Contents

Preface

Audience viii
Documentation Accessibility viii
Related Documents viii
Conventions ix

1 Introduction to Upgrading Oracle Identity and Access Management to 12c (12.2.1.4.0)

About the Starting Points for a Oracle Identity and Access Management Upgrade 1-2
About the Oracle Identity and Access Management Upgrade Scenarios 1-2
About the New Features for Oracle Identity and Access Management 12c (12.2.1.4.0) 1-3
About Upgrade Restrictions 1-3
How to Use This Guide 1-4

2 Pre-Upgrade Requirements

Oracle Fusion Middleware Pre-Upgrade Checklist 2-1
Creating a Complete Backup 2-3
   Backing Up the Schema Version Registry Table 2-4
   Maintaining Customized Domain and Environment Settings 2-4
Cloning Your Production Environment for Testing 2-5
Verifying Certification and System Requirements 2-6
   Verify Your Environment Meets Certification Requirements 2-7
   Verify System Requirements and Specifications 2-7
      Migrating from a 32-Bit to a 64-Bit Operating System 2-8
   Verify That the Database Hosting Oracle Fusion Middleware is Supported 2-11
   Verify That the JDK Is Certified for This Release of Oracle Fusion Middleware 2-11
Updating Policy Files when Using Enhanced Encryption (AES 256) 2-12
Purging Unused Data 2-12
Creating a Non-SYSDBA User to Run the Upgrade Assistant 2-13
Identifying Existing Schemas Available for Upgrade 2-15
Part II  Upgrading Oracle Identity and Access Management Highly Available Environments

5  Upgrading Oracle Access Management Highly Available Environments

About the Oracle Access Management Multinode Upgrade Process 5-1
Backing up the 12c (12.2.1.3.0) Middleware Home Folder on OAMHOSTs 5-4
Uninstalling the Software on an OAMHOST 5-4
  Starting the Uninstall Wizard 5-4
  Selecting the Product to Uninstall 5-4
  Navigating the Uninstall Wizard Screens 5-5
Installing Product Distributions on OAMHOSTs 5-5
Running a Pre-Upgrade Readiness Check 5-6
  About Running a Pre-Upgrade Readiness Check 5-6
  Starting the Upgrade Assistant in Readiness Mode 5-7
  Upgrade Assistant Parameters 5-7
  Performing a Readiness Check with the Upgrade Assistant 5-9
  Understanding the Readiness Report 5-11
Starting the Servers on OAMHOSTs 5-17
6  Upgrading Oracle Identity Manager Highly Available Environments

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About the Oracle Identity Manager Multinode Upgrade Process</td>
<td>6-2</td>
</tr>
<tr>
<td>Backing up the 12c (12.2.1.3.0) Middleware Home Folder on OIMHOSTs</td>
<td>6-7</td>
</tr>
<tr>
<td>Stopping Servers and Processes</td>
<td>6-7</td>
</tr>
<tr>
<td>Uninstalling the Software on an OIMHOST</td>
<td>6-9</td>
</tr>
<tr>
<td>Starting the Uninstall Wizard</td>
<td>6-9</td>
</tr>
<tr>
<td>Selecting the Product to Uninstall</td>
<td>6-9</td>
</tr>
<tr>
<td>Navigating the Uninstall Wizard Screens</td>
<td>6-9</td>
</tr>
<tr>
<td>Installing Product Distributions on an OIMHOST</td>
<td>6-10</td>
</tr>
<tr>
<td>Upgrading Schemas on OIMHOST1</td>
<td>6-10</td>
</tr>
<tr>
<td>Upgrading Domain Component Configurations on OIMHOST1</td>
<td>6-11</td>
</tr>
<tr>
<td>Copying oracle.iam.ui.custom-dev-starter-pack.war to the 12c (12.2.1.4.0) Middleware Home</td>
<td>6-11</td>
</tr>
<tr>
<td>Starting the Servers on an OIMHOST</td>
<td>6-11</td>
</tr>
<tr>
<td>Packing Domain Configurations on OIMHOST1</td>
<td>6-12</td>
</tr>
<tr>
<td>Replicating the Domain Configurations on OIMHOST2</td>
<td>6-12</td>
</tr>
<tr>
<td>Updating the JDK location</td>
<td>6-13</td>
</tr>
<tr>
<td>Updating the setDomainEnv.sh file</td>
<td>6-13</td>
</tr>
</tbody>
</table>

7  Upgrading Oracle Access Management Multi-Data Center Environments

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About the Oracle Access Management Multi-Data Center Topology</td>
<td>7-2</td>
</tr>
<tr>
<td>Roadmap for Upgrading Oracle Access Management MDC Setup</td>
<td>7-3</td>
</tr>
<tr>
<td>Backing Up the Existing MDC Environment</td>
<td>7-4</td>
</tr>
<tr>
<td>Enabling Write Permission to Master and Clones (If Necessary)</td>
<td>7-4</td>
</tr>
<tr>
<td>Disabling and Deleting All Replication Agreements Between Master and Clone</td>
<td>7-5</td>
</tr>
<tr>
<td>Redirecting Traffic to Master Data Center</td>
<td>7-5</td>
</tr>
<tr>
<td>Upgrading Oracle Access Management on Clone Data Center</td>
<td>7-5</td>
</tr>
<tr>
<td>Redirecting Traffic to Clone Data Center</td>
<td>7-5</td>
</tr>
<tr>
<td>Upgrading Oracle Access Management on Master Data Center</td>
<td>7-5</td>
</tr>
<tr>
<td>Freezing all Changes to Clones (if Necessary)</td>
<td>7-6</td>
</tr>
<tr>
<td>Syncing Access Metadata</td>
<td>7-6</td>
</tr>
<tr>
<td>Creating Replication Agreement</td>
<td>7-6</td>
</tr>
<tr>
<td>Bringing up the Master and Clone Data Centers Online</td>
<td>7-7</td>
</tr>
</tbody>
</table>
# Troubleshooting the Oracle Identity and Access Management Upgrade

## Troubleshooting the Oracle Access Management Upgrade

<table>
<thead>
<tr>
<th>Issue</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation State is set as FAILED when Restarting the Admin Server</td>
<td>8-1</td>
</tr>
<tr>
<td>AMInitServlet Fails to Preload when Restarting OAM Managed Server</td>
<td>8-2</td>
</tr>
<tr>
<td>File Not Found Exception when Starting the OAM Managed Server</td>
<td>8-2</td>
</tr>
<tr>
<td>WADL Generation Does not Show Description</td>
<td>8-3</td>
</tr>
<tr>
<td>Troubleshooting Security Policy Issues When Upgrading</td>
<td>8-3</td>
</tr>
<tr>
<td>Modifying the Java Security Posture</td>
<td>8-4</td>
</tr>
<tr>
<td>Upgrade Scenarios for OAM</td>
<td>8-4</td>
</tr>
</tbody>
</table>

## Troubleshooting the Oracle Identity Manager Upgrade

<table>
<thead>
<tr>
<th>Issue</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reading CSF Key Fails when Running Upgrade Assistance (UA)</td>
<td>9-2</td>
</tr>
<tr>
<td>Access Denied Error when running the upgrade-sharedlibs.sh utility</td>
<td>9-3</td>
</tr>
<tr>
<td>KeystoreService Exception in the Logs After Reconfiguring the OIM Domain</td>
<td>9-3</td>
</tr>
<tr>
<td>Warning when Generating the Pre-Upgrade Report for OIM</td>
<td>9-5</td>
</tr>
<tr>
<td>OIM Bootstrap for DEPLOYSOACOMPOSITES Task Fails After Upgrade</td>
<td>9-6</td>
</tr>
<tr>
<td>Authorization Policy Merge Issue</td>
<td>9-7</td>
</tr>
<tr>
<td>MAR Update or Metadata Merge Issue</td>
<td>9-9</td>
</tr>
<tr>
<td>Error When Opening ADF DI Excel Sheet After Upgrade</td>
<td>9-10</td>
</tr>
<tr>
<td>Compilation Error When Starting the SOA Server After Upgrade</td>
<td>9-11</td>
</tr>
<tr>
<td>Warning in Oracle Identity Manager Server Logs After Upgrade</td>
<td>9-12</td>
</tr>
<tr>
<td>Default Challenges Questions are not Updated After Upgrade</td>
<td>9-12</td>
</tr>
<tr>
<td>EditFailedException When Releasing Configuration From WebLogic Console</td>
<td>9-13</td>
</tr>
<tr>
<td>OIM Application Deployment Fails Intermittently</td>
<td>9-13</td>
</tr>
<tr>
<td>Oracle Identity Manager Server Throws OutOfMemoryError</td>
<td>9-13</td>
</tr>
<tr>
<td>LDAP User Create and Update Reconciliation Job Fails</td>
<td>9-14</td>
</tr>
<tr>
<td>BI Managed Server is Seen on WebLogic Console After Upgrade</td>
<td>9-15</td>
</tr>
<tr>
<td>Empty Pages or Panels After Upgrade</td>
<td>9-15</td>
</tr>
</tbody>
</table>

## Updating the JDK After Installing and Configuring an Oracle Fusion Middleware Product

<table>
<thead>
<tr>
<th>Issue</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Updating the JDK Location After Installing an Oracle Fusion Middleware Product</td>
<td>A-1</td>
</tr>
<tr>
<td>Updating the JDK Location in an Existing Oracle Home</td>
<td>A-2</td>
</tr>
<tr>
<td>Updating the JDK Location in an Existing Domain Home</td>
<td>A-3</td>
</tr>
</tbody>
</table>
Preface

This document describes how to upgrade an existing Oracle Identity and Access Management environment to 12c (12.2.1.4.0).

- **Audience**
  Identify the target audience for your book and learn more about this document intended for.

- **Documentation Accessibility**

- **Related Documents**

- **Conventions**
  Learn about the conventions used in this document.

**Audience**

Identify the target audience for your book and learn more about this document intended for.

This document is intended for system administrators who are responsible for installing, maintaining, and upgrading Oracle Identity and Access Management. It is assumed that readers have knowledge of the following:

- Oracle Fusion Middleware system administration and configuration.
- Configuration parameters and expected behavior of the system being upgraded.

**Documentation Accessibility**

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

**Access to Oracle Support**

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

**Related Documents**

Refer to the Oracle Fusion Middleware Library for additional information.

- For installation information, see Fusion Middleware Installation Documentation.
- For upgrade information, see Fusion Middleware Upgrade Documentation.
• For administration-related information, see Fusion Middleware Administration Documentation.
• For release-related information, see Fusion Middleware Release Notes.

Conventions

Learn about the conventions used in this document.

This document uses the following text conventions:

<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>monospace</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>
Introduction to Upgrading Oracle Identity and Access Management to 12c (12.2.1.4.0)

Before you begin, review all introductory information to understand the standard upgrade topologies and upgrade paths for Oracle Identity and Access Management 12c (12.2.1.4.0).

Note:
The product Oracle Identity Manager is referred to as Oracle Identity Manager (OIM) and Oracle Identity Governance (OIG) interchangeably in the guide.

Note:
For general information about Fusion Middleware upgrade planning and other upgrade concepts and resources, see the following sections in Planning an Upgrade of Oracle Fusion Middleware:
- Planning an Upgrade to Oracle Fusion Middleware 12c (12.2.1.4.0)
- Understanding In-Place versus Out-of-Place Upgrades
- Understanding the Basic Upgrade Tasks

The following topics describe the concepts related to upgrading Oracle Identity and Access Management:

- **About the Starting Points for a Oracle Identity and Access Management Upgrade**
  You can upgrade to Oracle Identity and Access Management 12c (12.2.1.4.0) from a supported 12c release.

- **About the Oracle Identity and Access Management Upgrade Scenarios**
  The steps to upgrade Oracle Identity and Access Management to 12c (12.2.1.4.0) depend on the existing 12c (12.2.1.3.0) production topology.

- **About the New Features for Oracle Identity and Access Management 12c (12.2.1.4.0)**
  Several changes have been made to Oracle Identity and Access Management between 12c (12.2.1.3.0) and 12c (12.2.1.4.0).

- **About Upgrade Restrictions**
  If you are using two or more Oracle Fusion Middleware products of the same or different versions in a single, supported, Oracle Fusion Middleware configuration,
you must consider the interoperability and compatibility factors before planning the upgrade.

- **How to Use This Guide**
  This guide covers various upgrade scenarios.

### About the Starting Points for a Oracle Identity and Access Management Upgrade

You can upgrade to Oracle Identity and Access Management 12c (12.2.1.4.0) from a supported 12c release.

Supported starting point for is upgrading Oracle Identity and Access Management to 12c (12.2.1.4.0) is Oracle Identity and Access Management 12c (12.2.1.3.0).

If you are not using the 12c (12.2.1.3.0) version of Oracle Identity and Access Management, you must upgrade to 12c (12.2.1.3.0) before you move to 12c (12.2.1.4.0).

For information about upgrading Oracle Identity and Access Management to 12c (12.2.1.3.0), see *Introduction to Upgrading Oracle Identity and Access Management to 12c (12.2.1.3.0)* in the *Upgrade Guide for Oracle Identity and Access Management* for 12c (12.2.1.3.0).

The upgrade procedures in this guide explain how to upgrade an existing Oracle Identity and Access Management 12c domain to Oracle Identity and Access Management 12c (12.2.1.4.0). If your domain contains other components, you will have to upgrade those components as well. Links to supporting documentation are provided wherever necessary.

### About the Oracle Identity and Access Management Upgrade Scenarios

The steps to upgrade Oracle Identity and Access Management to 12c (12.2.1.4.0) depend on the existing 12c (12.2.1.3.0) production topology.

As a result, it is difficult to provide exact upgrade instructions for every possible Oracle Identity and Access Management installation. Therefore, this upgrade documentation provides instructions for upgrading several typical Oracle Identity and Access Management topologies.

Your actual topology may vary, but the topologies described here provide an example that can be used as a guide to upgrade other similar Oracle Identity and Access Management topologies.

**Note:**

For additional information about the upgrade process and planning resources to ensure your upgrade is successful, see Preparing to Upgrade in *Planning an Upgrade of Oracle Fusion Middleware.*
You can upgrade the following topologies or deployments using the procedure described in this guide:

- Oracle Identity and Access Management single node environments
- Oracle Identity and Access Management highly available (multinode) environments
- Oracle Access Management Multi-data center setup

**Note:**

If you are using Oracle Access Management Mobile and Social, do NOT upgrade to 12c (12.2.1.4.0). Contact Oracle support for more details on the upgrade path for Mobile and Social.

### About the New Features for Oracle Identity and Access Management 12c (12.2.1.4.0)

Several changes have been made to Oracle Identity and Access Management between 12c (12.2.1.3.0) and 12c (12.2.1.4.0).

To understand what's new in general in 12c (12.2.1.4.0), see New and Changed Features in *Understanding Oracle Fusion Middleware*.

If your environment includes Oracle WebLogic Server with Oracle ADF, see Key Differences Between Application Developer 12c (12.2.1.3.0) and Infrastructure 12c (12.2.1.4.0).

For information about Oracle Access Management 12c (12.2.1.4.0), and it's features, refer to the following topics in the *Administrator's Guide for Oracle Access Management*:

- Features of Access Manager 12.2.1.4.0
- Features Not Supported in Access Manager 12.2.1.4.0
- Understanding Oracle Access Management Services
- Understanding Oracle Access Management Access Manager

For more information about Oracle Identity Governance 12c (12.2.1.4.0), refer to the following topics in the *Administering Oracle Identity Governance*:

- New and Changed Features for 12c (12.2.1.4.0)
- What is Oracle Identity Governance?
- What are the Different Modes of Oracle Identity Governance?

### About Upgrade Restrictions

If you are using two or more Oracle Fusion Middleware products of the same or different versions in a single, supported, Oracle Fusion Middleware configuration, you
must consider the interoperability and compatibility factors before planning the upgrade.

**Interoperability**

In the context of Oracle Fusion Middleware products, Interoperability is defined as the ability of two Oracle Fusion Middleware products or components of the same version (or release) to work together (interoperate) in a supported Oracle Fusion Middleware configuration. Specifically, interoperability applies when the first 4 digits of the release or version number are the same. For example, Oracle Fusion Middleware 12c (12.2.1.4.0) components are generally interoperable with other 12c (12.2.1.4.0) components.

**Compatibility**

In the context of Oracle Fusion Middleware products, Compatibility is defined as the ability of two Oracle Fusion Middleware components of different versions (or releases) to interoperate.

For a list of products and features available in Oracle Fusion Middleware Release 12.2.1.4.0, see Products and Features Available in Oracle Fusion Middleware 12c (12.2.1.4.0) in *Understanding Interoperability and Compatibility*.

---

**How to Use This Guide**

This guide covers various upgrade scenarios.

Depending on your existing 12c (12.2.1.3.0) deployment, refer to the respective topics for upgrading Oracle Identity and Access Management to 12c (12.2.1.4.0):

- **Single Node Environments**
  - For upgrading single node Oracle Access Management (OAM) setup, see [Upgrading Oracle Access Management Single Node Environments](#).
  - For upgrading single node Oracle Identity Manager (OIM) setup, see [Upgrading Oracle Identity Manager Single Node Environments](#).

- **Multi-node or Highly Available Environments**
  - For upgrading multi-node Oracle Access Management setup, see [Upgrading Oracle Access Management Highly Available Environments](#).
  - For upgrading multi-node Oracle Identity Manager setup, see [Upgrading Oracle Identity Manager Highly Available Environments](#).
  - For upgrading Oracle Access Management multi-data center setup, see [Upgrading Oracle Access Management Multi-Data Center Environments](#).

---

**Note:**

Before you begin the upgrade, ensure that you review the [Pre-Upgrade Requirements](#) and perform necessary pre-upgrade tasks.
Pre-Upgrade Requirements

Before you begin to upgrade Oracle Identity and Access Management 12c (12.2.1.4.0), you must perform pre-upgrade tasks such as backing up, cloning your current environment, and verifying that your system meets certified requirements.

- **Oracle Fusion Middleware Pre-Upgrade Checklist**
  Perform the tasks in this checklist before you begin any upgrade to ensure you have a successful upgrade and limited downtime.

- **Creating a Complete Backup**
  Before you start an upgrade, back up all system-critical files, including the databases that host your Oracle Fusion Middleware schemas.

- **Cloning Your Production Environment for Testing**
  Create a copy of your actual production environment, upgrade the cloned environment, verify that the upgraded components work as expected, and then (and only then) upgrade your production environment.

- **Verifying Certification and System Requirements**
  Review the certification matrix and system requirements documents to verify that your environment meets the necessary requirements for installation.

- **Updating Policy Files when Using Enhanced Encryption (AES 256)**
  If you plan to use enhanced encryption, such as Advanced Encryption Standard (AES) 256, in your upgraded environment, Oracle recommends that you apply the latest required policy files to the JDK before you upgrade.

- **Purging Unused Data**
  Purging unused data and maintaining a purging methodology before an upgrade can optimize the upgrade process.

- **Creating a Non-SYSDBA User to Run the Upgrade Assistant**
  Oracle recommends that you create a non-SYSDBA user called `FMW` to run the Upgrade Assistant. This user has the privileges required to modify schemas, but does not have full administrator privileges.

- **Identifying Existing Schemas Available for Upgrade**
  This optional task enables you to review the list of available schemas before you begin the upgrade by querying the schema version registry. The registry contains schema information such as version number, component name and ID, date of creation and modification, and custom prefix.

- **Updating Database Parameters for Oracle Identity Manager**
  You need to verify and update a few database parameters before upgrading the Oracle Identity Manager to 12c (12.2.1.4.0).

### Oracle Fusion Middleware Pre-Upgrade Checklist

Perform the tasks in this checklist before you begin any upgrade to ensure you have a successful upgrade and limited downtime.
Upgrades are performed while the servers are down. This checklist identifies important and often time-consuming pre-upgrade tasks that you can perform before the upgrade to limit your downtime. The more preparation you can do before you begin the upgrade process, the less time you will spend offline.

**Note:**

The pre-upgrade procedures you perform will depend on the configuration of your existing system, the components you are upgrading, and the environment you want to create at the end of the upgrade and configuration process. Complete only those tasks that apply to your configurations or use cases.

Table 2-1  Tasks to Perform Before You Upgrade to Oracle Fusion Middleware 12c (12.2.1.4.0)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required</strong></td>
<td>Back up all system-critical files and database(s) that contain any schemas that are to be upgraded. If the upgrade fails, you must restore your pre-upgrade environment and begin the upgrade again.</td>
</tr>
<tr>
<td>Create a complete backup of your existing</td>
<td>See <a href="#">Creating a Complete Backup</a>.</td>
</tr>
<tr>
<td>environment.</td>
<td>• Make sure that your backup includes the schema version registry table. See <a href="#">Backing Up the Schema Version Registry Table</a>.</td>
</tr>
<tr>
<td></td>
<td>• If you modified any of the startup scripts in your existing domain, you will need to copy them to temporary directory location (outside of the existing domain) during the upgrade and redeploy them after the upgrade. See <a href="#">Maintaining Customized Domain and Environment Settings</a>.</td>
</tr>
<tr>
<td><strong>Optional</strong></td>
<td>In addition to creating a complete backup of your system files, Oracle strongly recommends that you clone your production environment. This environment can be used to test the upgrade.</td>
</tr>
<tr>
<td>Clone your production environment to use</td>
<td>See <a href="#">Cloning Your Production Environment for Testing</a>.</td>
</tr>
<tr>
<td>as an upgrade testing platform.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 2-1 (Cont.) Tasks to Perform Before You Upgrade to Oracle Fusion Middleware 12c (12.2.1.4.0)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required</strong></td>
<td>Verify that you are installing and upgrading your product on a supported hardware and software configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution:</strong> Do not attempt an upgrade if you are unable to use the latest supported operating system. As with all supported configurations, failure to comply with these requirements may cause your upgrade to fail.</td>
</tr>
<tr>
<td></td>
<td>Oracle recommends that you verify this information right before you start the upgrade as the certification requirements are frequently updated.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Make sure that you have applied the latest patches to your components before you upgrade.</td>
</tr>
<tr>
<td></td>
<td>See Verifying Certification and System Requirements.</td>
</tr>
<tr>
<td><strong>Required for 32–bit Operating Systems Only</strong></td>
<td>Migrate to a 64-bit operating system before you can upgrade.</td>
</tr>
<tr>
<td></td>
<td>This is required only if you are currently running an unsupported 32–bit operating system.</td>
</tr>
<tr>
<td></td>
<td>See Migrating from a 32-Bit to a 64-Bit Operating System.</td>
</tr>
<tr>
<td><strong>Optional</strong></td>
<td>Update security policy files if you are using enhanced encryption (AES 256).</td>
</tr>
<tr>
<td></td>
<td>Some of the security algorithms used in Fusion Middleware 12c (12.2.1.4.0) require additional policy files for the JDK.</td>
</tr>
<tr>
<td></td>
<td>If you plan to use enhanced encryption, such as AES 256, Oracle recommends that you apply the latest required policy files to the JDK before you upgrade.</td>
</tr>
<tr>
<td></td>
<td>See Updating Policy Files when Using Enhanced Encryption (AES 256).</td>
</tr>
<tr>
<td><strong>Optional</strong></td>
<td>Purge any outdated or unused data before you upgrade.</td>
</tr>
<tr>
<td></td>
<td>To optimize performance, Oracle strongly recommends that you purge data and objects that will not be used in the upgraded environment.</td>
</tr>
<tr>
<td></td>
<td>See Purging Unused Data.</td>
</tr>
<tr>
<td><strong>Optional</strong></td>
<td>Create a Non-SYSDBA user to run the Upgrade Assistant.</td>
</tr>
<tr>
<td></td>
<td>Oracle recommends that you create the FMW user to run Upgrade Assistant. User FMW can run the Upgrade Assistant without system administration privileges.</td>
</tr>
<tr>
<td></td>
<td>See Creating a Non-SYSDBA User to Run the Upgrade Assistant.</td>
</tr>
</tbody>
</table>

### Creating a Complete Backup

Before you start an upgrade, back up all system-critical files, including the databases that host your Oracle Fusion Middleware schemas.

