPlans</td>
</tr>
<tr>
<td>UpdateODIUnicastConfiguration</td>
</tr>
<tr>
<td>UpdateFusionIIRScripts</td>
</tr>
</tbody>
</table>

The following table describes the plug-ins that are included in RUP Lite for OVM in online mode.

<table>
<thead>
<tr>
<th>Table A–8 Online Plug-ins for RUP Lite for OVM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plug-in Name</strong></td>
</tr>
<tr>
<td>ValidateEnvironment</td>
</tr>
<tr>
<td>SetupOnlineCredentials</td>
</tr>
<tr>
<td>DeployECSF</td>
</tr>
</tbody>
</table>
A.3.4 RUP Lite for OHS Utility

The *RUP Lite for OHS* utility manages the steps required to update Web Gate, OHS, and *ORACLE_COMMON*. The following steps are performed by RUP Lite for OHS to accomplish this upgrade:

- Stop Oracle Process Manager and Notification Server (OPMN) processes.
- Apply OPatches from the repository to Web Gate, OHS, and *ORACLE_COMMON*.
- Apply manually downloaded OPatches to Web Gate, OHS, and *ORACLE_COMMON*.
- Update the OHS configuration files.
- Apply OHS settings changes.
- Start the OPMN server process.
- Start the OHS instance.

A.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.
Upgrade Orchestrator Properties Files

This appendix describes the properties files used by Upgrade Orchestrator.

Orchestration runs using the properties defined in five properties files: pod.properties, PRIMORDIAL.properties, OHS.properties, MIDTIER.properties, and IDM.properties. The properties are set to specific values as part of your preparation to begin the upgrade. To configure any property, follow the instructions for each property’s description in the respective property file. The following properties files are required by Upgrade Orchestrator:

- pod.properties
- PRIMORDIAL.properties
- MIDTIER.properties
- IDM.properties
- OHS.properties

B.1 pod.properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORCHESTRATION_CHECKPOINT_LOCATION</td>
<td>Yes</td>
<td>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.</td>
</tr>
<tr>
<td>ORCHESTRATION_CHECKPOINT_ARCHIVE_LOCATION</td>
<td>Yes</td>
<td>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.</td>
</tr>
<tr>
<td>HOSTNAME_PRIMORDIAL</td>
<td>Yes</td>
<td>The host name of your Oracle Fusion Applications primordial host. This must be one and only one host name.</td>
</tr>
</tbody>
</table>
### Table B–1 (Cont.) pod.properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOSTNAME_MIDTIER</td>
<td>Yes</td>
<td>A comma separated list of all host names of your Oracle Fusion Applications Mid tier hosts. In Oracle VM environments, this must be a comma separated list of host names for primary, secondary, and BI hosts.</td>
</tr>
<tr>
<td>HOSTNAME_PRIMARY</td>
<td>Yes</td>
<td>A comma separated list of all host names of your Oracle Fusion Applications primary hosts. This is applicable only for Oracle VM environments.</td>
</tr>
<tr>
<td>HOSTNAME_SECONDARY</td>
<td>Yes</td>
<td>A comma separated list of all host names of your Oracle Fusion Applications secondary hosts. This is applicable only for Oracle VM environments.</td>
</tr>
<tr>
<td>HOSTNAME_BIINSTANCE</td>
<td>Yes</td>
<td>A comma separated list of all host names of your Oracle Fusion Applications BI hosts. This is applicable only for Oracle VM environments.</td>
</tr>
<tr>
<td>HOSTNAME_OSN</td>
<td>Yes</td>
<td>This property is not applicable.</td>
</tr>
<tr>
<td>HOSTNAME_OHS</td>
<td>Yes</td>
<td>A comma separated list of all host names for the Oracle Fusion Applications Web tier (APPOHS).</td>
</tr>
<tr>
<td>HOSTNAME_IDMOID</td>
<td>Yes</td>
<td>Host name, virtual or actual, of the OID server, for example, server_name.oracleoutsourcing.com.</td>
</tr>
<tr>
<td>HOSTNAME_IDMOIM</td>
<td>Yes</td>
<td>Host name, virtual or actual, of the OIM server, for example, server_name.oracleoutsourcing.com.</td>
</tr>
<tr>
<td>HOSTNAME_IDMOHS</td>
<td>Yes</td>
<td>Host name, virtual or actual, of the AuthOHS server, for example, server_name.oracleoutsourcing.com.</td>
</tr>
<tr>
<td>EMAIL_TO_RECIPIENT</td>
<td>Yes</td>
<td>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.</td>
</tr>
<tr>
<td>EMAIL_CC_RECIPIENT</td>
<td>No</td>
<td>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.</td>
</tr>
<tr>
<td>EMAIL_SENDER</td>
<td>No</td>
<td>The email address of the sender from which you want notifications to be sent. This must be a single value, such as <a href="mailto:no-reply@domain.com">no-reply@domain.com</a>.</td>
</tr>
<tr>
<td>EMAIL_DEFAULT_ENGINE</td>
<td>Yes</td>
<td>Valid email engine that can be used on all hosts for this pod. The default value is /usr/sbin/sendmail.</td>
</tr>
<tr>
<td>EMAIL_PROTOCOL</td>
<td>No</td>
<td>Value must always be smtp as that is only supported protocol.</td>
</tr>
<tr>
<td>SMTP_HOSTNAME</td>
<td>No</td>
<td>The valid smtp host name. The default value is localhost.</td>
</tr>
<tr>
<td>SMTP_PORT_NUMBER</td>
<td>No</td>
<td>The SMTP protocol port number.</td>
</tr>
<tr>
<td>SMTP_AUTHORIZATION</td>
<td>No</td>
<td>A true or false value to indicate whether authorization key is used to connect to the SMTP server. The default value is false.</td>
</tr>
<tr>
<td>SMTP_AUTH_USER</td>
<td>No</td>
<td>The SMTP authorized user id.</td>
</tr>
<tr>
<td>SMTP_AUTH_PASSWORD</td>
<td>No</td>
<td>The SMTP authorized password.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Mandatory</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SMTP_AUTH_ENCRYPTED_PASSWORD</td>
<td>No</td>
<td>The encrypted SMTP authorized password. If this property is empty, the SMTP_AUTH_PASSWORD value is used.</td>
</tr>
<tr>
<td>SMTP_SOCKET_FACTORY_CLASS</td>
<td>No</td>
<td>The factory class name to connect to the SMTP server.</td>
</tr>
<tr>
<td>REL8_REPOSITORY_LOCATION</td>
<td>Yes</td>
<td>The location where the Release 8 repository is downloaded to a shared mount, for example SHARED_LOCATION/11.1.8.0.0/Repository. As a best practice, it should be on the shared mount that is shared across all pods or environments.</td>
</tr>
<tr>
<td>SHARED_UPGRADE_LOCATION</td>
<td>Yes</td>
<td>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.</td>
</tr>
<tr>
<td>THREAD_POOL_SIZE</td>
<td>Yes</td>
<td>This property is used for parallel execution of tasks within orchestration. You can choose to change the default value of 10 to a different numeric value if you want to control how many tasks run in parallel. For example, a value of 1 means everything runs sequentially, a value of 2 means only two tasks can run in parallel.</td>
</tr>
<tr>
<td>PATCH_CONFLICT_MANAGER_LOCATION</td>
<td>Yes</td>
<td>The location of the patch conflict manager utility that you create in Section 2.3.4, &quot;Download and Unzip the Patch Conflict Manager Utility&quot;. The default value is/u01/PatchConflictManager.</td>
</tr>
<tr>
<td>SAAS_ENV</td>
<td>Yes</td>
<td>This property should be set to true only if your Oracle VM environments are created in the Oracle Cloud Customer Environment.</td>
</tr>
<tr>
<td>SAAS_FACONTROL_SCRIPTS_LOCATION</td>
<td>No</td>
<td>This property is not applicable.</td>
</tr>
<tr>
<td>REL8_SAAS_LCM_INSTALLER_DIR</td>
<td>Yes for Oracle VM</td>
<td>This property is applicable to Oracle Fusion Applications VMs only. This is the directory where FASAASLCMTOOLS.zip is downloaded and unzipped. As a best practice it should be on the shared mount that is shared across all pods/environments. SHARED_LOCATION/11.1.8.0.0/fasaaslcmtools is an example.</td>
</tr>
<tr>
<td>ORCH_REPORT_LOCATION</td>
<td>No</td>
<td>A shared location accessible to all hosts that is used to save the upgrade report, as described in Section A.1.3, &quot;Oracle Fusion Applications Orchestrator Upgrade Report.”</td>
</tr>
<tr>
<td>REL8_DOWNLOADED_PATCHES_LOCATION</td>
<td>No</td>
<td>The location of the post-release 8 patches that are identified as critical for upgrade, as described in Section 2.3.5.3, &quot;Download and Unzip Mandatory Post-Release 8 Patches.” This directory should be on a shared mount point shared across all hosts and ideally all pods, for example, SHARED_LOCATION/11.1.8.0.0_post_repos.</td>
</tr>
<tr>
<td>HC_OVERRIDE_FILES</td>
<td>No</td>
<td>The location of the directory that contains Health Checker configuration override files. The default value is APPLICATIONS_CONFIG/fapatch/healthchecker.</td>
</tr>
</tbody>
</table>
### B.2 PRIMORDIAL.properties