The backup must include the `SYSTEM.SCHEMA_VERSION_REGISTRY$` table so that you can restore the contents back to its pre-upgrade state if the upgrade fails.
The Upgrade Assistant Prerequisites screen prompts you to acknowledge that backups have been performed before you proceed with the actual upgrade. However, note that the Upgrade Assistant does not verify that a backup has been created.

See:
- Backing Up Your Environment in *Administering Oracle Fusion Middleware*
- Upgrading and Preparing Your Oracle Databases for 12c (12.2.1.4.0) in *Planning an Upgrade of Oracle Fusion Middleware*
- **Backing Up the Schema Version Registry Table**
  Your system backup must include the `SYSTEM.SCHEMA_VERSION_REGISTRY$` table or the `FMWREGISTRY.SCHEMA_VERSION_REGISTRY$` table.
- **Maintaining Customized Domain and Environment Settings**
  If you have modified any domain-generated, server startup scripts, or configuration files in your pre-upgrade environment, it is important to note that these changes are overwritten during the installation, domain upgrade, and reconfiguration operations. Save your customized files to a shared library location so that you can continue to use them after the upgrade.

**Backing Up the Schema Version Registry Table**

Your system backup must include the `SYSTEM.SCHEMA_VERSION_REGISTRY$` table or the `FMWREGISTRY.SCHEMA_VERSION_REGISTRY$` table.

Each Fusion Middleware schema has a row in the `SYSTEM.SCHEMA_VERSION_REGISTRY$` table. If you run the Upgrade Assistant to update an existing schema and it does not succeed, you must restore the original schema before you can try again. Before you run the Upgrade Assistant, make sure you back up your existing database schemas and the schema version registry.

**Note:**

Before you upgrade a schema using the Upgrade Assistant, you must perform a complete database backup. During the upgrade, you are required to acknowledge that backups have been performed.

**Maintaining Customized Domain and Environment Settings**

If you have modified any domain-generated, server startup scripts, or configuration files in your pre-upgrade environment, it is important to note that these changes are overwritten during the installation, domain upgrade, and reconfiguration operations. Save your customized files to a shared library location so that you can continue to use them after the upgrade.

Every domain installation includes dynamically-generated domain and server startup scripts, such as `setDomainEnv`. These files are replaced by newer versions during the installation and upgrade process. To maintain your custom domain-level environment settings, Oracle recommends that you create a separate file to store the custom domain information before you upgrade, instead of modifying the scripts directly.

For example, if you want to customize server startup parameters that apply to all servers in a domain, you can create a file called `setUserOverrides.cmd` (Windows) or
setUserOverrides.sh (UNIX) and configure it to add custom libraries to the WebLogic Server classpath, specify additional command-line options for running the servers, or specify additional environment variables. When using the `pack` and `unpack` commands, any custom settings that you add to this file are preserved during the domain upgrade operation and are carried over to the remote servers.

The following example illustrates startup customizations in a `setUserOverrides` file:

```bash
# add custom libraries to the WebLogic Server system classpath
if [ "${POST_CLASSPATH}" != "" ] ; then
    POST_CLASSPATH="${POST_CLASSPATH}${CLASSPATHSEP}${HOME}/foo/fooBar.jar"
    export POST_CLASSPATH
else
    POST_CLASSPATH="${HOME}/foo/fooBar.jar"
    export POST_CLASSPATH
fi

# specify additional java command-line options for servers
JAVA_OPTIONS="${JAVA_OPTIONS} -Dcustom.property.key=custom.value"
```

If the `setUserOverrides` file exists during a server startup, the file is included in the startup sequence and any overrides contained within this file take effect. You must store the `setUserOverrides` file in the `EXISTING_DOMAIN_HOME/bin` directory.

**Note:**

If you are unable to create the `setUserOverrides` script before an upgrade, you need to reapply your settings as described in Re-apply Customizations to Startup Scripts in *Upgrading Oracle WebLogic Server*.

---

**Cloning Your Production Environment for Testing**

Create a copy of your actual production environment, upgrade the cloned environment, verify that the upgraded components work as expected, and then (and only then) upgrade your production environment.

Cloning your production environment for testing is recommended, but not required.

Upgrades cannot be reversed. In most cases, if an error occurs, you must stop the upgrade and restore the entire environment from backup and begin the upgrade process from the beginning. Identifying potential upgrade issues in a development environment can eliminate unnecessary downtime.
Note:

It is beyond the scope of this document to describe the cloning procedures for all components and operating systems. Cloning procedures are component and operating system-specific. At a high level, you install the pre-upgrade version of your component domain on a test machine, create the required schemas using the Repository Creation Utility (RCU), and perform the upgrade.

Additional benefits of running an upgrade in a cloned production environment include the following:

• Uncover and correct any upgrade issues.
• Practice completing an end-to-end upgrade.
• Understand the upgrade performance and how purge scripts can help.
• Understand the time required to complete the upgrade.
• Understand the database resource usage (such as temporary tablespace; PGA, and so on).

Note:

You can run the pre-upgrade Readiness Check on the cloned production environment to help identify potential upgrade issues with your data, but you must perform a complete test upgrade on a cloned environment to ensure a successful upgrade.

Verifying Certification and System Requirements

Review the certification matrix and system requirements documents to verify that your environment meets the necessary requirements for installation.

Note:

When checking the certification, system requirements, and interoperability information, be sure to check specifically for any 32-bit or 64-bit system requirements. It is important for you to download software specifically designed for the 32-bit or 64-bit environment, explicitly.

WARNING:

Make sure that your current environment has been patched to the latest patch set before you begin the upgrade. Certifications are based on fully patched environments, unless stated otherwise.
Verify Your Environment Meets Certification Requirements
Oracle has tested and verified the performance of your product on all certified systems and environments. Make sure that you are installing your product on a supported hardware or software configuration.

Whenever new certifications occur, they are added to the appropriate certification document right away. New certifications can occur at any time, and for this reason the certification documents are kept outside of the documentation libraries and are available on Oracle Technology Network. See the Certification Matrix for 12c (12.2.1.4.0).

Verify System Requirements and Specifications
It is important to verify that the system requirements such as disk space, available memory, specific platform packages and patches, and other operating system-specific items are met.

Use the Oracle Fusion Middleware System Requirements and Specifications document to verify that the requirements of the certification are met. For example, if the Certification Matrix for 12c (12.2.1.4.0) indicates that your product is certified for installation on 64-Bit Oracle Linux 7, the System Requirements and Specifications document should be used to verify that your Oracle Linux 7 system has met the required minimum specifications such as disk space, available memory, specific platform packages and patches, and other operating system-specific items. This document is updated as needed and resides outside of the documentation libraries on the Oracle Technology Network (OTN).

Note:
When you install the Oracle Fusion Middleware Release 12c software in preparation for upgrade, you should use the same user account that you used to install and configure the existing, pre-upgrade Oracle Fusion Middleware software. On UNIX operating systems, this ensures that the proper owner and group is applied to new Oracle Fusion Middleware 12c files and directories.
If you are running a 32–bit environment, you will need to perform an additional set of steps:

- **Migrating from a 32-Bit to a 64-Bit Operating System**
  If you have a 32–bit operating system, then you must migrate your 32-bit environment to a 64-bit software environment before you upgrade.

### Migrating from a 32-Bit to a 64-Bit Operating System

If you have a 32–bit operating system, then you must migrate your 32-bit environment to a 64-bit software environment before you upgrade.

Make sure to validate the migration to ensure all your Oracle Fusion Middleware 12c (12.2.1.3.0) software is working properly on the 64-bit machine, and only then perform the upgrade to Oracle Fusion Middleware 12c (12.2.1.4.0).

In these tasks, *host* refers to the 32-bit source machine and *target* refers to the new 64-bit target machine.

---

**Note:**

These steps assume that your database is located on a separate host and will not be moved.

---

Upgrading an operating system typically involves the following:

---

**Caution:**

These steps are provided as an example of the operating system upgrade process and may or may not include all of the procedures you must perform to update your specific operating system. Consult your operating system's upgrade documentation for more information.

- **Procure the Hardware That Supports the Upgrade's 64-bit Software Requirement**
  Make sure that you have supported target hardware in place before you begin the upgrade process.

- **Stop All Processes**
  Before upgrading, you must stop all processes, including Managed Servers, the Administration Server, and Node Manager, if they are started on the host.

- **Back Up All Files from the 32-bit Host Machine**
  Make sure that you have created a complete backup of your entire 12c (12.2.1.3.0) deployment before you begin the upgrade process. These files can be used if there is an issue during the migration and you have to restart the process.

- **Set Up the Target 64-bit Machine with the 12c (12.2.1.3.0) Host Name and IP Address**
  The host name and IP address of the target machine must be made identical to the host. This requires you to change the IP address and name of the source machine or decommission the source machine to avoid conflicts in the network.
• **Restore the 12c (12.2.1.3.0) Backup from 32-bit Host to 64-bit Host**
  Restore the files you backed from the 32-bit host using the same directory structure that was used in 12c (12.2.1.3.0). The directory structure on the target machine must be identical to the structure of the host machine.

• **Install the 12c (12.2.1.4.0) Product Distributions on the Target Machine**
  Oracle recommends an Out-of-Place approach for upgrade. Therefore, you must install the 12c (12.2.1.4.0) product distributions in a new Oracle home on the target machine.

• **Upgrade the Target 64-bit Environment Using the Standard Upgrade Procedure**
  After installing the product on the target machine, you must upgrade each product component individually using an Upgrade Utility specified in the component-specific upgrade guide and complete any post-upgrade tasks.

Procure the Hardware That Supports the Upgrade's 64-bit Software Requirement

Make sure that you have supported target hardware in place before you begin the upgrade process.

Stop All Processes

Before upgrading, you must stop all processes, including Managed Servers, the Administration Server, and Node Manager, if they are started on the host.

> **Note:**

Ensure that the Database is up and running, during the upgrade.

Stop the Managed Servers

To stop a WebLogic Server Managed Server, use the `stopManagedWebLogic` script:

- (UNIX) `EXISTING_DOMAIN_HOME/bin/stopManagedWebLogic.sh`
multiple_server_name admin_url
- (Windows) `EXISTING_DOMAIN_HOME\bin\stopManagedWebLogic.cmd`
multiple_server_name admin_url

When prompted, enter your user name and password.

Stop the Administration Server

When you stop the Administration Server, you also stop the processes running in the Administration Server, including the WebLogic Server Administration Console and Fusion Middleware Control.

To stop the Administration Server, use the `stopWebLogic` script:

- (UNIX) `EXISTING_DOMAIN_HOME/bin/stopWebLogic.sh`
- (Windows) `EXISTING_DOMAIN_HOME\bin\stopWebLogic.cmd`

When prompted, enter your user name, password, and the URL of the Administration Server.

Stop Node Manager
To stop Node Manager, close the command shell in which it is running.

Alternatively, after having set the `nodemanager.properties` attribute `QuitEnabled` to `true` (the default is `false`), you can use WLST to connect to Node Manager and shut it down. See `stopNodeManager` in *WLST Command Reference for WebLogic Server*.

**Back Up All Files from the 32-bit Host Machine**

Make sure that you have created a complete backup of your entire 12c (12.2.1.3.0) deployment before you begin the upgrade process. These files can be used if there is an issue during the migration and you have to restart the process.

---

### Note:

If the upgrade from 32-bit to 64-bit takes place on the same machine, there is a risk of corrupting the source environment if the upgrade fails.

---

See *Backing Up Your Environment* in *Oracle Fusion Middleware Administrator's Guide*.

During the upgrade you must have access to the contents of the following:

- `12c_DOMAIN_HOME`
- `12c/nodemanager` directory located in `12c_ORACLE_HOME/wlserver/common`/  

Some of the backup and recovery procedures described in *Backing Up Your Environment* in *Oracle Fusion Middleware Administrator's Guide* are product-specific. Do not proceed with the upgrade until you have a complete backup.

**Set Up the Target 64-bit Machine with the 12c (12.2.1.3.0) Host Name and IP Address**

The host name and IP address of the target machine must be made identical to the host. This requires you to change the IP address and name of the source machine or decommission the source machine to avoid conflicts in the network.

The process of changing an IP address and host name vary by operating system. Consult your operating system's administration documentation for more information.

**Restore the 12c (12.2.1.3.0) Backup from 32-bit Host to 64-bit Host**

Restore the files you backed from the 32-bit host using the same directory structure that was used in 12c (12.2.1.3.0). The directory structure on the target machine must be identical to the structure of the host machine.

See *Recovering Your Environment* in *Oracle Fusion Middleware Administrator's Guide*. 
Install the 12c (12.2.1.4.0) Product Distributions on the Target Machine

Oracle recommends an Out-of-Place approach for upgrade. Therefore, you must install the 12c (12.2.1.4.0) product distributions in a new Oracle home on the target machine.

Refer to the component-specific installation guides for the component(s) you are installing.

Upgrade the Target 64-bit Environment Using the Standard Upgrade Procedure

After installing the product on the target machine, you must upgrade each product component individually using an Upgrade Utility specified in the component-specific upgrade guide and complete any post-upgrade tasks.

If you are upgrading additional components, see the component-specific upgrade guide.

Note:
The Node Manager upgrade procedure requires access to the original Node Manager files. Use the 12c (12.2.1.3.0) Node Manger files that you backed up from the 32-bit source machine as part of Back Up All Files from the 32-bit Host Machine.

Verify That the Database Hosting Oracle Fusion Middleware is Supported

You must have a supported Oracle database configured with the required schemas before you run Oracle Fusion Middleware 12c (12.2.1.4.0).

Review the Fusion Middleware database requirements before starting the upgrade to ensure that the database hosting Oracle Fusion Middleware is supported and has sufficient space to perform an upgrade. See the Certification Matrix for 12c (12.2.1.4.0).

Note:
If your database version is no longer supported, you must upgrade to a supported version before starting an upgrade. See Upgrading and Preparing Your Oracle Databases for 12c (12.2.1.4.0) in Planning an Upgrade of Oracle Fusion Middleware.

Verify That the JDK Is Certified for This Release of Oracle Fusion Middleware

At the time this document was published, the certified JDK for 12c (12.2.1.4.0) was 1.8.0_211.
Refer to the Oracle Fusion Middleware Supported System Configurations information on the Oracle Technology Network (OTN) to verify that the JDK you are using is supported.

If your JDK is not supported, or you do not have a JDK installed, you must download the required Java SE JDK, from the following website:


Make sure that the JDK is installed outside of the Oracle home. The Oracle Universal Installer validates that the designated Oracle home directory is empty, and the install does not progress until an empty directory is specified. If you install JDK under Oracle home, you may experience issues in future operations. Therefore, Oracle recommends that you use install the JDK in the following directory: `/home/oracle/products/jdk`

For more information on the difference between generic and platform-specific installers, see Understanding the Difference Between Generic and Platform-Specific Distributions in the Oracle Fusion Middleware Download, Installation, and Configuration Readme Files.

### Updating Policy Files when Using Enhanced Encryption (AES 256)

If you plan to use enhanced encryption, such as Advanced Encryption Standard (AES) 256, in your upgraded environment, Oracle recommends that you apply the latest required policy files to the JDK before you upgrade.

The Java platform defines a set of APIs spanning major security areas, including cryptography, public key infrastructure, authentication, secure communication, and access control. These APIs allow developers to easily integrate security mechanisms into their application code.

Some of the security algorithms used in Fusion Middleware 12c (12.2.1.4.0) require additional policy files for the JDK. See Java Cryptography Architecture Oracle Providers Documentation.

> **Note:**
>
> If you attempt to use enhanced encryption without applying these policy files to the JDK before you begin the upgrade, the upgrade can fail and you must restore the entire pre-upgrade environment and start the upgrade from the beginning.

### Purging Unused Data

Purging unused data and maintaining a purging methodology before an upgrade can optimize the upgrade process.

Some components have automated purge scripts. If you are using purge scripts, wait until the purge is complete before starting the upgrade process. The upgrade may fail if the purge scripts are running while using the Upgrade Assistant to upgrade your schemas.
Creating a Non-SYSDBA User to Run the Upgrade Assistant

Oracle recommends that you create a non-SYSDBA user called **FMW** to run the Upgrade Assistant. This user has the privileges required to modify schemas, but does not have full administrator privileges.

SYSDBA is an administrative privilege that is required to perform high-level administrative operations such as creating, starting up, shutting down, backing up, or recovering the database. The SYSDBA system privilege is for a fully empowered database administrator. When you connect with the SYSDBA privilege, you connect with a default schema and not with the schema that is generally associated with your user name. For SYSDBA, this schema is SYS. Access to a default schema can be a very powerful privilege. For example, when you connect as user SYS, you have unlimited privileges on data dictionary tables. Therefore, Oracle recommends that you create a non-SYSDBA user to upgrade the schemas. The privileges listed below must be granted to user FMW before starting the Upgrade Assistant.

**Notes:**

The non-SYSDBA user FMW is created solely for the purpose of running the Upgrade Assistant. After this step is complete, drop the FMW user. Note that privileges required for running the Upgrade Assistant may change from release to release. By default, the v$xatrans$ table does not exist. You must run the XAVIEW.SQL script to create this table before creating the user. Moreover, the grant select privilege on the v$xatrans$ table is required only by Oracle Identity Governance. If you do not require Oracle Identity Governance for configuration, or if you do not have the v$xatrans$ table, then remove the following line from the script:

```
grant select on v$xatrans$ to FMW with grant option;
```

In the example below, password is the password that you set for the FMW user. When granting privileges, make sure that you specify your actual password.

```sql
create user FMW identified by password;
grant dba to FMW;
grant execute on DBMS_LOB to FMW with grant option;
grant execute on DBMS_OUTPUT to FMW with grant option;
grant execute on DBMS_STATS to FMW with grant option;
grant execute on sys.dbms_aqadm to FMW with grant option;
grant execute on sys.dbms_aqin to FMW with grant option;
grant execute on sys.dbms_aqjms to FMW with grant option;
grant execute on sys.dbms_aq to FMW with grant option;
grant execute on utl_file to FMW with grant option;
grant execute on dbms_lock to FMW with grant option;
grant select on sys.V_$INSTANCE to FMW with grant option;
```
grant select on sys.GV_$INSTANCE to FMW with grant option;
grant select on sys.V_$SESSION to FMW with grant option;
grant select on sys.GV_$SESSION to FMW with grant option;
grant select on dba_scheduler_jobs to FMW with grant option;
grant select on dba_scheduler_job_run_details to FMW with grant option;
grant select on dba_scheduler_running_jobs to FMW with grant option;
grant select on dba_aq_agents to FMW with grant option;
grant execute on sys.DBMS_SHARED_POOL to FMW with grant option;
grant select on dba_2pc_pending to FMW with grant option;
grant select on dba_pending_transactions to FMW with grant option;
grant execute on DBMS_FLASHBACK to FMW with grant option;
grant execute on dbms_crypto to FMW with grant option;
grant execute on DBMS_REFUTIL to FMW with grant option;
grant execute on dbms_job to FMW with grant option;
grant select on pending_trans$ to FMW with grant option;
grant select on dba_scheduler_job_classes to fmw with grant option;
grant select on SYS.DBA_DATA_FILES to FMW with grant option;
grant select on SYS.V_$ASM_DISKGROUP to FMW with grant option;
grant select on v$session$ to FMW with grant option;
grant execute on sys.dbms_system to FMW with grant option;
grant execute on DBMS_SCHEDULER to FMW with grant option;
grant select on dba_data_files to FMW with grant option;
grant execute on UTL_RAW to FMW with grant option;
grant execute on DBMS_XMLDOM to FMW with grant option;
grant execute on DBMS_APPLICATION_INFO to FMW with grant option;
grant execute on DBMS_UTIL to FMW with grant option;
grant execute on DBMS_SESSION to FMW with grant option;
grant execute on DBMS_METADATA to FMW with grant option;
grant execute on DBMS_XMLGEN to FMW with grant option;
grant execute on DBMS_DATAPUMP to FMW with grant option;
grant execute on DBMS_MVIEW to FMW with grant option;
grant select on ALL_ENCRYPTED_COLUMNS to FMW with grant option;
grant select on dba_queue_subscribers to FMW with grant option;
grant execute on SYS.DBMS_ASSERT to FMW with grant option;
grant select on dba_subscr_registrations to FMW with grant option;
grant manage scheduler to FMW;

If you are upgrading Oracle Identity Manager (OIM) schema, ensure that the FMW user has the following additional privileges:

grant execute on SYS.DBMS_FLASHBACK to fmw with grant option;
grant execute on sys.DBMS_SHARED_POOL to fmw with grant option;
grant execute on SYS.DBMS_XMLGEN to FMW with grant option;
grant execute on SYS.DBMS_DB_VERSION to FMW with grant option;
grant execute on SYS.DBMS_SCHEDULER to FMW with grant option;
grant execute on SYS.DBMS_SQL to FMW with grant option;
grant execute on SYS.DBMS_UTIL to FMW with grant option;
grant ctxapp to FMW with admin option;
grant execute on SYS.DBMS_FLASHBACK TO FMW with grant option;
grant create MATERIALIZED VIEW to FMW with admin option;
grant all on SCHEMA_VERSION_REGISTRY TO FMW with grant option;
grant create SYNONYM to FMW with admin option;
grant execute on CTXSYS.CTX_ADM to FMW with grant option;
grant execute on CTXSYS.CTX_CLS TO FMW with grant option;

Chapter 2
Creating a Non-SYSDBA User to Run the Upgrade Assistant

2-14
grant execute on CTXSYS.CTX_DDL TO FMW with grant option;
grant execute on CTXSYS.CTX_DOC TO FMW with grant option;
grant execute on CTXSYS.CTX_OUTPUT TO FMW with grant option;
grant execute on CTXSYS.CTX_QUERY TO FMW with grant option;
grant execute on CTXSYS.CTX_REPORT TO FMW with grant option;
grant execute on CTXSYS.CTX_THES TO FMW with grant option;
grant execute on CTXSYS.CTX_ULEXER TO FMW with grant option;
grant create JOB to FMW with admin option;

Identifying Existing Schemas Available for Upgrade

This optional task enables you to review the list of available schemas before you begin the upgrade by querying the schema version registry. The registry contains schema information such as version number, component name and ID, date of creation and modification, and custom prefix.