#### Table B–2  PRIMORDIAL.properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REL8_LP_REPOSITORY_LOCATION</td>
<td>Yes, if upgrading languages</td>
<td>The location of all Release 8 Language Pack repositories, as described in Section 2.3.5.2, &quot;Download and Unzip Release 8 Language Packs.&quot; This directory should be on a shared mount point shared across all pods/environments, for example, SHARED_LOCATION/11.1.8.0.0/LPRepository.</td>
</tr>
<tr>
<td>REL8_RUPINSTALLER_UPGRADE_PARAM</td>
<td>No</td>
<td>You can leave this property blank because its value is automatically set by Upgrade Orchestrator during the upgrade. Alternatively, you can provide a space separated list of command line options passed to the RUP and Language Pack installers. For a list of options, refer to “Table 3-6” in the Oracle Fusion Applications Administrator’s Guide. If you set this parameter manually, use only -D options. Do not use -J-D options.</td>
</tr>
<tr>
<td>MANIFEST_FILE</td>
<td>Yes</td>
<td>The file name and location for the .xml manifest file for the host type and the upgrade level. For the Release 8 upgrade, the value should be ORCH_LOCATION/config/rel8_primordial.xml.</td>
</tr>
<tr>
<td>APPLICATIONS_BASE</td>
<td>Yes</td>
<td>The top-level directory for the Oracle Fusion Applications binaries. The default value is /u01/APPLTOP.</td>
</tr>
<tr>
<td>JRE_LOC</td>
<td>Yes</td>
<td>The absolute path where the Java Runtime Environment is installed. This option does not support relative paths. The default value is /u01/APPLTOP/fusionapps/jdk6.</td>
</tr>
<tr>
<td>SKIP_UPGRADE_FOR_LANGUAGE</td>
<td>No</td>
<td>A comma separated list of languages that you do not want orchestration to upgrade. The list items must:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Meet ISO language code convention</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Be a previously installed language</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Not be the JAZN policy store language</td>
</tr>
</tbody>
</table>
B.3 MIDTIER.properties

Table B–3 MIDTIER.properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPLICATIONS_BASE</td>
<td>Yes</td>
<td>The top-level directory for the Oracle Fusion Applications binaries. The default value is /u01/APPLTOP.</td>
</tr>
<tr>
<td>MANIFEST_FILE</td>
<td>Yes</td>
<td>The file name and location for the .xml manifest file for the host type and the upgrade level. For the Release 8 upgrade, the value should be ORCH_LOCATION/config/rel8_midtier.xml.</td>
</tr>
<tr>
<td>JRE_LOC</td>
<td>Yes</td>
<td>The absolute path where the Java Runtime Environment is installed. This option does not support relative paths. The default value is /u01/APPLTOP/fusionapps/jdk6.</td>
</tr>
</tbody>
</table>

B.4 IDM.properties

Table B–4 IDM.properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Mandatory</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MANIFEST_FILE</td>
<td>Yes</td>
<td>The file name and location for the .xml manifest file for the host type and the upgrade level. For the Release 8 upgrade, the value should be ORCH_LOCATION/config/rel8_idm.xml.</td>
</tr>
<tr>
<td>JRE_LOC</td>
<td>Yes</td>
<td>The absolute path where the Java Runtime Environment is installed. This option does not support relative paths. The default value is /u01/APPLTOP/fusionapps/jdk6.</td>
</tr>
</tbody>
</table>
| 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.

The possible values follow:

- MANUAL - The IDM upgrade is to be performed manually. If IDM is not Release 7 IDM Provisioned, orchestrator cannot upgrade IDM and this property must be set to MANUAL.
- SINGLE - All IDM Nodes (IDM, IAM, OHS) and the Database are installed on a single server.
- 3-NODE - The IDM, IAM and OHS Nodes are installed on independent servers and the Database is installed on the IDM node.
- 4-NODE - The Database, IDM, IAM and OHS Nodes are installed on independent servers.

SINGLE, 3-NODE, and 4-NODE topologies are supported for IDM upgrade through orchestrator. The property default value is 4-NODE.

REL8_IDM_UPGRADE_BINARIES_LOCATION No The location where Release 8 IDM binaries are downloaded, for example SHARED_LOCATION/11.1.8.0.0/IDMRepository.
### Table B–4  (Cont.) IDM.properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Mandator</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>REL8_IDM_UPGRADE_AUTOMATION_PROPERTIES_FILE</td>
<td>No</td>
<td>The absolute location of the patchAutomation.properties file to be used by the Release 8 IDM upgrade scripts. All properties related to IDM nodes (OID, OIM and OHS) are maintained in this file.</td>
</tr>
</tbody>
</table>

### 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. |

### B.5 OHS.properties

#### Table B–5  OHS.properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Mandator</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPLICATIONS_BASE</td>
<td>Yes</td>
<td>The top-level directory for the Oracle Fusion Applications binaries. The default value is /u01/APPLTOP.</td>
</tr>
<tr>
<td>MANIFEST_FILE</td>
<td>Yes</td>
<td>The file name and location for the .xml manifest file for the host type and the upgrade level. For the Release 8 upgrade, the value should be ORCH_LOCATION/config/rel8_ohs.xml.</td>
</tr>
<tr>
<td>RUPLITEOHS_UNZIP_LOCATION</td>
<td>Yes</td>
<td>Specify a location, local to the OHS host, where the web gate install zip file should be unzipped, to be used by the RUP Lite for OHS upgrade, for example, /u01/webgate.</td>
</tr>
<tr>
<td>JRE_LOC</td>
<td>Yes</td>
<td>The absolute path where the Java Runtime Environment is installed. This option does not support relative paths. An example is ORCH_LOCATION/jdk.</td>
</tr>
<tr>
<td>LOG_LOCATION</td>
<td>Yes</td>
<td>Location for logs to be written.</td>
</tr>
<tr>
<td>WT_MW_HOME</td>
<td>Yes</td>
<td>Location of the web tier MW_HOME, for example, /oracle/work/MW_HOME. If you have scaled out OHS hosts, copy this property for each OHS host, prefixed with the host name of the host to indicate the web tier MW_HOME location on the specific host.</td>
</tr>
<tr>
<td>WT_ORACLE_HOME</td>
<td>Yes</td>
<td>Location of the web tier directory, which is a sub-directory under WT_MW_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 web tier Oracle WT1 location on the specific host.</td>
</tr>
<tr>
<td>WT_CONFIG_HOME</td>
<td>Yes</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table B–5  (Cont.) OHS.properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Mandatory</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OHS_INSTANCE_ID</td>
<td>Yes</td>
<td>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.</td>
</tr>
<tr>
<td>OHS_UPGRADE_BINARIES_HOSTNAME</td>
<td>Yes</td>
<td>Comma separated list of your OHS host names which do not share the binaries.</td>
</tr>
</tbody>
</table>
This appendix describes how to start, stop and restart the various components of the Oracle Enterprise Deployment for Identity Management.