You can let the Upgrade Assistant upgrade all of the schemas in the domain, or you can select individual schemas to upgrade. To help decide, follow these steps to view a list of all the schemas that are available for an upgrade:

1. If you are using an Oracle database, connect to the database by using an account that has Oracle DBA privileges, and run the following from SQL*Plus:

   ```sql
   SET LINE 120
   COLUMN MRC_NAME FORMAT A14
   COLUMN COMP_ID FORMAT A20
   COLUMN VERSION FORMAT A12
   COLUMN STATUS FORMAT A9
   COLUMN UPGRADED FORMAT A8
   SELECT MRC_NAME, COMP_ID, OWNER, VERSION, STATUS, UPGRADED FROM
   SCHEMA_VERSION_REGISTRY ORDER BY MRC_NAME, COMP_ID;
   ```

2. Examine the report that is generated.

   If an upgrade is not needed for a schema, the schema_version_registry table retains the schema at its pre-upgrade version.

3. Note the schema prefix name that was used for your existing schemas. You will use the same prefix when you create new 12c (12.2.1.4.0) schemas.
**Notes:**

- If your existing schemas are not from a supported version, then you must upgrade them to a supported version before using the 12c (12.2.1.4.0) upgrade procedures. Refer to your pre-upgrade version documentation for more information.
- Some components, such as Oracle Enterprise Data Quality, Oracle GoldenGate Monitor, and Oracle GoldenGate Veridata, support an upgrade from versions other than the standard Oracle Fusion Middleware supported versions.
- If you used an OID-based policy store in the earlier versions, make sure to create a new OPSS schema before you perform the upgrade. After the upgrade, the OPSS schema remains an LDAP-based store.
- You can only upgrade schemas for products that are available for upgrade in Oracle Fusion Middleware release 12c (12.2.1.4.0). Do not attempt to upgrade a domain that includes components that are not yet available for upgrade to 12c (12.2.1.4.0).

---

**Updating Database Parameters for Oracle Identity Manager**

You need to verify and update a few database parameters before upgrading the Oracle Identity Manager to 12c (12.2.1.4.0).

**Note:**

This topic is applicable to only Oracle Identity Manager.

Complete the following steps:

1. Login as a SYS DB user.
2. To verify the value for the database parameter `max_string_size`, run the following command:

   ```sql
   SQL> SELECT value FROM v$parameter WHERE name='max_string_size';
   ```

3. If the value returned is:
   - **STANDARD**: Skip the rest of the steps in this procedure and go to the next procedure to continue with the upgrade.
   - **EXTENDED**: Continue with step 4.
4. Login as an OIM database user and then run the following command to find columns with size more than 4000 characters:

   ```sql
   SQL> SELECT table_name, column_name, data_length FROM user_tab_columns WHERE data_length>4000;
   ```
5. If any rows are listed, either trim the corresponding column data to 4000 characters or remove the rows.

Note:
If required, take backup of the listed rows in a new table.

6. Reset all the columns sizes found in step 4 to 4000 characters.
As an OIM database user, run the following command:

    SQL> ALTER TABLE <table_name> MODIFY <column_name> VARCHAR2(4000);

7. Drop any index, if exists, on the columns whose length was modified to more than 4000 characters.

8. As an OIM database user, run the following command to verify that there no more columns with size more than 4000:

    SQL> SELECT table_name, column_name, data_length FROM user_tab_columns WHERE data_length>4000;

9. If required, gather table and index stats for the identified columns.
Part I

Upgrading Oracle Identity and Access Management Single Node Environments

You can upgrade the Oracle Identity and Access Management 12c (12.2.1.4.0) single node environments using the procedure described in the following sections.

Topics

• **Upgrading Oracle Access Management Single Node Environments**
  You can upgrade Oracle Access Management from Release 12c (12.2.1.3.0) to Oracle Access Management 12c (12.2.1.4.0).

• **Upgrading Oracle Identity Manager Single Node Environments**
  You can upgrade Oracle Identity Manager from Release 12c (12.2.1.3.0) to Oracle Identity Governance 12c (12.2.1.4.0).
You can upgrade Oracle Access Management from Release 12c (12.2.1.3.0) to Oracle Access Management 12c (12.2.1.4.0).

**Note:**
If you are using an earlier version of Oracle Access Management, you must upgrade to Oracle Access Management 12c (12.2.1.3.0) first, and then to 12c (12.2.1.4.0).

Complete the steps in the following topics to perform the upgrade:

- **About the Oracle Access Management Single Node Upgrade Process**
  Review the roadmap for an overview of the upgrade process for Oracle Access Management single node deployments.

- **Completing the Pre-Upgrade Tasks for Oracle Access Management**
  Complete the pre-upgrade tasks described in this section before you upgrade Oracle Access Management.

- **Stopping Servers and Processes**
  Before you upgrade the schemas and configurations, you must shut down all of the pre-upgrade processes and servers, including the Administration Server and any managed servers on OIMHOST.

- **Uninstalling the Software**
  Follow the instructions in this section to start the Uninstall Wizard and remove the software.

- **Installing Product Distributions**
  Before beginning your upgrade, download Oracle Fusion Middleware Infrastructure and Oracle Identity and Access Management 12c (12.2.1.4.0) distributions on the target system and install them using Oracle Universal Installer.

- **Enabling WebGates to Work With Oracle Access Management**
  After upgrading to Oracle Access Management 12c (12.2.1.4.0), the earlier version of WebGates continues to work with Oracle Access Management. However, to leverage the latest security features of Oracle Access Management and WebGates 12c (12.2.1.4.0), you must upgrade the WebGates to 12c (12.2.1.4.0), and register the agent's profile with the Oracle Access Management Server.
About the Oracle Access Management Single Node Upgrade Process

Review the roadmap for an overview of the upgrade process for Oracle Access Management single node deployments.

The steps you take to upgrade your existing domain will vary depending on how your domain is configured and which components are being upgraded. Follow only those steps that are applicable to your deployment.

Table 3-1  Tasks for Upgrading Single Node Oracle Identity and Access Management Deployments

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required</strong></td>
<td>If you have not done so already, review the introductory topics in this guide and complete the required pre-upgrade tasks. See:</td>
</tr>
<tr>
<td></td>
<td>• Introduction to Upgrading Oracle Identity and Access Management</td>
</tr>
<tr>
<td></td>
<td>• Pre-Upgrade Requirements</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>Shut down the 12c environment (stop all Administration and Managed Servers). Ensure that the Database is up during the upgrade. WARNING: Failure to shut down your servers during an upgrade may lead to data corruption. See Stopping Servers and Processes.</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>Uninstall Oracle Fusion Middleware Infrastructure and Oracle Identity and Access Management 12c (12.2.1.3.0) in the existing Oracle home. See Uninstalling the Software.</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>Install Fusion Middleware Infrastructure and Oracle Identity and Access Management 12c (12.2.1.4.0) in the existing Oracle home. Install Fusion Middleware Infrastructure and Oracle Identity and Access Management in the same Oracle home on the same host as the 12c (12.2.1.3.0) production deployment before you begin the upgrade. In 12c (12.2.1.4.0), Oracle home is used to describe the 12c Middleware home. See Installing Product Distributions.</td>
</tr>
<tr>
<td><strong>Complete any necessary post-upgrade tasks.</strong></td>
<td>This is optional. Perform the following tasks based on your deployment:</td>
</tr>
<tr>
<td></td>
<td>• Enabling WebGates to Work With Oracle Access Management</td>
</tr>
</tbody>
</table>

Completing the Pre-Upgrade Tasks for Oracle Access Management

Complete the pre-upgrade tasks described in this section before you upgrade Oracle Access Management.

- Checking the Supported Starting Point for Oracle Access Management Upgrade
  The Oracle Access Management version that is supported for upgrade is 12c (12.2.1.3.0).
Checking the Supported Starting Point for Oracle Access Management Upgrade

The Oracle Access Management version that is supported for upgrade is 12c (12.2.1.3.0).

If you are using an earlier version of Oracle Access Management, you must upgrade to Oracle Access Management 12c (12.2.1.3.0) first, and then to 12c (12.2.1.4.0).

Stopping Servers and Processes

Before you upgrade the schemas and configurations, you must shut down all of the pre-upgrade processes and servers, including the Administration Server and any managed servers on OIMHOST.

An Oracle Fusion Middleware environment can consist of an Oracle WebLogic Server domain, an Administration Server, multiple managed servers, Java components, system components such as Identity Management components, and a database used as a repository for metadata. The components may be dependent on each other, so they must be stopped in the correct order.

**Note:**

- The procedures in this section describe how to stop the existing, pre-upgrade servers and processes using the WLST command-line utility or a script. You can also use the Oracle Fusion Middleware Control and the Oracle WebLogic Server Administration Console. See Starting and Stopping Administration and Managed Servers and Node Manager.
- Stop all of the servers in your deployment, except for the Database. The Database must be up during the upgrade process.

To stop your pre-upgrade Fusion Middleware environment, navigate to the pre-upgrade domain and follow the steps below.

**Step 1: Stop the Managed Servers**

To stop a WebLogic Server Managed Server, use the `stopManagedWebLogic` script:

- (UNIX) `EXISTING_DOMAIN_HOME/bin/stopManagedWebLogic.sh`
  
  `managed_server_name admin_url`

- (Windows) `EXISTING_DOMAIN_HOME\bin\stopManagedWebLogic.cmd`
  
  `managed_server_name admin_url`

When prompted, enter your user name and password.

**Step 2: Stop the Administration Server**

When you stop the Administration Server, you also stop the processes running in the Administration Server, including the WebLogic Server Administration Console and Fusion Middleware Control.
To stop the Administration Server, use the `stopWebLogic` script:

- (UNIX) `EXISTING_DOMAIN_HOME/bin/stopWebLogic.sh`
- (Windows) `EXISTING_DOMAIN_HOME\bin\stopWebLogic.cmd`

When prompted, enter your user name, password, and the URL of the Administration Server.

**Step 3: Stop Node Manager**

To stop Node Manager, close the command shell in which it is running.

Alternatively, after having set the `nodemanager.properties` attribute `QuitEnabled` to `true` (the default is `false`), you can use WLST to connect to Node Manager and shut it down. See `stopNodeManager` in *WLST Command Reference for WebLogic Server*.

---

**Uninstalling the Software**

Follow the instructions in this section to start the Uninstall Wizard and remove the software.

If you want to uninstall the product in a silent (command-line) mode, see Running the Oracle Universal Installer for Silent Uninstallation in *Installing Software with the Oracle Universal Installer*.

- Starting the Uninstall Wizard
- Selecting the Product to Uninstall
- Navigating the Uninstall Wizard Screens

**Starting the Uninstall Wizard**

Start the Uninstall Wizard:

1. Change to the following directory:
   - (UNIX) `ORACLE_HOME/oui/bin`
   - (Windows) `ORACLE_HOME\oui\bin`

2. Enter the following command:
   - (UNIX) `./deinstall.sh`
   - (Windows) `deinstall.cmd`

**Selecting the Product to Uninstall**

Because multiple products exist in the Oracle home, ensure that you are uninstalling the correct product.

After you run the Uninstall Wizard, the Distribution to Uninstall screen opens.

- For OAM or OIM only install: Click **Uninstall**.
- For OAM or OIM installed with other products: From the dropdown menu, select the Oracle Identity and Access Management 12.2.1.3.0 product and click **Uninstall**.
The uninstallation program shows the screens listed in Navigating the Uninstall Wizard Screens.

Run the Uninstall Wizard again to uninstall the Oracle Fusion Middleware Infrastructure. For instructions see, Uninstalling Oracle Fusion Middleware Infrastructure in Installing and Configuring the Oracle Fusion Middleware Infrastructure.

Navigating the Uninstall Wizard Screens

The Uninstall Wizard shows a series of screens to confirm the removal of the software.

If you need help on screen listed in the following table, click Help on the screen.

### Table 3-2 Uninstall Wizard Screens and Descriptions

<table>
<thead>
<tr>
<th>Screen</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome</td>
<td>Introduces you to the product Uninstall Wizard.</td>
</tr>
<tr>
<td>Uninstall Summary</td>
<td>Shows the Oracle home directory and its contents that are uninstalled. Verify that this is the correct directory. If you want to save these options to a response file, click Save Response File and enter the response file location and name. You can use the response file later to uninstall the product in silent (command-line) mode. See Running the Oracle Universal Installer for Silent Uninstall in Installing Software with the Oracle Universal Installer. Click Deinstall, to begin removing the software.</td>
</tr>
<tr>
<td>Uninstall Progress</td>
<td>Shows the uninstallation progress.</td>
</tr>
<tr>
<td>Uninstall Complete</td>
<td>Appears when the uninstallation is complete. Review the information on this screen, then click Finish to close the Uninstall Wizard.</td>
</tr>
</tbody>
</table>

**Note:**

After the product is uninstalled, ensure that the ORACLE_HOME folder exists and it does not contain any files or folders. If there are any remaining files or folders in the ORACLE_HOME folder, delete them.

Installing Product Distributions

Before beginning your upgrade, download Oracle Fusion Middleware Infrastructure and Oracle Identity and Access Management 12c (12.2.1.4.0) distributions on the target system and install them using Oracle Universal Installer.

**Note:**

When Infrastructure is required for the upgrade, you must install the Oracle Fusion Middleware distribution first before you install other Fusion Middleware products.

To install the 12c (12.2.1.4.0) distributions:
1. Sign in to the target system.

2. Download the following from Oracle Technology Network or Oracle Software Delivery Cloud to your target system:
   - If you have not yet installed Oracle Fusion Middleware Infrastructure, then download Oracle Fusion Middleware Infrastructure (fmw_12.2.1.4.0_infrastructure.jar)
   - Oracle Identity and Access Management (fmw_12.2.1.4.0_idm.jar)
   - Any additional distributions for your pre-upgrade environment

3. Change to the directory where you downloaded the 12c (12.2.1.4.0) product distribution.

4. If you have already installed Oracle Fusion Middleware Infrastructure (fmw_12.2.1.4.0_infrastructure.jar), go to step 15.

5. Start the installation program for Oracle Fusion Middleware Infrastructure:
   - (UNIX) JDK_HOME/bin/java -jar fmw_12.2.1.4.0_infrastructure.jar
   - (Windows) JDK_HOME\bin\java -jar fmw_12.2.1.4.0_infrastructure.jar

6. On UNIX operating systems, the Installation Inventory Setup screen appears if this is the first time you are installing an Oracle product on this host. Specify the location where you want to create your central inventory. Make sure that the operating system group name selected on this screen has write permissions to the central inventory location, and click Next.

   **Note:** The Installation Inventory Setup screen does not appear on Windows operating systems.

7. On the Welcome screen, review the information to make sure that you have met all the prerequisites. Click Next.

8. On the Auto Updates screen, select an option:
   - **Skip Auto Updates:** If you do not want your system to check for software updates at this time.
   - **Select patches from directory:** To navigate to a local directory if you downloaded patch files.
   - **Search My Oracle Support for Updates:** To automatically download software updates if you have a My Oracle Support account. You must enter Oracle Support credentials then click Search. To configure a proxy server for the installer to access My Oracle Support, click Proxy Settings. Click Test Connection to test the connection.

   Click Next.

9. On the Installation Location screen, specify the location for the Oracle home directory and click Next.

   For more information about Oracle Fusion Middleware directory structure, see Understanding Directories for Installation and Configuration in Oracle Fusion Middleware Planning an Installation of Oracle Fusion Middleware.
10. On the Installation Type screen, select the following:
   - For Infrastructure, select **Fusion Middleware Infrastructure**
   - For Oracle Identity and Access Management, select **Standalone Oracle Identity and Access Manager** or **Collocated Oracle Identity and Access Manager** based on your requirement.

   Click **Next**.

11. The Prerequisite Checks screen analyzes the host computer to ensure that the specific operating system prerequisites have been met.

   To view the list of tasks that are verified, select **View Successful Tasks**. To view log details, select **View Log**. If any prerequisite check fails, then an error message appears at the bottom of the screen. Fix the error and click **Rerun** to try again. To ignore the error or the warning message and continue with the installation, click **Skip** (not recommended).

12. On the Installation Summary screen, verify the installation options that you selected.

   If you want to save these options to a response file, click **Save Response File** and enter the response file location and name. The response file collects and stores all the information that you have entered, and enables you to perform a silent installation (from the command line) at a later time.

   Click **Install** to begin the installation.

13. On the Installation Progress screen, when the progress bar displays 100%, click **Finish** to dismiss the installer, or click **Next** to see a summary.

14. The Installation Complete screen displays the Installation Location and the Feature Sets that are installed. Review this information and click **Finish** to close the installer.

   **Note:**

   If your 12.2.1.3.0 setup was deployed using Life Cycle Management (LCM) tool, you must install Oracle HTTP Server 12c (12.2.1.4.0) in the 12c Middleware home. See Preparing to Install and Configure Oracle HTTP Server in *Installing and Configuring Oracle HTTP Server*.

   **Note:**

   Upgrading schemas is applicable only if your existing domain has both Oracle Access Management (OAM) and Oracle Identity Manager (OIM) installed.

---

**Enabling WebGates to Work With Oracle Access Management**

After upgrading to Oracle Access Management 12c (12.2.1.4.0), the earlier version of WebGates continues to work with Oracle Access Management. However, to leverage the latest security features of Oracle Access Management and WebGates 12c...
(12.2.1.4.0), you must upgrade the WebGates to 12c (12.2.1.4.0), and register the agent's profile with the Oracle Access Management Server.

**Note:**

If you have any other components of Oracle Identity and Access Management deployed, then all of the components must to be upgraded to 12c (12.2.1.4.0) to leverage the new security features of 12c (12.2.1.4.0).

To upgrade the WebGates, you must upgrade the respective Web Servers to 12c (12.2.1.4.0).

To upgrade the Oracle HTTP Server WebGates, upgrade Oracle HTTP Server to 12c (12.2.1.4.0). See Upgrading a Standalone Oracle HTTP Server in the *Upgrading Oracle HTTP Server*.

To upgrade the Oracle Traffic Directory WebGates, upgrade Oracle Traffic Directory to 12c (12.2.1.4.0). See Upgrading Oracle Traffic Director in the *Upgrading Oracle Traffic Director*.

After you upgrade the Web Servers, do the following:

1. Register or edit the WebGate profile and copy the WebGate artifacts to the WebGate config folder. See Upgrading to OHS/OTD 12c (12.2.1.4.0) WebGate in the *Installing WebGates for Oracle Access Manager*.

2. Start and stop the WebGates.
You can upgrade Oracle Identity Manager from Release 12c (12.2.1.3.0) to Oracle Identity Governance 12c (12.2.1.4.0).

Note: The product Oracle Identity Manager is referred to as Oracle Identity Manager (OIM) and Oracle Identity Governance (OIG) interchangeably in the guide.

Complete the steps in the following topics to perform the upgrade:

- **About the Oracle Identity Manager Single Node Upgrade Process**
  Review the roadmap for an overview of the upgrade process for Oracle Identity Manager single node deployments.

- **Generating and Analyzing Pre-Upgrade Report for Oracle Identity Manager**
  Run the pre-upgrade report utility before you begin the upgrade process for Oracle Identity Manager, and address all of the issues using the solution provided in the report.

- **Completing the Pre-Upgrade Tasks for Oracle Identity Manager**
  Complete the pre-upgrade tasks described in this section before you upgrade Oracle Identity Manager.

- **Stopping Servers and Processes**
  Before you upgrade the schemas and configurations, you must shut down all of the pre-upgrade processes and servers, including the Administration Server and any managed servers on OIMHOST.

- **Backing up the 12c (12.2.1.3.0) Middleware Home Folder on OIMHOST**
  Backup the 12c (12.2.1.3.0) Middleware Home on OIMHOST.

- **Uninstalling the Software**
  Follow the instructions in this section to start the Uninstall Wizard and remove the software.

- **Installing Product Distributions**
  Before beginning your upgrade, download Oracle Fusion Middleware Infrastructure, Oracle SOA Suite, and Oracle Identity and Access Management 12c (12.2.1.4.0) distributions on the target system and install them by using the Oracle Universal Installer in the existing 12c (12.2.1.3.0) Middleware home.

- **Updating the JDK location**
  When upgrading from 12c (12.2.1.3.0) to 12c (12.2.1.4.0), the reconfiguration wizard is not used. So, the latest JDK version is not automatically updated in the domain home.
- **Running a Pre-Upgrade Readiness Check**
  To identify potential issues with the upgrade, Oracle recommends that you run a readiness check before you start the upgrade process. Be aware that the readiness check may not be able to discover all potential issues with your upgrade. An upgrade may still fail, even if the readiness check reports success.

- **Tuning Database Parameters for Oracle Identity Manager**
  Before you upgrade the schemas, you must tune the Database parameters for Oracle Identity Manager.

- **Upgrading Product Schemas**
  After stopping servers and processes, use the Upgrade Assistant to upgrade supported product schemas to the current release of Oracle Fusion Middleware.

- **Tuning Application Module for User Interface**
  After you upgrade the Oracle Identity Manager middle tier successfully, tune the Application Module (AM) for user interface.

- **Upgrading Domain Component Configurations**
  Use the Upgrade Assistant to upgrade the domain component configurations inside the domain to match the updated domain configuration.

- **Copying oracle.iam.ui.custom-dev-starter-pack.war from 12c Middleware Home**

- **Post-Upgrade Task**
  If you had set custom configuration in your 12c (12.2.1.3.0) Middleware home, you need to copy the custom configuration present in your 12c (12.2.1.3.0) Middleware home to the 12c (12.2.1.4.0) Middleware home.

- **Starting the Servers**
  After you upgrade Oracle Identity Manager, start the servers.

- **Upgrading Oracle Identity Manager Design Console**
  Upgrade the Oracle Identity Manager Design Console after you upgrade the Oracle Identity Manager (OIM) domain component configurations.

- **Completing the Post-Upgrade Tasks for SSL Enabled Setup**
  If you are upgrading Oracle Identity Manager SSL enabled setup, you must perform the required post-upgrade tasks to complete the upgrade process.

- **Installing Standalone Oracle BI Publisher**
  When you upgrade Oracle Identity Manager 11g (11.1.2.3.0) to Oracle Identity Governance 12c (12.2.1.3.0), the embedded Oracle BI Publisher present in the 11g (11.1.2.3.0) deployment is removed. Therefore, post upgrade, you must install a new standalone Oracle BI Publisher 12c (12.2.1.3.0), for configuring the Oracle Identity Governance reports. Same BIP can be used after 12c (12.2.1.3.0) to 12c (12.2.1.4.0) upgrade.

---

**About the Oracle Identity Manager Single Node Upgrade Process**

Review the roadmap for an overview of the upgrade process for Oracle Identity Manager single node deployments.