This appendix contains the following topics.

- Starting, Stopping, and Restarting Oracle HTTP Server
- Starting, Stopping, and Restarting Oracle Identity Manager
- Starting and Stopping Oracle Identity Federation Managed Servers
- Starting, Stopping, and Restarting Oracle Access Manager Managed Servers
- Starting, Stopping, and Restarting WebLogic Administration Server
- Starting and Stopping Oracle Virtual Directory
- Starting and Stopping Oracle Internet Directory
- Starting and Stopping Node Manager

C.1 Starting, Stopping, and Restarting Oracle HTTP Server

Prior to starting/stopping the Oracle HTTP server:

- Set ORACLE_INSTANCE to WEB_ORACLE_INSTANCE.
- Set ORACLE_HOME to WEB_ORACLE_HOME.
- Ensure that the ORACLE_HOME/opmn/bin appears in the PATH.

C.1.1 Starting Oracle HTTP Server

Start the Oracle Web Tier by issuing the command:

```
opmnctl startall
```

C.1.2 Stopping Oracle HTTP Server

Stop the Web Tier by issuing the command

```
opmnctl stopall
```

to stop the entire Web Tier or

```
opmnctl stopproc process-type=OHS
```

to stop Oracle HTTP Server only.
C.1.3 Restarting Oracle HTTP Server

You can restart the Web Tier by issuing a Stop followed by a Start as described in the previous sections.

To restart the Oracle HTTP server only, use the following command.

\texttt{opmnctl restartproc process-type=OHS}

C.2 Starting, Stopping, and Restarting Oracle Identity Manager

Start and stop Oracle Identity Manager and Oracle SOA Suite servers as follows:

C.2.1 Starting Oracle Identity Manager

To start the Oracle Identity Manager Managed Server(s), log in to the WebLogic console at: \texttt{http://ADMIN.mycompany.com/oamconsole}

Then proceed as follows:

1. Select \textbf{Environment - Servers} from the Domain Structure menu.
2. Click the \textbf{Control} tab.
3. Select \textbf{SOA Servers} (WLS\_SOA1 and/or WLS\_SOA2).

\textbf{Note:} You can start the Oracle Identity Manager and Oracle SOA Suite servers independently of each other. There is no dependency in their start order. However, the SOA server must be up and running for all of the Oracle Identity Manager functionality to be available.

4. Click the \textbf{Start} button.
5. Click \textbf{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 \textbf{Start}.
8. Click \textbf{Yes} when asked to confirm that you want to start the server(s).

C.2.2 Stopping Oracle Identity Manager

To stop the Oracle Identity Manager Managed Server(s), log in to the WebLogic console at: \texttt{http://ADMIN.mycompany.com/oamconsole}

Then proceed as follows:

1. Select \textbf{Environment - Servers} from the Domain Structure menu.
2. Click the \textbf{Control} tab.
3. Select \textbf{OIM Servers} (WLS\_OIM1 and/or WLS\_OIM2) and (WLS\_SOA1 and/or WLS\_SOA2).
4. Click the \textbf{Shutdown} button and select \textbf{Force Shutdown now}.
5. Click \textbf{Yes} when asked to confirm that you want to shutdown the server(s).
C.2.3 Restarting Oracle Identity Manager

Restart the server by following the Stop and Start procedures in the previous sections.

C.3 Starting and Stopping Oracle Identity Federation Managed Servers

Start and stop Oracle Identity Federation Managed Servers as follows:

C.3.1 Starting Oracle Identity Federation

To start the Oracle Identity Federation Managed Server(s), log in to the WebLogic console at: http://ADMIN.mycompany.com/oamconsole

Then proceed as follows:
1. Select Environment - Servers from the Domain Structure menu.
2. Click the Control tab.
3. Select OIF Servers (WLS_OIF1 and/or WLS_OIF2).
4. Click Start.
5. Click Yes when asked to confirm that you want to start the server(s).

C.3.2 Stopping Oracle Identity Federation

To stop the Oracle Identity Federation Managed Server(s), log in to the WebLogic console at: http://ADMIN.mycompany.com/oamconsole

Then proceed as follows:
1. Select Environment - Servers from the Domain Structure menu.
2. Click the Control tab.
3. Select OIF Servers (WLS_OIF1 and/or WLS_OIF2).
4. Click Shutdown and select Force Shutdown now.
5. Click Yes when asked to confirm that you want to shut down the server(s).

C.3.3 Restarting Oracle Identity Federation

Restart the server by following the previous Stop and Start procedures.

C.3.4 Starting and Stopping the EMAgent

Start the EMAgent by executing the following command:

```
ORACLE_INSTANCE/bin/emctl start all
```

You can verify that the instance started successfully by executing:

```
ORACLE_INSTANCE/bin/emctl status -l
```

Stop the EMAgent by executing the following command:

```
ORACLE_INSTANCE/bin/emctl stop all
```
C.3.5 Stopping the Oracle Identity Federation Instances and EMAgent

Stop the Oracle Identity Federation Instance and EMAgent by executing the following command:

```
OIF_ORACLE_INSTANCE/bin/opmnctl stopall
```

C.4 Starting, Stopping, and Restarting Oracle Access Manager Managed Servers

Start and stop Oracle Access Manager Managed Servers as follows:

C.4.1 Starting an Access Manager Managed Server When None is Running

Normally, you start Access Manager managed servers by using the WebLogic console. After you have enabled Single Sign-On for the administration consoles, however, you must have at least one Access Manager Server running in order to access a console. If no Access Manager server is running, the only way you can start one is from the command line.

To start WLS_OAM1 manually, use the command:

```
NSERVER_HOME/bin/startManagedWeblogic.sh WLS_OAM1 t3://ADMINVHN:7001
```

where 7001 is `WLS_ADMIN_PORT` in Section A.3.

C.4.2 Starting an Oracle Access Manager Managed Server When Another is Running

To start an Oracle Access Manager Managed Server when you already have another one running, log in to the WebLogic console at:

```
http://ADMIN.mycompany.com/oamconsole
```

Then proceed as follows:

1. Select `Environment - Servers` from the Domain Structure menu.
2. Click the `Control` tab.
3. Select `OAM Servers (WLS_OAM1 and/or WLS_OAM2)`.
4. Click the `Start` button.
5. Click `Yes` when asked to confirm that you want to start the server(s).

**Note:** After you have enabled single sign-on for the administration consoles, ensure that at least one Oracle Access Manager Server is running to enable console access.

If you have used the Oracle WebLogic console to shut down all of the Oracle Access Manager Managed Servers, then restart one of those Managed Servers manually before using the console again.