The steps you take to upgrade your existing domain will vary depending on how your domain is configured and which components are being upgraded. Follow only those steps that are applicable to your deployment.
### Table 4-1  Tasks for Upgrading Oracle Identity Manager Single Node Environments

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Required**<br> If you have not done so already, review the introductory topics in this guide and complete the required pre-upgrade tasks. | See:  
• Introduction to Upgrading Oracle Identity and Access Management to 12c (12.2.1.4.0)  
• Pre-Upgrade Requirements |
| **Required**<br> Generate the pre-upgrade report for Oracle Identity Manager. Review the information in the report and perform the mandatory pre-upgrade tasks, if any. | See Generating and Analyzing Pre-Upgrade Report for Oracle Identity Manager. |
| **Required**<br> Complete the necessary pre-upgrade tasks specific to Oracle Identity Manager. | See Completing the Pre-Upgrade Tasks for Oracle Identity Manager. |
| **Required**<br> Shut down the 12c servers. This includes the Administration Server, Managed Servers, Node Manager, and system components like Oracle HTTP Server. Ensure that the Database is up during the upgrade. | WARNING: Failure to shut down your servers during an upgrade may lead to data corruption. See Stopping Servers and Processes. |
| **Required**<br> Create backup of the existing 12c (12.2.1.3.0) Middleware home folders on OIMHOST | See Backing up the 12c (12.2.1.3.0) Middleware Home Folder on OIMHOST. |
| **Required**<br> Uninstall Oracle Fusion Middleware Infrastructure and Oracle Identity and Access Management 12c (12.2.1.3.0) in the existing Oracle home. | See Uninstalling the Software. |
| **Required**<br> Install Fusion Middleware Infrastructure 12c (12.2.1.4.0), Oracle SOA Suite 12c (12.2.1.4.0) and Oracle Identity and Access Management 12c (12.2.1.4.0) in the prepped 12c (12.2.1.3.0) Middleware home. | Install the following products in the prepped 12c (12.2.1.3.0) Middleware home on the same host as the 12c production deployment before you begin the upgrade.  
• Fusion Middleware Infrastructure 12c (12.2.1.4.0)  
• Oracle SOA Suite 12c (12.2.1.4.0)  
• Oracle Identity and Access Management 12c (12.2.1.4.0)  
It is recommended that you use the simplified installation process to install the products mentioned above, using the quick installer. The quick installer installs the Infrastructure, Oracle SOA Suite, and Oracle Identity and Access Management 12c (12.2.1.4.0) in one go. See Installing Oracle Identity Governance Using Quick Installer in the Installing and Configuring Oracle Identity and Access Management.  
The other option is to install these products separately using their respective installers. See Installing Product Distributions. |
| **Required**<br> Update the JDK location | See Updating the JDK location. |
| **Optional**<br> Run a pre-upgrade readiness check. | See Running a Pre-Upgrade Readiness Check. |
### Table 4-1  (Cont.) Tasks for Upgrading Oracle Identity Manager Single Node Environments

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required</strong></td>
<td>Tune the Database parameters for Oracle Identity Manager. See <a href="#">Tuning Database Parameters for Oracle Identity Manager</a>.</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>Start the Upgrade Assistant to upgrade the 12c database schemas and to migrate all active (in flight) instance data. See <a href="#">Upgrading Product Schemas</a>. <strong>NOTE:</strong> The upgrade of active instance data is started automatically when running the Upgrade Assistant. Once the data is successfully upgraded to the new 12c (12.2.1.4.0) environment, you can close the Upgrade Assistant. The closed instances will continue to upgrade through a background process.</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>Upgrade Domain Component Configurations See <a href="#">Upgrading Domain Component Configurations</a>.</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>Tune the application module for Oracle Identity Manager. See <a href="#">Tuning Application Module for User Interface</a>.</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>Update the JDK location See <a href="#">Updating the JDK location</a>.</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>Copy the <code>oracle.iam.ui.custom-dev-starter-pack.war</code> file to the 12c (12.2.1.4.0) Middleware Home. See <a href="#">Copying oracle.iam.ui.custom-dev-starter-pack.war to the 12c (12.2.1.4.0) Middleware Home</a>.</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>Start the servers. See <a href="#">Starting the Servers</a>.</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>Upgrade the Oracle Identity Manager Design Console to 12c (12.2.1.4.0). See <a href="#">Upgrading Oracle Identity Manager Design Console</a>.</td>
</tr>
<tr>
<td><strong>Optional</strong></td>
<td>Perform the post-upgrade tasks for SSL enabled setup. See <a href="#">Completing the Post-Upgrade Tasks for SSL Enabled Setup</a>.</td>
</tr>
<tr>
<td><strong>Optional</strong></td>
<td>When you upgrade to Oracle Identity Governance 12c (12.2.1.4.0), the embedded Oracle BI Publisher present in the 11.1.2.3.0 deployment is removed. Therefore, you must install a new standalone Oracle BI Publisher 12c (12.2.1.3.0) post upgrade, and integrate it with Oracle Identity Governance 12c (12.2.1.4.0) to configure the Oracle Identity Governance reports. See <a href="#">Installing Standalone Oracle BI Publisher</a>.</td>
</tr>
</tbody>
</table>

---

**Note:**
The `jce` should use unlimited strength crypto policy.
Generating and Analyzing Pre-Upgrade Report for Oracle Identity Manager

Run the pre-upgrade report utility before you begin the upgrade process for Oracle Identity Manager, and address all of the issues using the solution provided in the report.

The pre-upgrade report utility analyzes your existing Oracle Identity Manager environment, and provides information about the mandatory prerequisites that you must complete before you begin the upgrade.

Note:

Run this report until no pending issues are listed in the report. It is important to address all of the issues listed in the pre-upgrade report before you proceed with the upgrade, as the upgrade might fail if the issues are not resolved.

Ensure that the Database and the 12.2.1.3.0 Oracle Identity Manager servers are up and running before you run the pre-upgrade report utility.

• Obtaining the Pre-Upgrade Report Utility
  Download the pre-upgrade report utility for Oracle Identity Manager from Oracle Technology Network (OTN).

• Generating the Pre-Upgrade Report
  Generate the pre-upgrade report before you start the upgrade process for Oracle Identity Manager, and resolve any issues listed in the report.

• Analyzing the Pre-Upgrade Report
  After you generate the pre-upgrade report for Oracle Identity Manager, review each of the reports, and perform all of the tasks described in them. If you do not perform the mandatory tasks described in the report, the upgrade might fail.

Obtaining the Pre-Upgrade Report Utility

Download the pre-upgrade report utility for Oracle Identity Manager from Oracle Technology Network (OTN).

The utility is available in a zip file named PreUpgradeReport_12cps4.zip at the following location on My Oracle Support:
My Oracle Support document ID 2579747.1

Generating the Pre-Upgrade Report

Generate the pre-upgrade report before you start the upgrade process for Oracle Identity Manager, and resolve any issues listed in the report.

To generate the pre-upgrade report for Oracle Identity Manager, complete the following steps:
1. Create a directory at any location and extract the contents of PreUpgradeReport_12cps4.zip in the new directory.

2. Create a directory in which to generate the pre-upgrade reports. For example, create a directory named OIM_preupgrade_reports.

3. Go to the directory where you extracted PreUpgradeReport_12cps4.zip and open the preupgrade_report_input.properties file in a text editor. Update the properties file with the appropriate values for the parameters listed in Table 4-2

Table 4-2 Parameters to be Specified in the preupgrade_report_input.properties File

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>oim.targetVersion</td>
<td>Specify the target version of the Oracle Identity Manager, that is, 12c (12.2.1.4.0).</td>
</tr>
<tr>
<td>oim.jdbcurl</td>
<td>Specify the JDBC URL for Oracle Identity Manager in one of the following formats: host:port/service_name or host:port:sid</td>
</tr>
<tr>
<td>oim.oimschemaowner</td>
<td>Specify the name of the OIM schema owner.</td>
</tr>
<tr>
<td>oim.mdsjdbcurl</td>
<td>Specify the MDS JDBC URL in the one of the following formats: host:port/service_name or host:port:sid</td>
</tr>
<tr>
<td>oim.mdsschemaowner</td>
<td>Specify the name of the MDS schema owner.</td>
</tr>
<tr>
<td>oim.databaseadminname</td>
<td>Specify the user with DBA privilege. For example, sys as sysdba.</td>
</tr>
<tr>
<td>oim.outputreportfolder</td>
<td>Specify the absolute path to the directory where you want the reports to be generated (OIM_preupgrade_reports). Ensure that this directory has read and write permissions.</td>
</tr>
<tr>
<td>oim.mwhome</td>
<td>Specify the absolute path to the Middleware home. For example: /Oracle/Middleware</td>
</tr>
<tr>
<td>oim.oimhome</td>
<td>Specify the absolute path to the existing OIM home. For example: oracle/Middleware/idm</td>
</tr>
<tr>
<td>oim.javahome</td>
<td>Specify the absolute path to the Java home. Ensure that you point to JAVA 8.</td>
</tr>
<tr>
<td>oim.wlshome</td>
<td>Specify the absolute path to the WebLogic Server home. For example: /Middleware/wlserver</td>
</tr>
<tr>
<td>oim.domain</td>
<td>Specify the absolute path to the Oracle Identity Manager domain home. For example: user_projects/domains/base_domain</td>
</tr>
</tbody>
</table>
4. Run the following command from the location where you extracted the contents of PreUpgradeReport.zip:

   - On UNIX:
     
     ```
     sh generatePreUpgradeReport.sh
     ```

   - On Windows:
     
     ```
     generatePreUpgradeReport.bat
     ```

5. Provide the details when the following are prompted:

   - **OIM Schema Password**: Enter the password of the Oracle Identity Manager (OIM) schema.
   - **MDS Schema Password**: Enter the password of the Metadata Services (MDS) schema.
   - **DBA Password**: Enter the password of the Database Administrator.

6. The reports are generated as HTML pages at the location you specified for the parameter `oim.outputreportfolder` in the `preupgrade_report_input.properties` file. The logs are stored in the log file `preUpgradeReport<time>.log` in the folder logs at the same location.

### Analyzing the Pre-Upgrade Report

After you generate the pre-upgrade report for Oracle Identity Manager, review each of the reports, and perform all of the tasks described in them. If you do not perform the mandatory tasks described in the report, the upgrade might fail.

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description and Action Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDS Back-up of source environment</td>
<td>This report lists the details regarding the MDS backup taken prior to upgrade.</td>
</tr>
<tr>
<td>Customized Notification Templates status on source environment</td>
<td>This report lists customized out-of-the-box (OOTB) notification templates. These customizations will be overwritten with OOTB values during upgrade.</td>
</tr>
<tr>
<td>Status of Domain Configuration</td>
<td>This report lists the applications (if any) that are in stage mode.</td>
</tr>
<tr>
<td>Authorization Policy Back-up of source environment</td>
<td>This report lists the details regarding the Oracle Identity Manager authorization policy backup taken prior to upgrade.</td>
</tr>
</tbody>
</table>

**Note:**

This report is generated only if there are any discrepancies found.
<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description and Action Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status of OIM default keystore in KSS on source environment</td>
<td>This report lists the OIM default keystore if it's present in the KSS of the source domain prior to upgrade.</td>
</tr>
<tr>
<td>Note:</td>
<td>This report is generated only if there are any discrepancies found.</td>
</tr>
<tr>
<td>Copy Custom UI WAR from source environment</td>
<td>This report reminds you to copy the custom UI war from the previous Middleware home to the new Middleware home, to get the UI customizations after upgrade.</td>
</tr>
<tr>
<td>Status of Database Vault Configuration</td>
<td>This is a conditional report. If database vault is enabled on source setup, then this report is created. This report displays information related to database vault settings.</td>
</tr>
<tr>
<td>Note:</td>
<td>This report is generated only if there are any discrepancies found.</td>
</tr>
</tbody>
</table>

### Completing the Pre-Upgrade Tasks for Oracle Identity Manager

Complete the pre-upgrade tasks described in this section before you upgrade Oracle Identity Manager.

- **Verifying the Memory Settings**
  To avoid the memory issues for Oracle Identity Manager, ensure that the memory settings are updated as per the requirements.

- **Opening the Non-SSL Ports for SSL Enabled Setup**
  If you have an SSL enabled and non-SSL disabled setup, you must open the non-SSL ports for Servers and Database before you proceed with the Oracle Identity Manager upgrade.
Verifying the Memory Settings

To avoid the memory issues for Oracle Identity Manager, ensure that the memory settings are updated as per the requirements.

On Linux, do the following:

1. Ensure that you set the following parameters in the `/etc/security/limits.conf` file, to the specified values:
   
   ```
   FUSION_USER_ACCOUNT soft nofile 32767
   FUSION_USER_ACCOUNT hard nofile 327679
   ```

2. Ensure that you set `UsePAM` to `Yes` in the `/etc/ssh/sshd_config` file.

3. Restart `sshd`.

4. Log out (or reboot) and log in to the system again.

Note:

Before you start the Oracle Identity Governance 12c (12.2.1.4.0) Server, post upgrade, run the following command to increase the limit of open files, so that you do not run into memory issues:

```
limit maxproc 16384
```

Opening the Non-SSL Ports for SSL Enabled Setup

If you have an SSL enabled and non-SSL disabled setup, you must open the non-SSL ports for Servers and Database before you proceed with the Oracle Identity Manager upgrade.

Stopping Servers and Processes

Before you upgrade the schemas and configurations, you must shut down all of the pre-upgrade processes and servers, including the Administration Server and any managed servers on OIMHOST.

An Oracle Fusion Middleware environment can consist of an Oracle WebLogic Server domain, an Administration Server, multiple managed servers, Java components, system components such as Identity Management components, and a database used as a repository for metadata. The components may be dependent on each other, so they must be stopped in the correct order.
To stop your pre-upgrade Fusion Middleware environment, navigate to the pre-upgrade domain and follow the steps below.

**Step 1: Stop the Managed Servers**

To stop a WebLogic Server Managed Server, use the `stopManagedWebLogic` script:

- (UNIX) `EXISTING_DOMAIN_HOME/bin/stopManagedWebLogic.sh`  
  `managed_server_name admin_url`
- (Windows) `EXISTING_DOMAIN_HOME\bin\stopManagedWebLogic.cmd`  
  `managed_server_name admin_url`

When prompted, enter your user name and password.

**Step 2: Stop the Administration Server**

When you stop the Administration Server, you also stop the processes running in the Administration Server, including the WebLogic Server Administration Console and Fusion Middleware Control.

To stop the Administration Server, use the `stopWebLogic` script:

- (UNIX) `EXISTING_DOMAIN_HOME/bin/stopWebLogic.sh`
- (Windows) `EXISTING_DOMAIN_HOME\bin\stopWebLogic.cmd`

When prompted, enter your user name, password, and the URL of the Administration Server.

**Step 3: Stop Node Manager**

To stop Node Manager, close the command shell in which it is running.

Alternatively, after having set the `nodemanager.properties` attribute `QuitEnabled` to `true` (the default is `false`), you can use WLST to connect to Node Manager and shut it down. See `stopNodeManager` in `WLST Command Reference for WebLogic Server`.

---

**Backing up the 12c (12.2.1.3.0) Middleware Home Folder on OIMHOST**

Backup the 12c (12.2.1.3.0) Middleware Home on OIMHOST.

As a backup, copy and rename the 12.2.1.3.0 Middleware home folder on OIMHOST.
Uninstalling the Software

Follow the instructions in this section to start the Uninstall Wizard and remove the software.

If you want to uninstall the product in a silent (command-line) mode, see Running the Oracle Universal Installer for Silent Uninstallation in Installing Software with the Oracle Universal Installer.

• Starting the Uninstall Wizard
• Selecting the Product to Uninstall
• Navigating the Uninstall Wizard Screens

Starting the Uninstall Wizard

Start the Uninstall Wizard:

1. Change to the following directory:
   (UNIX) ORACLE_HOME/oui/bin
   (Windows) ORACLE_HOME\oui\bin
2. Enter the following command:
   (UNIX) ./deinstall.sh
   (Windows) deinstall.cmd

Selecting the Product to Uninstall

Because multiple products exist in the Oracle home, ensure that you are uninstalling the correct product.

After you run the Uninstall Wizard, the Distribution to Uninstall screen opens.

• For OAM or OIM only install: Click Uninstall.
• For OAM or OIM installed with other products: From the dropdown menu, select the Oracle Identity and Access Management 12.2.1.3.0 product and click Uninstall.

The uninstallation program shows the screens listed in Navigating the Uninstall Wizard Screens.

Run the Uninstall Wizard again to uninstall the Oracle Fusion Middleware Infrastructure. For instructions see, Uninstalling Oracle Fusion Middleware Infrastructure in Installing and Configuring the Oracle Fusion Middleware Infrastructure.

Navigating the Uninstall Wizard Screens

The Uninstall Wizard shows a series of screens to confirm the removal of the software.
If you need help on screen listed in the following table, click **Help** on the screen.

### Table 4-4  Uninstall Wizard Screens and Descriptions

<table>
<thead>
<tr>
<th>Screen</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome</td>
<td>Introduces you to the product Uninstall Wizard.</td>
</tr>
<tr>
<td>Uninstall Summary</td>
<td>Shows the Oracle home directory and its contents that are uninstalled. Verify that this is the correct directory. If you want to save these options to a response file, click <strong>Save Response File</strong> and enter the response file location and name. You can use the response file later to uninstall the product in silent (command-line) mode. See Running the Oracle Universal Installer for Silent Uninstall in <em>Installing Software with the Oracle Universal Installer</em>. Click <strong>Deinstall</strong>, to begin removing the software.</td>
</tr>
<tr>
<td>Uninstall Progress</td>
<td>Shows the uninstallation progress.</td>
</tr>
<tr>
<td>Uninstall Complete</td>
<td>Appears when the uninstallation is complete. Review the information on this screen, then click <strong>Finish</strong> to close the Uninstall Wizard.</td>
</tr>
</tbody>
</table>

**Note:**

After the product is uninstalled, ensure that the `ORACLE_HOME` folder exists and it does not contain any files or folders. If there are any remaining files or folders in the `ORACLE_HOME` folder, delete them.

### Installing Product Distributions

Before beginning your upgrade, download Oracle Fusion Middleware Infrastructure, Oracle SOA Suite, and Oracle Identity and Access Management 12c (12.2.1.4.0) distributions on the target system and install them by using the Oracle Universal Installer in the existing 12c (12.2.1.3.0) Middleware home.

**Note:**

When Infrastructure is required for the upgrade, you must install the Oracle Fusion Middleware distribution first before you install other Fusion Middleware products.

It is recommended that you use the simplified installation process to install the products mentioned above, using the quickstart installer (`fmw_12.2.1.4.0_idmquickstart_generic.jar`). The quickstart installer installs the Infrastructure, Oracle SOA Suite, and Oracle Identity and Access Management 12c (12.2.1.4.0) in one go.

See Installing Oracle Identity Governance Using Quickstart Installer in the *Installing and Configuring Oracle Identity and Access Management*.

The other option is to install the required product distributions — Infrastructure, Oracle SOA Suite, and Oracle Identity and Access Management 12c (12.2.1.4.0) separately. To do this, complete the following steps:
1. Sign in to the target system.

2. Download the following from Oracle Technology Network or Oracle Software Delivery Cloud to your target system:
   - If you not yet installed Oracle Fusion Middleware Infrastructure, then download Oracle Fusion Middleware Infrastructure
     (fmw_12.2.1.4.0_infrastructure_generic.jar)
   - Oracle SOA Suite (fmw_12.2.1.4.0_soa_generic.jar)
   - Oracle Identity and Access Management (fmw_12.2.1.4.0_idm.jar)

   **Note:** Ensure that the ORACLE_HOME folder exists and it does not contain any files or folders. If there are any remaining files or folders in the ORACLE_HOME folder, delete them.

3. Change to the directory where you downloaded the 12c (12.2.1.4.0) product distribution.

4. If you have already installed Oracle Fusion Middleware Infrastructure (fmw_12.2.1.4.0_infrastructure_generic.jar), got to step 15.

5. Start the installation program for Oracle Fusion Middleware Infrastructure:
   - (UNIX) JDK_HOME/bin/java -jar fmw_12.2.1.4.0_infrastructure.jar
   - (Windows) JDK_HOME\bin\java -jar fmw_12.2.1.4.0_infrastructure.jar

6. On UNIX operating systems, the Installation Inventory Setup screen appears if this is the first time you are installing an Oracle product on this host.
   Specify the location where you want to create your central inventory. Make sure that the operating system group name selected on this screen has write permissions to the central inventory location, and click **Next**.

   **Note:** The Installation Inventory Setup screen does not appear on Windows operating systems.

7. On the Welcome screen, review the information to make sure that you have met all the prerequisites. Click **Next**.

8. On the Auto Updates screen, select an option:
   - **Skip Auto Updates:** If you do not want your system to check for software updates at this time.
   - **Select patches from directory:** To navigate to a local directory if you downloaded patch files.
   - **Search My Oracle Support for Updates:** To automatically download software updates if you have a My Oracle Support account. You must enter Oracle Support credentials then click **Search**. To configure a proxy server for the installer to access My Oracle Support, click **Proxy Settings**. Click **Test Connection** to test the connection.
Click **Next**.

**9.** On the Installation Location screen, specify the location for the existing 12c (12.2.1.3.0) Middleware home directory and click **Next**.

For example: If 12c (12.2.1.3.0) Oracle_home is located under /u01/im/12c, first uninstall 12c (12.2.1.3.0) and clean up the directory to install 12c (12.2.1.4.0) into /u01/im/12c.

For more information about Oracle Fusion Middleware directory structure, see Understanding Directories for Installation and Configuration in *Oracle Fusion Middleware Planning an Installation of Oracle Fusion Middleware*.

**10.** On the Installation Type screen, select the following:

- For Infrastructure, select **Fusion Middleware Infrastructure**
- For Oracle SOA Suite, select **Oracle SOA Suite**
- For Oracle Identity and Access Management, select **Oracle Identity and Access Management**

Click **Next**.

**11.** The Prerequisite Checks screen analyzes the host computer to ensure that the specific operating system prerequisites have been met.

To view the list of tasks that are verified, select **View Successful Tasks**. To view log details, select **View Log**. If any prerequisite check fails, then an error message appears at the bottom of the screen. Fix the error and click **Rerun** to try again. To ignore the error or the warning message and continue with the installation, click **Skip** (not recommended).

**12.** On the Installation Summary screen, verify the installation options that you selected.

If you want to save these options to a response file, click **Save Response File** and enter the response file location and name. The response file collects and stores all the information that you have entered, and enables you to perform a silent installation (from the command line) at a later time.

Click **Install** to begin the installation.

**13.** On the Installation Progress screen, when the progress bar displays 100%, click **Finish** to dismiss the installer, or click **Next** to see a summary.

**14.** The Installation Complete screen displays the Installation Location and the Feature Sets that are installed. Review this information and click **Finish** to close the installer.

**15.** After you have installed Oracle Fusion Middleware Infrastructure, enter the following command to start the installer for your product distribution and repeat the steps above to navigate through the installer screens:

For installing Oracle SOA Suite 12c (12.2.1.4.0), run the following installer:

- (UNIX) `JDK_HOME/bin/java -jar fmw_12.2.1.4.0_soa_generic.jar`
- (Windows) `JDK_HOME\bin\java -jar fmw_12.2.1.4.0_soa_generic.jar`

For installing Oracle Identity and Access Management 12c (12.2.1.4.0), run the following installer:

- (UNIX) `JDK_HOME/bin/java -jar fmw_12.2.1.4.0_idm.jar`
- (Windows) `JDK_HOME\bin\java -jar fmw_12.2.1.4.0_idm.jar`
Updating the JDK location

When upgrading from 12c (12.2.1.3.0) to 12c (12.2.1.4.0), the reconfiguration wizard is not used. So, the latest JDK version is not automatically updated in the domain home.

After upgrading to 12c (12.2.1.4.0), you must search the references to the current JDK in domain home and replace those instances with the location of the new JDK.

If you have installed the latest version of the JDK in the same location as the existing JDK, by overwriting the files, then you can skip updating the JDK location.

You must manually search the references to the current JDK in domain home and replace those instances with the location of the new JDK. For information about updating the JDK location, see Updating the JDK Location in an Existing Domain Home.

Running a Pre-Upgrade Readiness Check

To identify potential issues with the upgrade, Oracle recommends that you run a readiness check before you start the upgrade process. Be aware that the readiness check may not be able to discover all potential issues with your upgrade. An upgrade may still fail, even if the readiness check reports success.

• About Running a Pre-Upgrade Readiness Check
  You can run the Upgrade Assistant in -readiness mode to detect issues before you perform the actual upgrade. You can run the readiness check in GUI mode using the Upgrade Assistant or in silent mode using a response file.

• Starting the Upgrade Assistant in Readiness Mode
  Use the -readiness parameter to start the Upgrade Assistant in readiness mode.

• Performing a Readiness Check with the Upgrade Assistant
  Navigate through the screens in the Upgrade Assistant to complete the pre-upgrade readiness check.

• Understanding the Readiness Report
  After performing a readiness check for your domain, review the report to determine whether you need to take any action for a successful upgrade.
About Running a Pre-Upgrade Readiness Check

You can run the Upgrade Assistant in -readiness mode to detect issues before you perform the actual upgrade. You can run the readiness check in GUI mode using the Upgrade Assistant or in silent mode using a response file.

The Upgrade Assistant readiness check performs a read-only, pre-upgrade review of your Fusion Middleware schemas and WebLogic domain configurations that are at a supported starting point. The review is a read-only operation.

The readiness check generates a formatted, time-stamped readiness report so you can address potential issues before you attempt the actual upgrade. If no issues are detected, you can begin the upgrade process. Oracle recommends that you read this report thoroughly before performing an upgrade.

You can run the readiness check while your existing Oracle Fusion Middleware domain is online (while other users are actively using it) or offline.

You can run the readiness check any number of times before performing any actual upgrade. However, do not run the readiness check after an upgrade has been performed, as the report results may differ from the result of pre-upgrade readiness checks.

**Note:**

To prevent performance from being affected, Oracle recommends that you run the readiness check during off-peak hours.

Starting the Upgrade Assistant in Readiness Mode

Use the -readiness parameter to start the Upgrade Assistant in readiness mode.

To perform a readiness check on your pre-upgrade environment with the Upgrade Assistant:

1. Go to the oracle_common/upgrade/bin directory:
   - (UNIX) `ORACLE_HOME/oracle_common/upgrade/bin`
   - (Windows) `ORACLE_HOME\oracle_common\upgrade\bin`

2. Start the Upgrade Assistant.
   - (UNIX) `./ua -readiness`
   - (Windows) `ua.bat -readiness`
Note:

If the `DISPLAY` environment variable is not set up properly to allow for GUI mode, you may encounter the following error:

```
Xlib: connection to ":1.0" refused by server
Xlib: No protocol specified
```

To resolve this issue, set the `DISPLAY` environment variable to the system name or IP address of your local workstation, and rerun Upgrade Assistant.

If you continue to receive these errors after setting `DISPLAY`, try launching another GUI tool, such as `vncconfig`. If you see the same errors, your `DISPLAY` environment variable may still not be set correctly.

For information about other parameters that you can specify on the command line, see:

- Upgrade Assistant Parameters

### Upgrade Assistant Parameters

When you start the Upgrade Assistant from the command line, you can specify additional parameters.

#### Table 4-5 Upgrade Assistant Command-Line Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-readiness</code></td>
<td>Required for readiness checks</td>
<td>Performs the upgrade readiness check without performing an actual upgrade. Schemas and configurations are checked. Do not use this parameter if you have specified the <code>-examine</code> parameter.</td>
</tr>
<tr>
<td><code>-threads</code></td>
<td>Optional</td>
<td>Identifies the number of threads available for concurrent schema upgrades or readiness checks of the schemas. The value must be a positive integer in the range 1 to 8. The default is 4.</td>
</tr>
<tr>
<td><code>-response</code></td>
<td>Required for silent upgrades or silent readiness checks</td>
<td>Runs the Upgrade Assistant using inputs saved to a response file generated from the data that is entered when the Upgrade Assistant is run in GUI mode. Using this parameter runs the Upgrade Assistant in silent mode (without displaying Upgrade Assistant screens).</td>
</tr>
</tbody>
</table>
### Table 4-5  (Cont.) Upgrade Assistant Command-Line Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-examine</td>
<td>Optional</td>
<td>Performs the examine phase but does not perform an actual upgrade. Do not specify this parameter if you have specified the -readiness parameter.</td>
</tr>
</tbody>
</table>
| -logLevel attribute | Optional             | Sets the logging level, specifying one of the following attributes:  
  • TRACE  
  • NOTIFICATION  
  • WARNING  
  • ERROR  
  • INCIDENT_ERROR  
  The default logging level is NOTIFICATION.  
  Consider setting the -logLevel TRACE attribute to so that more information is logged. This is useful when troubleshooting a failed upgrade. The Upgrade Assistant's log files can become very large if -logLevel TRACE is used. |
| -logDir location  | Optional             | Sets the default location of upgrade log files and temporary files. You must specify an existing, writable directory where the Upgrade Assistant creates log files and temporary files.  
  The default locations are:  
  (UNIX)  
  ORACLE_HOME/oracle_common/upgrade/logs  
  ORACLE_HOME/oracle_common/upgrade/temp  
  (Windows)  
  ORACLE_HOME/oracle_common\upgrade\logs  
  ORACLE_HOME/oracle_common\upgrade\temp  
  -help               | Optional             | Displays all of the command-line options.                                                                                                                                                                    |
Performing a Readiness Check with the Upgrade Assistant

Navigate through the screens in the Upgrade Assistant to complete the pre-upgrade readiness check.

Readiness checks are performed only on schemas or component configurations that are at a supported upgrade starting point.

To complete the readiness check:

1. On the Welcome screen, review information about the readiness check. Click Next.

2. On the Readiness Check Type screen, select the readiness check that you want to perform:
   
   • **Individually Selected Schemas** allows you to select individual schemas for review before upgrade. The readiness check reports whether a schema is supported for an upgrade or where an upgrade is needed. When you select this option, the screen name changes to Selected Schemas.
   
   • **Domain Based** allows the Upgrade Assistant to discover and select all upgrade-eligible schemas or component configurations in the domain specified in the Domain Directory field. When you select this option, the screen name changes to Schemas and Configuration.

   Leave the default selection if you want the Upgrade Assistant to check all schemas and component configurations at the same time, or select a specific option:

   – **Include checks for all schemas** to discover and review all components that have a schema available to upgrade.
   
   – **Include checks for all configurations** to review component configurations for a managed WebLogic Server domain.

   Click Next.

3. If you selected **Individually Selected Schemas**: On the Available Components screen, select the components that have a schema available to upgrade for which you want to perform a readiness check.

   If you selected **Domain Based**: On the Component List screen, review the list of components that are present in your domain for which you want to perform a readiness check.

   If you select a component that has dependent components, those components are automatically selected. For example, if you select Oracle Platform Security Services, Oracle Audit Services is automatically selected.

   Depending on the components you select, additional screens may display. For example, you may need to:

   • Specify the domain directory.
     
     Ensure that you specify the 12c (12.2.1.3.0) domain directory.
   
   • Specify schema credentials to connect to the selected schema: **Database Type**, **DBA User Name**, and **DBA Password**. Then click **Connect**.
Note:

Oracle database is the default database type. Make sure that you select the correct database type before you continue. If you discover that you selected the wrong database type, do not go back to this screen to change it to the correct type. Instead, close the Upgrade Assistant and restart the readiness check with the correct database type selected to ensure that the correct database type is applied to all schemas.

- Select the **Schema User Name** option and specify the **Schema Password**.

Note:

The Upgrade Assistant automatically enables default credentials. If you are unable to connect, make sure that you manually enter the credentials for your schema before you continue.

Click **Next** to start the readiness check.

4. On the Readiness Summary screen, review the summary of the readiness checks that will be performed based on your selections.

If you want to save your selections to a response file to run the Upgrade Assistant again later in response (or silent) mode, click **Save Response File** and provide the location and name of the response file. A silent upgrade performs exactly the same function that the Upgrade Assistant performs, but you do not have to manually enter the data again.

For a detailed report, click **View Log**.

Click **Next**.

5. On the Readiness Check screen, review the status of the readiness check. The process can take several minutes.

If you are checking multiple components, the progress of each component displays in its own progress bar in parallel.

When the readiness check is complete, click **Continue**.

The following components are marked as **ready for upgrade** although they are not upgraded. Ignore the **ready for upgrade** message against these components:

- Oracle JRF
- Common Infrastructure Services
- Oracle Web Services Manager

6. On the End of Readiness screen, review the results of the readiness check (**Readiness Success** or **Readiness Failure**):

- If the readiness check is successful, click **View Readiness Report** to review the complete report. Oracle recommends that you review the Readiness Report before you perform the actual upgrade even when the readiness check is successful. Use the **Find** option to search for a particular word or phrase within the report. The report also indicates where the completed Readiness Check Report file is located.
• If the readiness check encounters an issue or error, click View Log to review the log file, identify and correct the issues, and then restart the readiness check. The log file is managed by the command-line options you set.

Understanding the Readiness Report

After performing a readiness check for your domain, review the report to determine whether you need to take any action for a successful upgrade.

The format of the readiness report file is:

`readiness<timestamp>.txt`

Where, `timestamp` indicates the date and time of when the readiness check was run.

A readiness report contains the following information:

Table 4-6  Readiness Report Elements

<table>
<thead>
<tr>
<th>Report Information</th>
<th>Description</th>
<th>Required Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Readiness Status: SUCCESS or FAILURE</td>
<td>The top of the report indicates whether the readiness check passed or completed with one or more errors.</td>
<td>If the report completed with one or more errors, search for FAIL and correct the failing issues before attempting to upgrade. You can re-run the readiness check as many times as necessary before an upgrade.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>The date and time that the report was generated.</td>
<td>No action required.</td>
</tr>
<tr>
<td>Log file location</td>
<td>The directory location of the generated log file.</td>
<td>No action required.</td>
</tr>
<tr>
<td>/oracle_common/upgrade/logs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Directory</td>
<td>Displays the domain location</td>
<td>No action required.</td>
</tr>
<tr>
<td>Readiness report location</td>
<td>The directory location of the generated readiness report.</td>
<td>No action required.</td>
</tr>
<tr>
<td>/oracle_common/upgrade/logs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Names of components that were checked</td>
<td>The names and versions of the components included in the check and status.</td>
<td>If your domain includes components that cannot be upgraded to this release, such as SOA Core Extension, do not attempt an upgrade.</td>
</tr>
<tr>
<td>Names of schemas that were checked</td>
<td>The names and current versions of the schemas included in the check and status.</td>
<td>Review the version numbers of your schemas. If your domain includes schemas that cannot be upgraded to this release, do not attempt an upgrade.</td>
</tr>
<tr>
<td>Individual Object Test Status: FAIL</td>
<td>The readiness check test detected an issue with a specific object.</td>
<td>Do not upgrade until all failed issues have been resolved.</td>
</tr>
</tbody>
</table>
Table 4-6  (Cont.) Readiness Report Elements

<table>
<thead>
<tr>
<th>Report Information</th>
<th>Description</th>
<th>Required Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual Object Test Status: PASS</td>
<td>The readiness check test detected no issues for the specific object.</td>
<td>If your readiness check report shows only the PASS status, you can upgrade your environment. Note, however, that the Readiness Check cannot detect issues with externals such as hardware or connectivity during an upgrade. You should always monitor the progress of your upgrade.</td>
</tr>
<tr>
<td>Completed Readiness Check of &lt;Object&gt; Status: FAILURE</td>
<td>The readiness check detected one or more errors that must be resolved for a particular object such as a schema, an index, or datatype.</td>
<td>Do not upgrade until all failed issues have been resolved.</td>
</tr>
<tr>
<td>Completed Readiness Check of &lt;Object&gt; Status: SUCCESS</td>
<td>The readiness check test detected no issues.</td>
<td>No action required.</td>
</tr>
</tbody>
</table>

Here is a sample Readiness Report file. Your report may not include all of these checks.

Upgrade readiness check completed with one or more errors.

This readiness check report was created on Fri Aug 16 13:29:41 PDT 2019
Log file is located at: /oracle/work/middleware_latest/oracle_common/
upgrade/logs/ua2019-08-16-13-23-36PM.log
Readiness Check Report File: /oracle/work/middleware_latest/oracle_common/
upgrade/logs/readiness2019-08-16-13-29-41PM.txt
Domain Directory: /oracle/work/middleware_latest/oracle_common/
upgrade/logs/readiness2019-08-16-13-29-41PM.txt

Starting readiness check of components.

Oracle Platform Security Services
Starting readiness check of Oracle Platform Security Services.
  Schema User Name: DEV3_OPSS
  Database Type: Oracle Database
  Database Connect String:
    VERSION Schema DEV3_OPSS is currently at version 12.1.2.0.0.

Readiness checks will now be performed.
Starting schema test: TEST_DATABASE_VERSION Test that the database server version number is supported for upgrade
  INFO  Database product version: Oracle Database 12c Enterprise
Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options
Starting schema test: TEST_DATABASE_VERSION --> Test that the database server version number is supported for upgrade ++ PASS
Starting schema test: TEST_REQUIRED_TABLES Test that the schema contains all the required tables
Starting schema test: TEST_REQUIRED_TABLES --> Test that the schema contains all the required tables ++ PASS
Starting schema test: Test that the schema does not contain any
Running a Pre-Upgrade Readiness Check

Oracle Audit Services
Starting readiness check of Oracle Audit Services.
Schema User Name: DEV3_IAU
Database Type: Oracle Database
Database Connect String:
VERSION Schema DEV3_IAU is currently at version 12.1.2.0.0.
Readiness checks will now be performed.
Starting schema test: TEST_DATABASE_VERSION Test that the database server version number is supported for upgrade
INFO Database product version: Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 – 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options
Completed schema test: TEST_DATABASE_VERSION --> Test that the database server version number is supported for upgrade +++ PASS
Starting schema test: TEST_REQUIRED_TABLES Test that the schema contains all the required tables
Completed schema test: TEST_REQUIRED_TABLES --> Test that the schema contains all the required tables +++ PASS
Starting schema test: TEST_UNEXPECTED_TABLES Test that the schema does not contain any unexpected tables
Completed schema test: TEST_UNEXPECTED_TABLES --> Test that the schema does not contain any unexpected tables +++ PASS
Starting schema test: TEST_ENOUGH_TABLESPACE Test that the schema tablespaces automatically extend if full
Completed schema test: TEST_ENOUGH_TABLESPACE --> Test that the schema tablespaces automatically extend if full +++ PASS
Starting schema test: TEST_USER_TABLESPACE_QUOTA Test that tablespace quota for this user is sufficient to perform the upgrade
Completed schema test: TEST_USER_TABLESPACE_QUOTA --> Test that tablespace quota for this user is sufficient to perform the upgrade +++ PASS
Starting schema test: TEST_ONLINE_TABLESPACE Test that schema tablespaces are online
Completed schema test: TEST_ONLINE_TABLESPACE --> Test that schema tablespaces are online +++ PASS
Starting permissions test: TEST_DBA_TABLE_GRANTS Test that DBA user has privilege to view all user tables
Completed permissions test: TEST_DBA_TABLE_GRANTS --> Test that DBA user has privilege to view all user tables +++ PASS
Starting schema test: SEQUENCE_TEST Test that the Oracle Platform Security Services schema sequence and its properties are valid
Completed schema test: SEQUENCE_TEST --> Test that the Oracle Platform Security Services schema sequence and its properties are valid +++ PASS
Finished readiness check of Oracle Platform Security Services with status: SUCCESS.
Starting schema test: TEST_USER_TABLESPACE_QUOTA  Test that tablespace quota for this user is sufficient to perform the upgrade
Completed schema test: TEST_USER_TABLESPACE_QUOTA --> Test that tablespace quota for this user is sufficient to perform the upgrade +++ PASS

Starting schema test: TEST_ONLINE_TABLESPACE  Test that schema tablespaces are online
Completed schema test: TEST_ONLINE_TABLESPACE --> Test that schema tablespaces are online +++ PASS

Starting permissions test: TEST_DBA_TABLE_GRANTS  Test that DBA user has privilege to view all user tables
Completed permissions test: TEST_DBA_TABLE_GRANTS --> Test that DBA user has privilege to view all user tables +++ PASS

Starting schema test: TEST_MISSING_COLUMNS  Test that tables and views are not missing any required columns
Completed schema test: TEST_MISSING_COLUMNS --> Test that tables and views are not missing any required columns +++ PASS

Starting schema test: TEST_UNEXPECTED_COLUMNS  Test that tables and views do not contain any unexpected columns
Completed schema test: TEST_UNEXPECTED_COLUMNS --> Test that tables and views do not contain any unexpected columns +++ PASS

Starting datatype test for table OIDCOMPONENT: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes
Completed datatype test for table OIDCOMPONENT: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes +++ PASS

Starting datatype test for table IAU_CUSTOM_01: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes
Completed datatype test for table IAU_CUSTOM_01: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes +++ PASS

Starting datatype test for table IAU_BASE: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes
Completed datatype test for table IAU_BASE: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes +++ PASS

Starting datatype test for table WS_POLICYATTACHMENT: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes
Completed datatype test for table WS_POLICYATTACHMENT: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes +++ PASS

Starting datatype test for table OWSM_PM_EJB: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes
Completed datatype test for table OWSM_PM_EJB: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes +++ PASS

Starting datatype test for table XMLPSERVER: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes
Completed datatype test for table XMLPSERVER: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes +++ PASS

Starting datatype test for table SOA_HCFP: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes
Completed datatype test for table SOA_HCFP: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes +++ PASS
Starting schema test: SEQUENCE_TEST  Test that the audit schema sequence and its properties are valid
Completed schema test: SEQUENCE_TEST --> Test that the audit schema sequence and its properties are valid +++ PASS
Starting schema test: SYNONYMS_TEST  Test that the audit schema required synonyms are present
Completed schema test: SYNONYMS_TEST --> Test that the audit schema required synonyms are present +++ PASS
Finished readiness check of Oracle Audit Services with status: FAILURE.

Common Infrastructure Services
Starting readiness check of Common Infrastructure Services.
  Schema User Name: DEV3_STB
  Database Type: Oracle Database
  Database Connect String:
Starting schema test: TEST_REQUIRED_TABLES  Test that the schema contains all the required tables
Completed schema test: TEST_REQUIRED_TABLES --> Test that the schema contains all the required tables +++ PASS
Completed schema test: ALL_TABLES --> TEST_REQUIRED_TABLES +++ Test that the schema contains all the required tables
Starting schema test: TEST_UNEXPECTED_TABLES  Test that the schema does not contain any unexpected tables
Completed schema test: ALL_TABLES --> TEST_UNEXPECTED_TABLES +++ Test that the schema does not contain any unexpected tables
Starting schema test: TEST_REQUIRED_VIEWS  Test that the schema contains all the required database views
Completed schema test: ALL_TABLES --> TEST_REQUIRED_VIEWS +++ Test that the schema contains all the required database views
Starting schema test: TEST_MISSING_COLUMNS  Test that tables and views are not missing any required columns
Completed schema test: ALL_TABLES --> TEST_MISSING_COLUMNS +++ Test that tables and views are not missing any required columns
Starting schema test: TEST_DATABASE_VERSION  Test that the database server version number is supported for upgrade
INFO   Database product version: Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
        With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options
Completed schema test: TEST_DATABASE_VERSION --> Test that the database server version number is supported for upgrade +++ PASS
Completed schema test: ALL_TABLES --> TEST_DATABASE_VERSION +++ Test that the database server version number is supported for upgrade
Finished readiness check of Common Infrastructure Services with status: SUCCESS.

Oracle JRF
Starting readiness check of Oracle JRF.
Finished readiness check of Oracle JRF with status: SUCCESS.

System Components Infrastructure
Starting readiness check of System Components Infrastructure.
Starting config test: TEST_SOURCE_CONFIG  Checking the source
configuration.
INFO /oracle/work/middleware_1212/user_projects/domains/jrf_domain/opmn/topology.xml was not found. No upgrade is needed.
Completed config test: TEST_SOURCE_CONFIG --> Checking the source configuration. +++ PASS
Finished readiness check of System Components Infrastructure with status: ALREADY_UPGRADED.

Common Infrastructure Services
Starting readiness check of Common Infrastructure Services.
Starting config test: CIEConfigPlugin.readiness.test This tests the readiness of the domain from CIE side.
Completed config test: CIEConfigPlugin.readiness.test --> This tests the readiness of the domain from CIE side. +++ PASS
Finished readiness check of Common Infrastructure Services with status: SUCCESS.

Finished readiness check of components.

Tuning Database Parameters for Oracle Identity Manager

Before you upgrade the schemas, you must tune the Database parameters for Oracle Identity Manager.

See Performance Tuning Guidelines and Diagnostics Collection for Oracle Identity Manager (OIM) (Doc ID 1539554.1).

Upgrading Product Schemas

After stopping servers and processes, use the Upgrade Assistant to upgrade supported product schemas to the current release of Oracle Fusion Middleware.

The Upgrade Assistant allows you to upgrade individually selected schemas or all schemas associated with a domain. The option you select determines which Upgrade Assistant screens you will use.

- **Identifying Existing Schemas Available for Upgrade**
  This optional task enables you to review the list of available schemas before you begin the upgrade by querying the schema version registry. The registry contains schema information such as version number, component name and ID, date of creation and modification, and custom prefix.

- **Starting the Upgrade Assistant**
  Run the Upgrade Assistant to upgrade product schemas, domain component configurations, or standalone system components to 12c (12.2.1.4.0).

- **Upgrading Oracle Identity Manager Schemas Using the Upgrade Assistant**
  Navigate through the screens in the Upgrade Assistant to upgrade the product schemas.

- **Verifying the Schema Upgrade**
  After completing all the upgrade steps, verify that the upgrade was successful by checking that the schema version in schema_version_registry has been properly updated.
Identifying Existing Schemas Available for Upgrade

This optional task enables you to review the list of available schemas before you begin the upgrade by querying the schema version registry. The registry contains schema information such as version number, component name and ID, date of creation and modification, and custom prefix.