To start WLS_OAM1 manually, use the command:

```
NSERVER_HOME/bin/startManagedWeblogic.sh WLS_OAM1 t3://ADMINVHN:7001
```

C.4.3 Stopping Oracle Access Manager Managed Servers

To stop the Oracle Access Manager Managed Server(s), log in to the WebLogic console at:

```
http://ADMIN.mycompany.com/oamconsole
```
Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu.
2. Click the **Control** tab.
3. Select **OAM Servers (WLS_OAM1 and/or WLS_OAM2)**.
4. Click the **Shutdown** button and select **Force Shutdown now**.
5. Click **Yes** when asked to confirm that you want to shut down the server(s).

### C.4.4 Restarting Oracle Access Manager Managed Servers

Restart the server by following the **Stop and Start** procedures in the previous sections.

### C.5 Starting, Stopping, and Restarting WebLogic Administration Server

Start and stop the WebLogic Administration Server as described in the following sections.

---

**Note:** **Admin_user** and **Admin_Password** are only used to authenticate connections between Node Manager and clients. They are independent from the server administration ID and password and are stored in the `ASERVER_HOME/config/nodemanager/nm_password.properties` file.

---

### C.5.1 Starting WebLogic Administration Server

The recommended way to start the Administration server is to use WLST and connect to Node Manager:

```bash
cd ORACLE_COMMON_HOME/common/bin
./wlst.sh
```

Once in WLST shell, execute

```bash
nmConnect('Admin_User','Admin_Password','ADMINHOST1','5556', 'IDMDomain','ASERVER_HOME')
nmStart('AdminServer')
```

Alternatively, you can start the Administration server by using the command:

```
DOMAIN_HOME/bin/startWeblogic.sh
```

### C.5.2 Stopping WebLogic Administration Server

To stop the Administration Server, log in to the WebLogic console at:

```
http://ADMIN.mycompany.com/oamconsole
```

Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu.
2. Click the **Control** tab.
3. Select **AdminServer(admin)**.
4. Click **Shutdown** and select **Force Shutdown now**.
5. Click Yes when asked to confirm that you want to shut down the Administration Server.

C.5.3 Restarting WebLogic Administration Server

Restart the server by following the Stop and Start procedures in the previous sections.

C.6 Starting and Stopping Oracle Virtual Directory

Start and stop Oracle Virtual Directory as follows.

C.6.1 Starting Oracle Virtual Directory

Start system components such as Oracle Virtual Directory by typing:

```
ORACLE_INSTANCE/bin/opmnctl startall
```

You can verify that the system components have started by executing:

```
ORACLE_INSTANCE/bin/opmnctl status -l
```

C.6.2 Stopping Oracle Virtual Directory

Stop system components such as Oracle Virtual Directory by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl stopall
```

C.7 Starting and Stopping Oracle Internet Directory

Start and stop Oracle Internet Directory as follows.

C.7.1 Starting Oracle Internet Directory

Start system components such as Oracle Internet Directory by typing

```
ORACLE_INSTANCE/bin/opmnctl startall
```

You can verify that the system components have started by executing:

```
ORACLE_INSTANCE/bin/opmnctl status -l
```

C.7.2 Stopping Oracle Internet Directory

Stop system components such as Oracle Internet Directory by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl stopall
```

C.8 Starting and Stopping Node Manager

Start and stop the Node Manager as follows:
C.8.1 Starting Node Manager

If the Node Manager being started is the one that controls the Administration Server (IDMHOST1 or IDMHOST2), then prior to starting the Node Manager, set `JAVA_OPTIONS` to `-DDomainRegistrationEnabled=true` and issue the commands:

```
cd IAM_MW_HOME/wlserver_10.3/server/bin
./startNodeManager.sh
```

C.8.2 Stopping Node Manager

To stop Node Manager, kill the process started in the previous section.

C.8.3 Starting Node Manager for an Administration Server

Set the environment variable `JAVA_OPTIONS` to `-DDomainRegistrationEnabled=true` and issue the commands:

```
cd IAM_MW_HOME/wlserver_10.3/server/bin
./startNodeManager.sh
```

**Note:** It is important to set `-DDomainRegistrationEnabled=true` whenever you start a Node Manager that manages the Administration Server.