You can let the Upgrade Assistant upgrade all of the schemas in the domain, or you can select individual schemas to upgrade. To help decide, follow these steps to view a list of all the schemas that are available for an upgrade:

1. If you are using an Oracle database, connect to the database by using an account that has Oracle DBA privileges, and run the following from SQL*Plus:

   ```sql
   SET LINE 120
   COLUMN MRC_NAME FORMAT A14
   COLUMN COMP_ID FORMAT A20
   COLUMN VERSION FORMAT A12
   COLUMN STATUS FORMAT A9
   COLUMN UPGRADED FORMAT A8
   SELECT MRC_NAME, COMP_ID, OWNER, VERSION, STATUS, UPGRADED FROM SCHEMA_VERSION_REGISTRY ORDER BY MRC_NAME, COMP_ID;
   ```

2. Examine the report that is generated.

   If an upgrade is not needed for a schema, the `SCHEMA_VERSION_REGISTRY` table retains the schema at its pre-upgrade version.

3. Note the schema prefix name that was used for your existing schemas. You will use the same prefix when you create new 12c (12.2.1.4.0) schemas.

**Notes:**

- If your existing schemas are not from a supported version, then you must upgrade them to a supported version before using the 12c (12.2.1.4.0) upgrade procedures. Refer to your pre-upgrade version documentation for more information.

- Some components, such as Oracle Enterprise Data Quality, Oracle GoldenGate Monitor, and Oracle GoldenGate Veridata, support an upgrade from versions other than the standard Oracle Fusion Middleware supported versions.

- If you used an OID-based policy store in the earlier versions, make sure to create a new OPSS schema before you perform the upgrade. After the upgrade, the OPSS schema remains an LDAP-based store.

- You can only upgrade schemas for products that are available for upgrade in Oracle Fusion Middleware release 12c (12.2.1.4.0). Do not attempt to upgrade a domain that includes components that are not yet available for upgrade to 12c (12.2.1.4.0).
Starting the Upgrade Assistant

Run the Upgrade Assistant to upgrade product schemas, domain component configurations, or standalone system components to 12c (12.2.1.4.0).

To start the Upgrade Assistant:

**Note:**

Before you start the Upgrade Assistant, make sure that the JVM character encoding is set to UTF-8 for the platform on which the Upgrade Assistant is running. If the character encoding is not set to UTF-8, then you will not be able to download files containing Unicode characters in their names. This can cause the upgrade to fail.

To ensure that UTF-8 is used by the JVM, use the JVM option `-Dfile.encoding=UTF-8`.

1. Go to the oracle_common/upgrade/bin directory:
   - (UNIX) `ORACLE_HOME/oracle_common/upgrade/bin`
   - (Windows) `ORACLE_HOME\oracle_common\upgrade\bin`

2. Start the Upgrade Assistant:
   - (UNIX) `./ua`
   - (Windows) `ua.bat`

For information about other parameters that you can specify on the command line, such as logging parameters, see:

### Upgrading Oracle Identity Manager Schemas Using the Upgrade Assistant

Navigate through the screens in the Upgrade Assistant to upgrade the product schemas.

To upgrade product schemas with the Upgrade Assistant:

1. On the Welcome screen, review an introduction to the Upgrade Assistant and information about important pre-upgrade tasks. Click **Next**.

   **Note:**

   For more information about any Upgrade Assistant screen, click **Help** on the screen.

2. On the Selected Schemas screen, select the schema upgrade operation that you want to perform:
• **Individually Selected Schemas** if you want to select individual schemas for upgrade and you do not want to upgrade all of the schemas used by the domain.

[Caution:]

Upgrade only those schemas that are used to support your 12c (12.2.1.4.0) components. Do not upgrade schemas that are currently being used to support components that are not included in Oracle Fusion Middleware 12c (12.2.1.4.0).

• **All Schemas Used by a Domain** to allow the Upgrade Assistant to discover and select all components that have a schema available to upgrade in the domain specified in the Domain Directory field. This is also known as a domain assisted schema upgrade. Additionally, the Upgrade Assistant pre-populates connection information on the schema input screens.

[Note:]

Oracle recommends that you select **All Schemas Used by a Domain** for most upgrades to ensure all of the required schemas are included in the upgrade.

[Note:]

If you are upgrading SSL enabled Oracle Identity Manager setup, select **Individually Selected Schemas** option, and then select Oracle Identity Manager schema only. This automatically selects the dependant schemas. For upgrading SSL enabled setup, you must provide the non-SSL Database connection details on the Schema Credentials screen.

Click **Next**.

3. If you selected **Individually Selected Schemas**: On the Available Components screen, select the components for which you want to upgrade schemas. When you select a component, the schemas and any dependencies are automatically selected.

[Note:]

• For the individual schema option, the domain configuration is not accessed, and therefore password values are carried forward from the previous screen. If you encounter any connection failure, check the cause and fix it.

• For the Upgrade Assistant utility to use the correct UMS schema, manually edit the UMS schema by adding _UMS as a suffix. For example, edit **DEV** to **DEV_UMS** for successful SOA upgrade.
4. On the Screen name, select the domain folder.

5. On the Prerequisites screen, acknowledge that the prerequisites have been met by selecting all the check boxes. Click Next.

**Note:**
The Upgrade Assistant does not verify whether the prerequisites have been met.

6. On the Schema Credentials screen(s), specify the database connection details for each schema you are upgrading (the screen name changes based on the schema selected):
   - Select the database type from the **Database Type** drop-down menu.
   - Enter the database connection details, and click **Connect**.
   - Select the schema you want to upgrade from the **Schema User Name** drop-down menu, and then enter the password for the schema. Be sure to use the correct schema prefix for the schemas you are upgrading.

7. On the Examine screen, review the status of the Upgrade Assistant as it examines each schema, verifying that the schema is ready for upgrade. If the status is **Examine finished**, click Next.

   If the examine phase fails, Oracle recommends that you cancel the upgrade by clicking **No** in the Examination Failure dialog. Click **View Log** to see what caused the error and refer to Troubleshooting Your Upgrade in Upgrading with the Upgrade Assistant for information on resolving common upgrade errors.

**Note:**
- If you resolve any issues detected during the examine phase without proceeding with the upgrade, you can start the Upgrade Assistant again without restoring from backup. However, if you proceed by clicking **Yes** in the Examination Failure dialog box, you need to restore your pre-upgrade environment from backup before starting the Upgrade Assistant again.
- Canceling the examination process has no effect on the schemas or configuration data; the only consequence is that the information the Upgrade Assistant has collected must be collected again in a future upgrade session.

8. On the Upgrade Summary screen, review the summary of the options you have selected for schema upgrade.

   Verify that the correct Source and Target Versions are listed for each schema you intend to upgrade.

   If you want to save these options to a response file to run the Upgrade Assistant again later in response (or silent) mode, click **Save Response File** and provide the location and name of the response file. A silent upgrade performs exactly the same function that the Upgrade Assistant performs, but you do not have to manually enter the data again.
Click **Upgrade** to start the upgrade process.

9. On the Upgrade Progress screen, monitor the status of the upgrade.

⚠️ **Caution:**

Allow the Upgrade Assistant enough time to perform the upgrade. Do not cancel the upgrade operation unless absolutely necessary. Doing so may result in an unstable environment.

If any schemas are not upgraded successfully, refer to the Upgrade Assistant log files for more information.

💡 **Note:**

The progress bar on this screen displays the progress of the current upgrade procedure. It does not indicate the time remaining for the upgrade.

Click **Next**.

10. If the upgrade is successful: On the Upgrade Success screen, click **Close** to complete the upgrade and close the wizard.

If the upgrade fails: On the Upgrade Failure screen, click **View Log** to view and troubleshoot the errors. The logs are available at `ORACLE_HOME/oracle_common/upgrade/logs`.

💡 **Note:**

If the upgrade fails, you must restore your pre-upgrade environment from backup, fix the issues, then restart the Upgrade Assistant.

### Verifying the Schema Upgrade

After completing all the upgrade steps, verify that the upgrade was successful by checking that the schema version in `schema_version_registry` has been properly updated.

If you are using an Oracle database, connect to the database as a user having Oracle DBA privileges, and run the following from SQL*Plus to get the current version numbers:

```
SET LINE 120
COLUMN MRC_NAME FORMAT A14
COLUMN COMP_ID FORMAT A20
COLUMN VERSION FORMAT A12
COLUMN STATUS FORMAT A9
COLUMN UPGRADED FORMAT A8
SELECT MRC_NAME, COMP_ID, OWNER, VERSION, STATUS, UPGRADED FROM
SCHEMA_VERSION_REGISTRY ORDER BY MRC_NAME, COMP_ID ;
```
In the query result:

- Check that the number in the VERSION column matches the latest version number for that schema. For example, verify that the schema version number is 12.2.1.4.0.

**Note:**

However, not all schema versions will be updated. Some schemas do not require an upgrade to this release and will retain their pre-upgrade version number.

- The STATUS field will be either UPGRADING or UPGRADED during the schema patching operation, and will become VALID when the operation is completed.
- If the status appears as INVALID, the schema update failed. You should examine the logs files to determine the reason for the failure.
- Synonym objects owned by IAU_APPEND and IAU_VIEWER will appear as INVALID, but that does not indicate a failure. They become invalid because the target object changes after the creation of the synonym. The synonyms objects will become valid when they are accessed. You can safely ignore these INVALID objects.

**Tuning Application Module for User Interface**

After you upgrade the Oracle Identity Manager middle tier successfully, tune the Application Module (AM) for user interface.

See Tuning Application Module (AM) for User Interface in *Oracle Fusion Middleware Tuning Performance*.

**Upgrading Domain Component Configurations**

Use the Upgrade Assistant to upgrade the domain component configurations inside the domain to match the updated domain configuration.

- **Starting the Upgrade Assistant**
  Run the Upgrade Assistant to upgrade product schemas, domain component configurations, or standalone system components to 12c (12.2.1.4.0).

- **Upgrading Oracle Identity Manager Domain Component Configurations**
  Navigate through the screens in the Upgrade Assistant to upgrade component configurations in the WebLogic domain.

- **Verifying the Domain-Specific-Component Configurations Upgrade**
  To verify that the domain-specific-component configurations upgrade was successful, sign in to the Administration console and the Oracle Enterprise Manager Fusion Middleware Control and verify that the version numbers for each component is 12.2.1.4.0.
Starting the Upgrade Assistant

Run the Upgrade Assistant to upgrade product schemas, domain component configurations, or standalone system components to 12c (12.2.1.4.0).

To start the Upgrade Assistant:

**Note:**

Before you start the Upgrade Assistant, make sure that the JVM character encoding is set to UTF-8 for the platform on which the Upgrade Assistant is running. If the character encoding is not set to UTF-8, then you will not be able to download files containing Unicode characters in their names. This can cause the upgrade to fail.

To ensure that UTF-8 is used by the JVM, use the JVM option `-Dfile.encoding=UTF-8`.

1. Go to the `oracle_common/upgrade/bin` directory:
   - (UNIX) `ORACLE_HOME/oracle_common/upgrade/bin`
   - (Windows) `ORACLE_HOME\oracle_common\upgrade\bin`

2. Start the Upgrade Assistant:
   - (UNIX) `./ua`
   - (Windows) `ua.bat`

   For information about other parameters that you can specify on the command line, such as logging parameters, see:

   - Upgrade Assistant Parameters

### Upgrade Assistant Parameters

When you start the Upgrade Assistant from the command line, you can specify additional parameters.

| Table 4-7    Upgrade Assistant Command-Line Parameters |
|-------------|-----------------------------------------------|
| Parameter   | Required or Optional | Description                                                  |
| -readiness  | Required for readiness checks                  | Performs the upgrade readiness check without performing an actual upgrade. Schemas and configurations are checked. Do not use this parameter if you have specified the -examine parameter. |
| Note:       | Readiness checks cannot be performed on standalone installations (those not managed by the WebLogic Server). | |

---

**Chapter 4**

Upgrading Domain Component Configurations

4-33
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-threads</td>
<td>Optional</td>
<td>Identifies the number of threads available for concurrent schema upgrades or readiness checks of the schemas. The value must be a positive integer in the range 1 to 8. The default is 4.</td>
</tr>
<tr>
<td>-response</td>
<td>Required for silent upgrades or silent readiness checks</td>
<td>Runs the Upgrade Assistant using inputs saved to a response file generated from the data that is entered when the Upgrade Assistant is run in GUI mode. Using this parameter runs the Upgrade Assistant in silent mode (without displaying Upgrade Assistant screens).</td>
</tr>
<tr>
<td>-examine</td>
<td>Optional</td>
<td>Performs the examine phase but does not perform an actual upgrade. Do not specify this parameter if you have specified the -readiness parameter.</td>
</tr>
<tr>
<td>-logLevel attribute</td>
<td>Optional</td>
<td>Sets the logging level, specifying one of the following attributes: • TRACE • NOTIFICATION • WARNING • ERROR • INCIDENT_ERROR The default logging level is NOTIFICATION. Consider setting the -logLevel TRACE attribute to so that more information is logged. This is useful when troubleshooting a failed upgrade. The Upgrade Assistant's log files can become very large if -logLevel TRACE is used.</td>
</tr>
</tbody>
</table>
Table 4-7  (Cont.) Upgrade Assistant Command-Line Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
</table>
| -logDir location | Optional | Sets the default location of upgrade log files and temporary files. You must specify an existing, writable directory where the Upgrade Assistant creates log files and temporary files. The default locations are: (UNIX) 
ORACLE_HOME/oracle_common/upgrade/logs 
ORACLE_HOME/oracle_common/upgrade/temp (Windows) 
ORACLE_HOME/oracle_common\upgrade\logs 
ORACLE_HOME/oracle_common\upgrade\temp |

- help | Optional | Displays all of the command-line options. |

Upgrading Oracle Identity Manager Domain Component Configurations

Navigate through the screens in the Upgrade Assistant to upgrade component configurations in the WebLogic domain.

Run the Upgrade Assistant to upgrade the domain component configurations to match the updated domain configuration.

To upgrade domain component configurations with the Upgrade Assistant:

1. On the Welcome screen, review an introduction to the Upgrade Assistant and information about important pre-upgrade tasks. Click Next.

   Note:
   For more information about any Upgrade Assistant screen, click Help on the screen.

2. On the next screen:
• Select **All Configurations Used By a Domain**. The screen name changes to WebLogic Components.

• In the **Domain Directory** field, specify the OIM domain directory. Click **Next**.

3. If your pre-upgrade environment has multiple WebLogic domains, but the Oracle Web Services Manager (OWSM) Policy Manager is in only one domain, and OWSM agents are in the other domains: On the OWSM Policy Manager screen, provide the credentials for the WebLogic Administration Server domain where the Oracle Web Services Manager (OWSM) Policy Manager is deployed.

4. On the Component List screen, verify that the list includes all the components for which you want to upgrade configurations and click **Next**.

If you do not see the components you want to upgrade, click **Back** to go to the previous screen and specify a different domain.

5. On the Prerequisites screen, acknowledge that the prerequisites have been met by selecting all the check boxes. Click **Next**.

<table>
<thead>
<tr>
<th><strong>Note:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The Upgrade Assistant does not verify whether the prerequisites have been met.</td>
</tr>
</tbody>
</table>

6. If there are remote managed servers hosting User Messaging Services (UMS) configuration files: On the UMS Configuration screen, provide the credentials to these servers so that the Upgrade Assistant can access the configuration files.

<table>
<thead>
<tr>
<th><strong>Note:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>You may need to manually copy the UMS configuration files if the Upgrade Assistant is unable to locate them. See Error while Copying User Messaging Service (UMS) Configuration Files.</td>
</tr>
</tbody>
</table>

7. On the Old (i.e 12c) OIM Home Location screen, select **12c Source**, and specify the absolute path to the 12c (12.2.1.3.0) OIM Oracle Home. Click **Next**.

8. On the Examine screen, review the status of the Upgrade Assistant as it examines each component, verifying that the component configuration is ready for upgrade. If the status is **Examine finished**, click **Next**.

If the examine phase fails, Oracle recommends that you cancel the upgrade by clicking **No** in the Examination Failure dialog. Click **View Log** to see what caused the error and refer to Troubleshooting Your Upgrade in *Upgrading with the Upgrade Assistant* for information on resolving common upgrade errors.
9. On the Upgrade Summary screen, review the summary of the options you have selected for component configuration upgrade.

The response file collects and stores all the information that you have entered, and enables you to perform a silent upgrade at a later time. The silent upgrade performs exactly the same function that the Upgrade Assistant performs, but you do not have to manually enter the data again. If you want to save these options to a response file, click **Save Response File** and provide the location and name of the response file.

Click **Upgrade** to start the upgrade process.

10. On the Upgrade Progress screen, monitor the status of the upgrade.

**Caution:**

Allow the Upgrade Assistant enough time to perform the upgrade. Do not cancel the upgrade operation unless absolutely necessary. Doing so may result in an unstable environment.

If any components are not upgraded successfully, refer to the Upgrade Assistant log files for more information.

**Note:**

The progress bar on this screen displays the progress of the current upgrade procedure. It does not indicate the time remaining for the upgrade.

Click **Next**.

11. If the upgrade is successful: On the Upgrade Success screen, click **Close** to complete the upgrade and close the wizard. The Post-Upgrade Actions window describes the manual tasks you must perform to make components functional in the new installation. This window appears only if a component has post-upgrade steps.
If the upgrade fails: On the Upgrade Failure screen, click **View Log** to view and troubleshoot the errors. The logs are available at `ORACLE_HOME/oracle_common/upgrade/logs`.

**Note:**

If the upgrade fails you must restore your pre-upgrade environment from backup, fix the issues, then restart the Upgrade Assistant.

### Verifying the Domain-Specific-Component Configurations Upgrade

To verify that the domain-specific-component configurations upgrade was successful, sign in to the Administration console and the Oracle Enterprise Manager Fusion Middleware Control and verify that the version numbers for each component is `12.2.1.4.0`.

To sign in to the Administration Console, go to: `http://administration_server_host:administration_server_port/console`

To sign in to Oracle Enterprise Manager Fusion Middleware Control Console, go to: `http://administration_server_host:administration_server_port/em`

**Note:**

After upgrade, make sure you run the administration tools from the new 12c (12.2.1.4.0) Oracle home directory and not from the previous Oracle home directory.

During the upgrade process, some OWSM documents, including policy sets and predefined documents such as policies and assertion templates, may need to be upgraded. If a policy set or a predefined document is upgraded, its version number is incremented by 1.

If you created the FMW user to run the Upgrade Assistant, ensure that you delete the account after verifying your upgrade was successful.

### Copying `oracle.iam.ui.custom-dev-starter-pack.war` from 12c Middleware Home

You have to manually copy the `oracle.iam.ui.custom-dev-starter-pack.war` file from backup of 12c (12.2.1.3.0) Middleware Home to 12c (12.2.1.4.0) Middleware home: `ORACLE_HOME/idm/server/apps/`. 
Post-Upgrade Task

If you had set custom configuration in your 12c (12.2.1.3.0) Middleware home, you need to copy the custom configuration present in your 12c (12.2.1.3.0) Middleware home to the 12c (12.2.1.4.0) Middleware home.

- If you have scheduled jobs with parameters referring to the 12c (12.2.1.3.0) Middleware home, then you need to update them to the corresponding 12c (12.2.1.4.0) Middleware home.
- To preserve customized configuration data (if present), copy the contents from standard directories such as XLIntegrations and connectorResources under the 12c (12.2.1.3.0) Middleware home to the corresponding directories under the 12c (12.2.1.4.0) Middleware home.

Starting the Servers

After you upgrade Oracle Identity Manager, start the servers.

You must start the servers in the following order:

1. Start the Administration Server.
2. Start the Oracle SOA Suite Managed Server with the Administration Server URL. For example:

   ./startManagedWebLogic.sh soa_server1 t3://weblogic_admin_host:weblogic_admin_port

3. Once the SOA server is in running state, start the Oracle Identity Manager Managed Server with the Administration Server URL.

   After the upgrade, when the OIM server starts for the first time, the 12c (12.2.1.4.0) bootstrap starts automatically and the server will not shut down.

   For more information about stopping the servers and processes, see Stopping Servers and Processes.

Upgrading Oracle Identity Manager Design Console

Upgrade the Oracle Identity Manager Design Console after you upgrade the Oracle Identity Manager (OIM) domain component configurations.

To upgrade the Oracle Identity Manager Design Console, complete the following steps:

1. Replace the 12c (12.2.1.3.0) designconsole/config/xlconfig.xml with the 12c (12.2.1.4.0) designconsole/config/xlconfig.xml file.
2. If the host name and the port of the OIM Managed Server has changed, update the URL in the Design Console’s start window accordingly.
Completing the Post-Upgrade Tasks for SSL Enabled Setup

If you are upgrading Oracle Identity Manager SSL enabled setup, you must perform the required post-upgrade tasks to complete the upgrade process.

Complete the following tasks if you have upgraded an SSL enabled setup:

1. Changes done for SSL settings in setDomainEnv.sh, startWeblogic.sh, startManagedWeblogic.sh, and datasources are lost after upgrade. Re-do all of the changes.

2. Start the WebLogic Administration Server. To start the Administration Server, use the startWebLogic script:
   - (UNIX) $EXISTING_DOMAIN_HOME/bin/startWebLogic.sh
   - (Windows) $EXISTING_DOMAIN_HOME\bin\startWebLogic.cmd
   When prompted, enter your user name, password, and the URL of the Administration Server.

3. Make necessary changes to the following newly created datasources, for SSL settings:
   - LocalSvcTblDataSource
   - opss-audit-DBDS
   - opss-audit-viewDS
   - opss-data-source
   - WLSSchemaDataSource

4. In case of Customer Identity and Java Standard Trust, import your identity trust certificate to the new JDK home. The 12c (12.2.1.4.0) uses jdk1.8.0_211. To import the identity trust certificate to the new JDK home, use the following command:

   ```
   ./
   keytool -importcert -alias startssl -keystore $JAVA_HOME/jre/lib/security/cacerts -storepass changeit -file supportcert.pem
   ```

5. Verify that all of the SSL configuration changes including the SSL port related changes done in 12c (pre upgrade), are present post upgrade. If the changes are lost, you must redo them post upgrade. Some of the SSL configuration changes include:
   - OimFrontEndURL
   - backOfficeURL
   - SOA Server URL
   - ForeignJNDIProvider-SOA

For more information about configuring SSL for Oracle Identity Governance, see Updating Oracle Identity Governance in Administering Oracle Identity Governance.

Installing Standalone Oracle BI Publisher

When you upgrade Oracle Identity Manager 11g (11.1.2.3.0) to Oracle Identity Governance 12c (12.2.1.3.0), the embedded Oracle BI Publisher present in the 11g
(11.1.2.3.0) deployment is removed. Therefore, post upgrade, you must install a new standalone Oracle BI Publisher 12c (12.2.1.3.0), for configuring the Oracle Identity Governance reports. Same BIP can be used after 12c (12.2.1.3.0) to 12c (12.2.1.4.0) upgrade.

For information about installing and configuring Oracle BI Publisher 12c (12.2.1.4.0), see Installing and Configuring Oracle BI Publisher in Developing and Customizing Applications for Oracle Identity Governance.

For information about integrating standalone Oracle BI Publisher with Oracle Identity Governance 12c (12.2.1.4.0), see Integrating Standalone BI Publisher with Oracle Identity Governance in Developing and Customizing Applications for Oracle Identity Governance.
You can upgrade Oracle Identity and Access Management highly available 12c (12.2.1.3.0) environments to 12c (12.2.1.4.0) using the procedure described in this part.

**Topics**

- **Upgrading Oracle Access Management Highly Available Environments**
  Describes the process of upgrading an Oracle Access Management highly available environments from 12c (12.2.1.3.0) to 12c (12.2.1.4.0).

- **Upgrading Oracle Identity Manager Highly Available Environments**
  Describes the process of upgrading an Oracle Identity Manager highly available environment from 12c (12.2.1.3.0) to Oracle Identity Governance 12c (12.2.1.4.0).

- **Upgrading Oracle Access Management Multi-Data Center Environments**
  You can upgrade Oracle Access Management deployed across multi-data centers (MDC) from 12c (12.2.1.3.0) to 12c (12.2.1.4.0).
Upgrading Oracle Access Management Highly Available Environments

Describes the process of upgrading an Oracle Access Management highly available environments from 12c (12.2.1.3.0) to 12c (12.2.1.4.0).

Topics

- **About the Oracle Access Management Multinode Upgrade Process**
  Review the topology and the roadmap for an overview of the upgrade process for Oracle Access Management highly available environments.

- **Backing up the 12c (12.2.1.3.0) Middleware Home Folder on OAMHOSTs**
  Backup the 12c (12.2.1.3.0) Middleware Home on both OAMHOST1 and OAMHOST2.

- **Uninstalling the Software on an OAMHOST**
  Follow the instructions in this section to start the Uninstall Wizard and remove the software.

- **Installing Product Distributions on OAMHOSTs**
  Install the binaries on an OAMHOST.

- **Running a Pre-Upgrade Readiness Check**
  To identify potential issues with the upgrade, Oracle recommends that you run a readiness check before you start the upgrade process. Be aware that the readiness check may not be able to discover all potential issues with your upgrade. An upgrade may still fail, even if the readiness check reports success.

- **Starting the Servers on OAMHOSTs**
  After you upgrade Oracle Access Management on an OAMHOST, start the servers.

- **Enabling WebGates to Work With Oracle Access Management**
  After upgrading to Oracle Access Management 12c (12.2.1.4.0), the earlier version of WebGates continues to work with Oracle Access Management. However, to leverage the latest security features of Oracle Access Management and WebGates 12c (12.2.1.4.0), you must upgrade the WebGates to 12c (12.2.1.4.0), and register the agent's profile with the Oracle Access Management Server.

**About the Oracle Access Management Multinode Upgrade Process**

Review the topology and the roadmap for an overview of the upgrade process for Oracle Access Management highly available environments.

The steps you take to upgrade your existing domain will vary depending on how your domain is configured and which components are being upgraded. Follow only those steps that are applicable to your deployment.
Upgrade Topology

The following topology shows the Oracle Access Management cluster set up that can be upgraded to 12c (12.2.1.4.0) by following the procedure described in this chapter.

Figure 5-1  Oracle Access Management High Availability Upgrade Topology

On OAMHOST1, the following installations have been performed:

- An Oracle Access Management Access Manager instance has been installed in the WLS_OAM1 Managed Server.
- A WebLogic Server Administration Server has been installed. Under normal operations, this is the active Administration Server.

On OAMHOST2, the following installations have been performed:

- An Oracle Access Management Access Manager instance has been installed in the WLS_OAM2 Managed Server.
- A WebLogic Server Administration Server has been installed. Under normal operations, this is the passive Administration Server. You make this Administration Server active if the Administration Server on OAMHOST1 becomes unavailable.

The instances in the WLS_OAM1 and WLS_OAM2 Managed Servers on OAMHOST1 and OAMHOST2 are configured in a cluster named OAM_CLUSTER.

Table 5-1  Tasks for Upgrading Oracle Access Management Highly Available Environments

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required</td>
<td>If you have not done so already, review the introductory topics in this guide and complete the required pre-upgrade tasks. See:</td>
</tr>
<tr>
<td></td>
<td>• Introduction to Upgrading Oracle Identity and Access Management to 12c (12.2.1.4.0)</td>
</tr>
<tr>
<td></td>
<td>• Pre-Upgrade Requirements</td>
</tr>
<tr>
<td>Required</td>
<td>Create backup of the existing 12c (12.2.1.3.0) Middleware home folders on OAMHOSTs See Backing up the 12c (12.2.1.3.0) Middleware Home Folder on OAMHOSTs.</td>
</tr>
</tbody>
</table>
Table 5-1 (Cont.) Tasks for Upgrading Oracle Access Management Highly Available Environments

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required on OAMHOST1</strong>&lt;br&gt;Shut down the 12c environment (stop all Administration and Managed Servers) on OAMHOST1. Ensure that the Database is up during the upgrade.</td>
<td><strong>WARNING</strong>: Failure to shut down your servers during an upgrade may lead to data corruption. See <em>Stopping Servers and Processes</em>.</td>
</tr>
<tr>
<td><strong>Required on OAMHOST1</strong>&lt;br&gt;On OAMHOST1, uninstall Oracle Fusion Middleware Infrastructure and Oracle Identity and Access Management 12c (12.2.1.3.0) in the existing Oracle home.</td>
<td>See <em>Uninstalling the Software on an OAMHOST</em>.</td>
</tr>
<tr>
<td><strong>Required on OAMHOST1</strong>&lt;br&gt;On OAMHOST1, install Infrastructure (JRF) 12c (12.2.1.4.0), Oracle SOA Suite12c (12.2.1.4.0) and Oracle Identity and Access Management 12c (12.2.1.4.0) in the existing Oracle home.</td>
<td>See <em>Installing Product Distributions on OAMHOSTs</em>.</td>
</tr>
<tr>
<td><strong>Optional</strong>&lt;br&gt;Run a pre-upgrade readiness check</td>
<td>See <em>Running a Pre-Upgrade Readiness Check</em>.</td>
</tr>
<tr>
<td><strong>Required on OAMHOST1</strong>&lt;br&gt;Start the servers on OAMHOST1.</td>
<td>See <em>Starting the Servers</em>.</td>
</tr>
<tr>
<td><strong>Required on OAMHOST2</strong>&lt;br&gt;Shut down the 12c environment (stop all Managed Servers) on OAMHOST2. Ensure that the Database is up during the upgrade.</td>
<td><strong>WARNING</strong>: Failure to shut down your servers during an upgrade may lead to data corruption. See <em>Stopping Servers and Processes</em>.</td>
</tr>
<tr>
<td><strong>Required on OAMHOST2</strong>&lt;br&gt;On OAMHOST2, uninstall Oracle Fusion Middleware Infrastructure and Oracle Identity and Access Management 12c (12.2.1.3.0) in the existing Oracle home.</td>
<td>See <em>Uninstalling the Software on an OAMHOST</em>.</td>
</tr>
<tr>
<td><strong>Required on OAMHOST2</strong>&lt;br&gt;On OAMHOST2, install Infrastructure (JRF) 12c (12.2.1.4.0), Oracle SOA Suite12c (12.2.1.4.0) and Oracle Identity and Access Management 12c (12.2.1.4.0) in the existing Oracle home.</td>
<td>See <em>Installing Product Distributions on OAMHOSTs</em>.</td>
</tr>
<tr>
<td><strong>Required on OAMHOST2</strong>&lt;br&gt;Start the node manager and managed servers on OAMHOST2.</td>
<td>See <em>Starting the Servers</em>.</td>
</tr>
</tbody>
</table>
| **Required on OAMHOST2**<br>Complete any necessary post-upgrade tasks. | This is optional. Perform the following tasks based on your deployment:  
  • *Enabling WebGates to Work With Oracle Access Management* |
Backing up the 12c (12.2.1.3.0) Middleware Home Folder on OAMHOSTs

Backup the 12c (12.2.1.3.0) Middleware Home on both OAMHOST1 and OAMHOST2.

As a backup, copy and rename the 12.2.1.3.0 Middleware home folder on OAMHOST1 and OAMHOST2.

For example:

From /scratch/work/u01/mw12c to /scratch/work/u01/mw12c_old

Uninstalling the Software on an OAMHOST

Follow the instructions in this section to start the Uninstall Wizard and remove the software.

If you want to uninstall the product in a silent (command-line) mode, see Running the Oracle Universal Installer for Silent Uninstallation in Installing Software with the Oracle Universal Installer.

• Starting the Uninstall Wizard
• Selecting the Product to Uninstall
• Navigating the Uninstall Wizard Screens

Starting the Uninstall Wizard

Start the Uninstall Wizard:

1. Change to the following directory:
   (UNIX) ORACLE_HOME/oui/bin
   (Windows) ORACLE_HOME\oui\bin

2. Enter the following command:
   (UNIX) ./deinstall.sh
   (Windows) deinstall.cmd

Selecting the Product to Uninstall

Because multiple products exist in the Oracle home, ensure that you are uninstalling the correct product.

After you run the Uninstall Wizard, the Distribution to Uninstall screen opens.

• For OAM or OIM only install: Click Uninstall.
• For OAM or OIM installed with other products: From the dropdown menu, select the Oracle Identity and Access Management 12.2.1.3.0 product and click Uninstall.

The uninstallation program shows the screens listed in Navigating the Uninstall Wizard Screens.
Run the Uninstall Wizard again to uninstall the Oracle Fusion Middleware Infrastructure. For instructions see, Uninstalling Oracle Fusion Middleware Infrastructure in Installing and Configuring the Oracle Fusion Middleware Infrastructure.

Navigating the Uninstall Wizard Screens

The Uninstall Wizard shows a series of screens to confirm the removal of the software.

If you need help on screen listed in the following table, click Help on the screen.

**Table 5-2   Uninstall Wizard Screens and Descriptions**

<table>
<thead>
<tr>
<th>Screen</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome</td>
<td>Introduces you to the product Uninstall Wizard.</td>
</tr>
<tr>
<td>Uninstall Summary</td>
<td>Shows the Oracle home directory and its contents that are uninstalled. Verify that this is the correct directory. If you want to save these options to a response file, click Save Response File and enter the response file location and name. You can use the response file later to uninstall the product in silent (command-line) mode. See Running the Oracle Universal Installer for Silent Uninstall in Installing Software with the Oracle Universal Installer. Click Deinstall, to begin removing the software.</td>
</tr>
<tr>
<td>Uninstall Progress</td>
<td>Shows the uninstallation progress.</td>
</tr>
<tr>
<td>Uninstall Complete</td>
<td>Appears when the uninstallation is complete. Review the information on this screen, then click Finish to close the Uninstall Wizard.</td>
</tr>
</tbody>
</table>

**Note:**

After the product is uninstalled, ensure that the ORACLE_HOME folder exists and it does not contain any files or folders. If there are any remaining files or folders in the ORACLE_HOME folder, delete them.

Installing Product Distributions on OAMHOSTs

Install the binaries on an OAMHOST.

Complete the following steps:

1. After uninstalling the 12c (12.2.1.3.0) product on an OAMHOST, install the following products on the OAMHOST.
   - Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0)
   - Oracle Identity and Access Management 12c (12.2.1.4.0)
   - Any additional distributions for your pre-upgrade environment

For more information, see Installing Product Distributions.
Running a Pre-Upgrade Readiness Check

To identify potential issues with the upgrade, Oracle recommends that you run a readiness check before you start the upgrade process. Be aware that the readiness check may not be able to discover all potential issues with your upgrade. An upgrade may still fail, even if the readiness check reports success.

- **About Running a Pre-Upgrade Readiness Check**
  You can run the Upgrade Assistant in `readiness` mode to detect issues before you perform the actual upgrade. You can run the readiness check in GUI mode using the Upgrade Assistant or in silent mode using a response file.

- **Starting the Upgrade Assistant in Readiness Mode**
  Use the `-readiness` parameter to start the Upgrade Assistant in readiness mode.

- **Performing a Readiness Check with the Upgrade Assistant**
  Navigate through the screens in the Upgrade Assistant to complete the pre-upgrade readiness check.

- **Understanding the Readiness Report**
  After performing a readiness check for your domain, review the report to determine whether you need to take any action for a successful upgrade.

**About Running a Pre-Upgrade Readiness Check**

You can run the Upgrade Assistant in `readiness` mode to detect issues before you perform the actual upgrade. You can run the readiness check in GUI mode using the Upgrade Assistant or in silent mode using a response file.

The Upgrade Assistant readiness check performs a read-only, pre-upgrade review of your Fusion Middleware schemas and WebLogic domain configurations that are at a supported starting point. The review is a read-only operation.

The readiness check generates a formatted, time-stamped readiness report so you can address potential issues before you attempt the actual upgrade. If no issues are detected, you can begin the upgrade process. Oracle recommends that you read this report thoroughly before performing an upgrade.

You can run the readiness check while your existing Oracle Fusion Middleware domain is online (while other users are actively using it) or offline.

You can run the readiness check any number of times before performing any actual upgrade. However, do not run the readiness check after an upgrade has been performed, as the report results may differ from the result of pre-upgrade readiness checks.
Starting the Upgrade Assistant in Readiness Mode

Use the -readiness parameter to start the Upgrade Assistant in readiness mode.

To perform a readiness check on your pre-upgrade environment with the Upgrade Assistant:

1. Go to the oracle_common/upgrade/bin directory:
   - (UNIX) $ORACLE_HOME/oracle_common/upgrade/bin
   - (Windows) $ORACLE_HOME/oracle_common\upgrade\bin

2. Start the Upgrade Assistant.
   - (UNIX) ./ua -readiness
   - (Windows) ua.bat -readiness

Note:
If the DISPLAY environment variable is not set up properly to allow for GUI mode, you may encounter the following error:

```
Xlib: connection to ":1.0" refused by server
Xlib: No protocol specified
```

To resolve this issue, set the DISPLAY environment variable to the system name or IP address of your local workstation, and rerun Upgrade Assistant.

If you continue to receive these errors after setting DISPLAY, try launching another GUI tool, such as vncconfig. If you see the same errors, your DISPLAY environment variable may still not be set correctly.

For information about other parameters that you can specify on the command line, see:

- Upgrade Assistant Parameters

Upgrade Assistant Parameters

When you start the Upgrade Assistant from the command line, you can specify additional parameters.
### Table 5-3  Upgrade Assistant Command-Line Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-readiness</code></td>
<td>Required for readiness checks</td>
<td>Performs the upgrade readiness check without performing an actual upgrade. Schemas and configurations are checked. Do not use this parameter if you have specified the <code>-examine</code> parameter. Note: Readiness checks cannot be performed on standalone installations (those not managed by the WebLogic Server).</td>
</tr>
<tr>
<td><code>-threads</code></td>
<td>Optional</td>
<td>Identifies the number of threads available for concurrent schema upgrades or readiness checks of the schemas. The value must be a positive integer in the range 1 to 8. The default is 4.</td>
</tr>
<tr>
<td><code>-response</code></td>
<td>Required for silent upgrades or silent readiness checks</td>
<td>Runs the Upgrade Assistant using inputs saved to a response file generated from the data that is entered when the Upgrade Assistant is run in GUI mode. Using this parameter runs the Upgrade Assistant in silent mode (without displaying Upgrade Assistant screens).</td>
</tr>
<tr>
<td><code>-examine</code></td>
<td>Optional</td>
<td>Performs the examine phase but does not perform an actual upgrade. Do not specify this parameter if you have specified the <code>-readiness</code> parameter.</td>
</tr>
</tbody>
</table>
| `-logLevel attribute` | Optional | Sets the logging level, specifying one of the following attributes:  
• TRACE  
• NOTIFICATION  
• WARNING  
• ERROR  
• INCIDENT_ERROR  
The default logging level is NOTIFICATION. Consider setting the `-logLevel TRACE` attribute to so that more information is logged. This is useful when troubleshooting a failed upgrade. The Upgrade Assistant's log files can become very large if `-logLevel TRACE` is used. |
### Table 5-3 (Cont.) Upgrade Assistant Command-Line Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
</table>
| `-logDir location` | Optional            | Sets the default location of upgrade log files and temporary files. You must specify an existing, writable directory where the Upgrade Assistant creates log files and temporary files. The default locations are:  
  (UNIX) 
  `ORACLE_HOME/oracle_common/upgrade/logs` 
  `ORACLE_HOME/oracle_common/upgrade/temp`  
  (Windows) 
  `ORACLE_HOME/oracle_common\upgrade\logs`  
  `ORACLE_HOME/oracle_common\upgrade\temp` |
| `-help`     | Optional             | Displays all of the command-line options.                                    |

#### Performing a Readiness Check with the Upgrade Assistant

Navigate through the screens in the Upgrade Assistant to complete the pre-upgrade readiness check.

Readiness checks are performed only on schemas or component configurations that are at a supported upgrade starting point.

To complete the readiness check:

1. On the Welcome screen, review information about the readiness check. Click **Next**.
2. On the Readiness Check Type screen, select the readiness check that you want to perform:
   - **Individually Selected Schemas** allows you to select individual schemas for review before upgrade. The readiness check reports whether a schema is supported for an upgrade or where an upgrade is needed. When you select this option, the screen name changes to Selected Schemas.
   - **Domain Based** allows the Upgrade Assistant to discover and select all upgrade-eligible schemas or component configurations in the domain specified in the **Domain Directory** field.
When you select this option, the screen name changes to Schemas and Configuration.

Leave the default selection if you want the Upgrade Assistant to check all schemas and component configurations at the same time, or select a specific option:

– Include checks for all schemas to discover and review all components that have a schema available to upgrade.

– Include checks for all configurations to review component configurations for a managed WebLogic Server domain.

Click Next.

3. If you selected Individually Selected Schemas: On the Available Components screen, select the components that have a schema available to upgrade for which you want to perform a readiness check.

If you selected Domain Based: On the Component List screen, review the list of components that are present in your domain for which you want to perform a readiness check.

If you select a component that has dependent components, those components are automatically selected. For example, if you select Oracle Platform Security Services, Oracle Audit Services is automatically selected.

Depending on the components you select, additional screens may display. For example, you may need to:

• Specify the domain directory.
  Ensure that you specify the 12c (12.2.1.3.0) domain directory.

• Specify schema credentials to connect to the selected schema: Database Type, DBA User Name, and DBA Password. Then click Connect.

  Note:
  Oracle database is the default database type. Make sure that you select the correct database type before you continue. If you discover that you selected the wrong database type, do not go back to this screen to change it to the correct type. Instead, close the Upgrade Assistant and restart the readiness check with the correct database type selected to ensure that the correct database type is applied to all schemas.

• Select the Schema User Name option and specify the Schema Password.

  Note:
  The Upgrade Assistant automatically enables default credentials. If you are unable to connect, make sure that you manually enter the credentials for your schema before you continue.

Click Next to start the readiness check.
4. On the Readiness Summary screen, review the summary of the readiness checks that will be performed based on your selections.

If you want to save your selections to a response file to run the Upgrade Assistant again later in response (or silent) mode, click **Save Response File** and provide the location and name of the response file. A silent upgrade performs exactly the same function that the Upgrade Assistant performs, but you do not have to manually enter the data again.

For a detailed report, click **View Log**.

Click **Next**.

5. On the Readiness Check screen, review the status of the readiness check. The process can take several minutes.

If you are checking multiple components, the progress of each component displays in its own progress bar in parallel.

When the readiness check is complete, click **Continue**.

The following components are marked as **ready for upgrade** although they are not upgraded. Ignore the **ready for upgrade** message against these components:

- Oracle JRF
- Common Infrastructure Services
- Oracle Web Services Manager

6. On the End of Readiness screen, review the results of the readiness check (**Readiness Success** or **Readiness Failure**):

- If the readiness check is successful, click **View Readiness Report** to review the complete report. Oracle recommends that you review the Readiness Report before you perform the actual upgrade even when the readiness check is successful. Use the **Find** option to search for a particular word or phrase within the report. The report also indicates where the completed Readiness Check Report file is located.

- If the readiness check encounters an issue or error, click **View Log** to review the log file, identify and correct the issues, and then restart the readiness check. The log file is managed by the command-line options you set.

**Understanding the Readiness Report**

After performing a readiness check for your domain, review the report to determine whether you need to take any action for a successful upgrade.

The format of the readiness report file is:

`readiness<timestamp>.txt`

Where, `timestamp` indicates the date and time of when the readiness check was run.

A readiness report contains the following information:
### Table 5-4  Readiness Report Elements

<table>
<thead>
<tr>
<th>Report Information</th>
<th>Description</th>
<th>Required Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Readiness Status: SUCCESS or FAILURE</td>
<td>The top of the report indicates whether the readiness check passed or completed with one or more errors.</td>
<td>If the report completed with one or more errors, search for FAIL and correct the failing issues before attempting to upgrade. You can re-run the readiness check as many times as necessary before an upgrade.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>The date and time that the report was generated.</td>
<td>No action required.</td>
</tr>
<tr>
<td>Log file location /oracle_common/upgrade/logs</td>
<td>The directory location of the generated log file.</td>
<td>No action required.</td>
</tr>
<tr>
<td>Domain Directory</td>
<td>Displays the domain location.</td>
<td>No action required.</td>
</tr>
<tr>
<td>Readiness report location /oracle_common/upgrade/logs</td>
<td>The directory location of the generated readiness report.</td>
<td>No action required.</td>
</tr>
<tr>
<td>Names of components that were checked</td>
<td>The names and versions of the components included in the check and status.</td>
<td>If your domain includes components that cannot be upgraded to this release, such as SOA Core Extension, do not attempt an upgrade.</td>
</tr>
<tr>
<td>Names of schemas that were checked</td>
<td>The names and current versions of the schemas included in the check and status.</td>
<td>Review the version numbers of your schemas. If your domain includes schemas that cannot be upgraded to this release, do not attempt an upgrade.</td>
</tr>
<tr>
<td>Individual Object Test Status: FAIL</td>
<td>The readiness check test detected an issue with a specific object.</td>
<td>Do not upgrade until all failed issues have been resolved.</td>
</tr>
<tr>
<td>Individual Object Test Status: PASS</td>
<td>The readiness check test detected no issues for the specific object.</td>
<td>If your readiness check report shows only the PASS status, you can upgrade your environment. Note, however, that the Readiness Check cannot detect issues with externals such as hardware or connectivity during an upgrade. You should always monitor the progress of your upgrade.</td>
</tr>
<tr>
<td>Completed Readiness Check of &lt;Object&gt; Status: FAILURE</td>
<td>The readiness check detected one or more errors that must be resolved for a particular object such as a schema, an index, or datatype.</td>
<td>Do not upgrade until all failed issues have been resolved.</td>
</tr>
<tr>
<td>Completed Readiness Check of &lt;Object&gt; Status: SUCCESS</td>
<td>The readiness check test detected no issues.</td>
<td>No action required.</td>
</tr>
</tbody>
</table>

Here is a sample Readiness Report file. Your report may not include all of these checks.

*Upgrade readiness check completed with one or more errors.*
Starting readiness check of components.

Oracle Platform Security Services

Starting readiness check of Oracle Platform Security Services.

- Schema User Name: DEV3_OPSS
- Database Type: Oracle Database
- Database Connect String:

  VERSION Schema DEV3_OPSS is currently at version 12.1.2.0.0.

Readiness checks will now be performed.

Starting schema test: TEST_DATABASE_VERSION Test that the database server version number is supported for upgrade

  INFO Database product version: Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
  With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options

  Completed schema test: TEST_DATABASE_VERSION --> Test that the database server version number is supported for upgrade +++ PASS

Starting schema test: TEST_REQUIRED_TABLES Test that the schema contains all the required tables

  Completed schema test: TEST_REQUIRED_TABLES --> Test that the schema contains all the required tables +++ PASS

Starting schema test: Test that the schema does not contain any unexpected tables TEST_UNEXPECTED_TABLES

  Completed schema test: Test that the schema does not contain any unexpected tables --> TEST_UNEXPECTED_TABLES +++ Test that the schema does not contain any unexpected tables

Starting schema test: TEST_ENOUGH_TABLESPACE Test that the schema tablespaces automatically extend if full

  Completed schema test: TEST_ENOUGH_TABLESPACE --> Test that the schema tablespaces automatically extend if full +++ PASS

Starting schema test: TEST_USER_TABLESPACE_QUOTA Test that tablespace quota for this user is sufficient to perform the upgrade

  Completed schema test: TEST_USER_TABLESPACE_QUOTA --> Test that tablespace quota for this user is sufficient to perform the upgrade +++ PASS

Starting schema test: TEST_ONLINE_TABLESPACE Test that schema tablespaces are online

  Completed schema test: TEST_ONLINE_TABLESPACE --> Test that schema tablespaces are online +++ PASS

Starting permissions test: TEST_DBA_TABLE_GRANTS Test that DBA user has privilege to view all user tables

  Completed permissions test: TEST_DBA_TABLE_GRANTS --> Test that DBA user has privilege to view all user tables +++ PASS

Starting schema test: SEQUENCE_TEST Test that the Oracle Platform Security Services schema sequence and its properties are valid

  Completed schema test: SEQUENCE_TEST --> Test that the Oracle Platform Security Services schema sequence and its properties are valid +++ PASS
Finished readiness check of Oracle Platform Security Services with status: SUCCESS.

Oracle Audit Services
Starting readiness check of Oracle Audit Services.
  Schema User Name: DEV3_IAU
  Database Type: Oracle Database
  Database Connect String:
  VERSION Schema DEV3_IAU is currently at version 12.1.2.0.0.

Readiness checks will now be performed.
Starting schema test:  TEST_DATABASE_VERSION  Test that the database server version number is supported for upgrade
  INFO   Database product version: Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
  With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options
  Completed schema test: TEST_DATABASE_VERSION --> Test that the database server version number is supported for upgrade +++ PASS

Starting schema test:  TEST_REQUIRED_TABLES  Test that the schema contains all the required tables
  Completed schema test: TEST_REQUIRED_TABLES --> Test that the schema contains all the required tables +++ PASS

Starting schema test:  TEST_UNEXPECTED_TABLES  Test that the schema does not contain any unexpected tables
  Completed schema test: TEST_UNEXPECTED_TABLES --> Test that the schema does not contain any unexpected tables +++ PASS

Starting schema test:  TEST_ENOUGH_TABLESPACE  Test that the schema tablespaces automatically extend if full
  Completed schema test: TEST_ENOUGH_TABLESPACE --> Test that the schema tablespaces automatically extend if full +++ PASS

Starting schema test:  TEST_USER_TABLESPACE_QUOTA  Test that tablespace quota for this user is sufficient to perform the upgrade
  Completed schema test: TEST_USER_TABLESPACE_QUOTA --> Test that tablespace quota for this user is sufficient to perform the upgrade +++ PASS

Starting schema test:  TEST_ONLINE_TABLESPACE  Test that schema tablespaces are online
  Completed schema test: TEST_ONLINE_TABLESPACE --> Test that schema tablespaces are online +++ PASS

Starting permissions test:  TEST_DBA_TABLE_GRANTS  Test that DBA user has privilege to view all user tables
  Completed permissions test: TEST_DBA_TABLE_GRANTS --> Test that DBA user has privilege to view all user tables +++ PASS

Starting schema test:  TEST_MISSING_COLUMNS  Test that tables and views are not missing any required columns
  Completed schema test: TEST_MISSING_COLUMNS --> Test that tables and views are not missing any required columns +++ PASS

Starting schema test:  TEST_UNEXPECTED_COLUMNS  Test that tables and views do not contain any unexpected columns
  Completed schema test: TEST_UNEXPECTED_COLUMNS --> Test that tables and views do not contain any unexpected columns +++ PASS

Starting datatype test for table OIDCOMPONENT: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes
  Completed datatype test for table OIDCOMPONENT:
TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes +++ PASS
  Starting datatype test for table IAU_CUSTOM_01:
  TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes
  Completed datatype test for table IAU_CUSTOM_01:
  TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes +++ PASS
  Starting datatype test for table IAU_BASE: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes
  Completed datatype test for table IAU_BASE: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes +++ PASS
  Starting datatype test for table WS_POLICYATTACHMENT:
  TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes
  Completed datatype test for table WS_POLICYATTACHMENT:
  TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes +++ PASS
  Starting datatype test for table OWSM_PM_EJB: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes
  Completed datatype test for table OWSM_PM_EJB: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes +++ PASS
  Starting datatype test for table XMLPSERVER: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes
  Completed datatype test for table XMLPSERVER: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes +++ PASS
  Starting datatype test for table SOA_HCFP: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes
  Completed datatype test for table SOA_HCFP: TEST_COLUMN_DATATYPES_V2 --> Test that all table columns have the proper datatypes +++ PASS
  Starting schema test: SEQUENCE_TEST Test that the audit schema sequence and its properties are valid
  Completed schema test: SEQUENCE_TEST --> Test that the audit schema sequence and its properties are valid +++ PASS
  Starting schema test: SYNONYMS_TEST Test that the audit schema required synonyms are present
  Completed schema test: SYNONYMS_TEST --> Test that the audit schema required synonyms are present +++ PASS
  Finished readiness check of Oracle Audit Services with status: FAILURE.

Common Infrastructure Services
Starting readiness check of Common Infrastructure Services.
  Schema User Name: DEV3_STB
  Database Type: Oracle Database
  Database Connect String:
  Starting schema test: TEST_REQUIRED_TABLES Test that the schema contains all the required tables
  Completed schema test: TEST_REQUIRED_TABLES --> Test that the schema contains all the required tables +++ PASS
  Completed schema test: ALL_TABLES --> TEST_REQUIRED_TABLES +++ Test that the schema contains all the required tables
  Starting schema test: TEST_UNEXPECTED_TABLES Test that the schema does not contain any unexpected tables
  Completed schema test: ALL_TABLES --> TEST_UNEXPECTED_TABLES +++ Test that the schema does not contain any unexpected tables
Starting schema test: TEST_REQUIRED.Views Test that the schema contains all the required database views
Completed schema test: ALL_TABLES --> TEST_REQUIRED.Views +++ Test that the schema contains all the required database views
Starting schema test: TEST_MISSING_COLUMNS Test that tables and views are not missing any required columns
Completed schema test: ALL_TABLES --> TEST_MISSING_COLUMNS +++ Test that tables and views are not missing any required columns
Starting schema test: TEST_DATABASE_VERSION Test that the database server version number is supported for upgrade
Starting schema test: TEST_DATABASE_VERSION Test that the database server version number is supported for upgrade
INFO Database product version: Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options
Completed schema test: TEST_DATABASE_VERSION --> Test that the database server version number is supported for upgrade +++ PASS
Completed schema test: ALL_TABLES --> TEST_DATABASE_VERSION +++ Test that the database server version number is supported for upgrade
Finished schema test of Common Infrastructure Services with status: SUCCESS.

Oracle JRF
Starting readiness check of Oracle JRF.
Finished readiness check of Oracle JRF with status: SUCCESS.

System Components Infrastructure
Starting readiness check of System Components Infrastructure.
Starting config test: TEST_SOURCE_CONFIG Checking the source configuration.
INFO /oracle/work/middleware_1212/user_projects/domains/jrf_domain/opmn/topology.xml was not found. No upgrade is needed.
Completed config test: TEST_SOURCE_CONFIG --> Checking the source configuration. +++ PASS
Finished readiness check of System Components Infrastructure with status: ALREADY_UPGRADED.

Common Infrastructure Services
Starting readiness check of Common Infrastructure Services.
Starting config test: CIEConfigPlugin.readiness.test This tests the readiness of the domain from CIE side.
Completed config test: CIEConfigPlugin.readiness.test --> This tests the readiness of the domain from CIE side. +++ PASS
Finished readiness check of Common Infrastructure Services with status: SUCCESS.

Finished readiness check of components.
Starting the Servers on OAMHOSTs

After you upgrade Oracle Access Management on an OAMHOST, start the servers.

You must start the servers in the following order:

1. Start the Node Manager on the required OAMHOST.
2. Start the Administration Server on the required OAMHOST.
3. Start the Oracle Access Management Managed Servers on the required OAMHOST.

Enabling WebGates to Work With Oracle Access Management

After upgrading to Oracle Access Management 12c (12.2.1.4.0), the earlier version of WebGates continues to work with Oracle Access Management. However, to leverage the latest security features of Oracle Access Management and WebGates 12c (12.2.1.4.0), you must upgrade the WebGates to 12c (12.2.1.4.0), and register the agent's profile with the Oracle Access Management Server.

Note:

If you have any other components of Oracle Identity and Access Management deployed, then all of the components must be upgraded to 12c (12.2.1.4.0) to leverage the new security features of 12c (12.2.1.4.0).

To upgrade the WebGates, you must upgrade the respective Web Servers to 12c (12.2.1.4.0).
To upgrade the Oracle HTTP Server WebGates, upgrade Oracle HTTP Server to 12c (12.2.1.4.0). See Upgrading a Standalone Oracle HTTP Server in the Upgrading Oracle HTTP Server.

To upgrade the Oracle Traffic Director WebGates, upgrade Oracle Traffic Director to 12c (12.2.1.4.0). See Upgrading Oracle Traffic Director in the Upgrading Oracle Traffic Director.

After you upgrade the Web Servers, do the following:

1. Register or edit the WebGate profile and copy the WebGate artifacts to the WebGate config folder. See Upgrading to OHS/OTD 12c (12.2.1.4.0) WebGate in the Installing WebGates for Oracle Access Manager.
2. Start and stop the WebGates.
Upgrading Oracle Identity Manager Highly Available Environments

Describes the process of upgrading an Oracle Identity Manager highly available environment from 12c (12.2.1.3.0) to Oracle Identity Governance 12c (12.2.1.4.0).

Note:
The product Oracle Identity Manager is referred to as Oracle Identity Manager (OIM) and Oracle Identity Governance (OIG) interchangeably in the guide.

Topics

• About the Oracle Identity Manager Multinode Upgrade Process
  Review the topology and the roadmap for an overview of the upgrade process for Oracle Identity Manager highly available environments.

• Backing up the 12c (12.2.1.3.0) Middleware Home Folder on OIMHOSTs
  Backup the 12c (12.2.1.3.0) Middleware Home on both OIMHOST1 and OIMHOST2.

• Stopping Servers and Processes
  Before you upgrade the schemas and configurations, you must shut down all of the pre-upgrade processes and servers, including the Administration Server and any managed servers on OIMHOST.

• Uninstalling the Software on an OIMHOST
  Follow the instructions in this section to start the Uninstall Wizard and remove the software.

• Installing Product Distributions on an OIMHOST
  Install the 12c (12.2.1.4.0) binaries on the required OIMHOST.

• Upgrading Schemas on OIMHOST1
  Upgrade all of the necessary schemas for Oracle Identity Manager, on OIMHOST1 by using the Upgrade Assistant.

• Upgrading Domain Component Configurations on OIMHOST1
  Use the Upgrade Assistant to upgrade the domain component's configurations inside the domain to match the updated domain configuration.

• Copying oracle.iam.ui.custom-dev-starter-pack.war to the 12c (12.2.1.4.0) Middleware Home
  After you upgrade the domain component configurations on OIMHOST1 by using the upgrade-sharedlibs.sh utility, copy the oracle.iam.ui.custom-dev-starter-pack.war file from backup of 12c (12.2.1.3.0) Middleware home to 12c (12.2.1.4.0) Middleware home manually.
• **Starting the Servers on an OIMHOST**
  After you upgrade Oracle Identity Manager on an OIMHOST, start the server.

• **Packing Domain Configurations on OIMHOST1**
  After upgrading domain component configurations on OIMHOST1, pack the upgraded domain on OIMHOST1. You must unpack it later on OIMHOST2.

• **Replicating the Domain Configurations on OIMHOST2**
  Replicate the domain configurations on OIMHOST2. This involves unpacking the upgraded domain on OIMHOST2, which was packed on OIMHOST1.

• **Updating the JDK location**
  When upgrading from 12c (12.2.1.3.0) to 12c (12.2.1.4.0), the reconfiguration wizard is not used. So, the latest JDK version is not automatically updated in the domain home.

• **Updating the setDomainEnv.sh file**
  For upgrading Oracle Identity Governance (OIG) from 12c (12.2.1.3.0) to 12c (12.2.1.4.0), you need to delete a property in the `setDomainEnv.sh` file.

## About the Oracle Identity Manager Multinode Upgrade Process

Review the topology and the roadmap for an overview of the upgrade process for Oracle Identity Manager highly available environments.

The steps you take to upgrade your existing domain will vary depending on how your domain is configured and which components are being upgraded. Follow only those steps that are applicable to your deployment.

### Upgrade Topology

The following topology shows the Oracle Identity Manager cluster set up that can be upgraded to 12c (12.2.1.4.0) by following the procedure described in this chapter.

![Oracle Identity Manager High Availability Upgrade Topology](image-url)
On OIMHOST1, the following installations have been performed:

- An Oracle Identity Manager instance has been installed in the WLS_OIM1 Managed Server and a SOA instance has been installed in the WLS_SOA1 Managed Server.
- A WebLogic Server Administration Server has been installed. Under normal operations, this is the active Administration Server.

On OIMHOST2, the following installations have been performed:

- An Oracle Identity Manager instance has been installed in the WLS_OIM2 Managed Server and a SOA instance has been installed in the WLS_SOA2 Managed Server.
- A WebLogic Server Administration Server has been installed. Under normal operations, this is the passive Administration Server. You make this Administration Server active if the Administration Server on OIMHOST1 becomes unavailable.

The instances in the WLS_OIM1 and WLS_OIM2 Managed Servers on OIMHOST1 and OIMHOST2 are configured as the OIM_CLUSTER cluster.

The instances in the WLS_SOA1 and WLS_SOA2 Managed Servers on OIMHOST1 and OIMHOST2 are configured as the SOA_CLUSTER cluster.

Pre-upgrade task for Oracle Identity Manager highly available environments

In the Oracle Identity Manager highly available environments setup, if Node 1 (Admin server) is upgraded to 12c (12.2.1.4.0) and Node 2 is still on 12c (12.2.1.3.0), then do not perform any admin operations, like creating new artifacts, on the 12c (12.2.1.3.0) node. For example: creating IT resources, adding provisioning task to resource history, and so on.

If you need to perform the tasks in a heterogeneous cluster mode. That is, Node 1 on 12c (12.2.1.4.0) and Node 2 on 12c (12.2.1.3.0). Then consider performing any of the following options:

- **Option 1**: Configure OHS to go for Node 1 on 12c (12.2.1.4.0), only for all admin operations.

- **Option 2**: Prior to upgrade, move OIM applications session from the replicated_if_clustered mode to the memory mode. In this setting, failover of one node will not be handled by other node. If a node crashes, all users session on the node would be lost. You need to login again and perform the operations again which were in progress when the node crashed.

Complete the following steps to move the OIM applications session from the replicated_if_clustered mode to the memory mode:

1. On Node 2 on 12c (12.2.1.3.0), change the session descriptor, from replicated_if_clustered to memory, for following files:

   - `<12c_middleware_home>/idm/server/apps/oim.ear/xlWebApp.war/WEB-INF/weblogic.xml`
   
   - `<12c_middleware_home>/idm/server/apps/oim.ear/iam-consoles-faces.war/WEB-INF/weblogic.xml`

For example: change from

```xml
<session-descriptor>
<persistent-store-type>replicated_if_clustered</persistent-store-
```
2. Restart Node 2.

3. On Node 1, after installing the 12c (12.2.1.4.0) binaries, change the session descriptor, from `replicated_if_clustered` to `memory`, for file:
   `<12c_middleware_home>/idm/server/apps/oim.ear/iam-consoles-faces.war/WEB-INF/weblogic.xml`

   **Note:**
   xIWebApp is not present in 12c (12.2.1.4.0) binaries.

4. Proceed with the upgrade process on the Node1 Admin server.

5. After upgrading all the nodes to 12c (12.2.1.4.0), you can switch again to the `replicated_if_clustered` mode.

### Table 6-1  Tasks for Upgrading Oracle Identity Manager Highly Available Environments

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required</td>
<td>If you have not done so already, review the introductory topics in this guide and complete the required pre-upgrade tasks. See:</td>
</tr>
<tr>
<td></td>
<td>• Introduction to Upgrading Oracle Identity and Access Management to 12c (12.2.1.4.0)</td>
</tr>
<tr>
<td></td>
<td>• Pre-Upgrade Requirements</td>
</tr>
<tr>
<td>Required</td>
<td>Generate the pre-upgrade report for Oracle Identity Manager. Review the information in the report and perform the mandatory pre-upgrade tasks, if any. See Generating and Analyzing Pre-Upgrade Report for Oracle Identity Manager.</td>
</tr>
<tr>
<td>Required</td>
<td>Complete the necessary pre-upgrade tasks specific to Oracle Identity Manager. See Completing the Pre-Upgrade Tasks for Oracle Identity Manager.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>Create backup of the existing 12c (12.2.1.3.0) Middleware home folders on OIMHOSTs</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td><strong>Backup any UI customizations made in 12c (12.2.1.3.0), which is the oracle.iam.ui.custom-dev-starter-pack.war file.</strong></td>
</tr>
<tr>
<td><strong>Required on OIMHOST1</strong></td>
<td>Shut down the 12c server on OIMHOST1. This includes the Administration Server, Managed Servers, Node Manager, and system components like Oracle HTTP Server. Ensure that the Database is up during the upgrade.</td>
</tr>
<tr>
<td><strong>Required on OIMHOST1</strong></td>
<td>On OIMHOST1, uninstall Oracle Fusion Middleware Infrastructure and Oracle Internet Directory 12c (12.2.1.3.0) in the existing Oracle home.</td>
</tr>
<tr>
<td><strong>Required on OIMHOST1</strong></td>
<td>On OIMHOST1, install Infrastructure (JRF) 12c (12.2.1.4.0), Oracle SOA Suite 12c (12.2.1.4.0), and Oracle Identity and Access Management 12c (12.2.1.4.0) in the Oracle home.</td>
</tr>
<tr>
<td><strong>Required on OIMHOST1</strong></td>
<td>Update the JDK location.</td>
</tr>
<tr>
<td><strong>Optional</strong></td>
<td>Run a pre-upgrade readiness check.</td>
</tr>
<tr>
<td><strong>Required on OIMHOST1</strong></td>
<td>Upgrade the necessary schemas on OIMHOST1.</td>
</tr>
<tr>
<td><strong>Required on OIMHOST1</strong></td>
<td>Upgrade the Oracle Identity Manager configurations on OIMHOST1, using the Upgrade Assistant.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td><strong>The jce should use unlimited strength crypto policy.</strong></td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Required on OIMHOST1</strong></td>
<td>Copy the <code>oracle.iam.ui.custom-dev-starter-pack.war</code> file to 12c (12.2.1.4.0) Middleware Home on OIMHOST1. See Copying <code>oracle.iam.ui.custom-dev-starter-pack.war</code> to the 12c (12.2.1.4.0) Middleware Home.</td>
</tr>
<tr>
<td><strong>Required on OIMHOST1</strong></td>
<td>Update the <code>setDomainEnv.sh</code> file. See Updating the <code>setDomainEnv.sh</code> file.</td>
</tr>
<tr>
<td><strong>Required on OIMHOST1</strong></td>
<td>Start the servers in the following order. Also, ensure that each server is started and running before starting the next server the following list: 1. Start the Administration server. 2. Start the SOA server. 3. Start the OIM server. See Starting the Servers.</td>
</tr>
<tr>
<td><strong>Required on OIMHOST1</strong></td>
<td>Pack the domain on OIMHOST1 See Packing Domain Configurations on OIMHOST1.</td>
</tr>
<tr>
<td><strong>Required on OIMHOST2</strong></td>
<td>Shut down the 12c server on OIMHOST2. This includes the SOA server, OIM server, and Node Manager. Ensure that the Database is up during the upgrade. <strong>WARNING:</strong> Failure to shut down your servers during an upgrade may lead to data corruption. See Stopping Servers and Processes.</td>
</tr>
<tr>
<td><strong>Required on OIMHOST2</strong></td>
<td>On OIMHOST2, uninstall Oracle Fusion Middleware Infrastructure and Oracle Internet Directory 12c (12.2.1.3.0) in the existing Oracle home. See Uninstalling the Software on an OIMHOST.</td>
</tr>
<tr>
<td><strong>Required on OIMHOST2</strong></td>
<td>On OIMHOST2, install Infrastructure (JRF) 12c (12.2.1.4.0), Oracle SOA Suite 12c (12.2.1.4.0), and Oracle Identity and Access Management 12c (12.2.1.4.0) in the Oracle home. See Installing Product Distributions on an OIMHOST.</td>
</tr>
<tr>
<td><strong>Required on OIMHOST2</strong></td>
<td>Update the JDK location See Updating the JDK location.</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>Replicate the domain configurations on OIMHOST2. This includes unpacking the domain on OIMHOST2. See Replicating the Domain Configurations on OIMHOST2.</td>
</tr>
<tr>
<td><strong>Required on OIMHOST2</strong></td>
<td>Copy the <code>oracle.iam.ui.custom-dev-starter-pack.war</code> file to 12c (12.2.1.4.0) Middleware Home on OIMHOST1. See Copying <code>oracle.iam.ui.custom-dev-starter-pack.war</code> to the 12c (12.2.1.4.0) Middleware Home.</td>
</tr>
<tr>
<td><strong>Required on OIMHOST2</strong></td>
<td>Update the <code>setDomainEnv.sh</code> file. See Updating the <code>setDomainEnv.sh</code> file.</td>
</tr>
</tbody>
</table>
Table 6-1  (Cont.) Tasks for Upgrading Oracle Identity Manager Highly Available Environments

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required on OIMHOST2</strong></td>
<td>Start the servers in the following order. Also, ensure that each server is started and running before starting the next server the following list:</td>
</tr>
<tr>
<td>1. Start the SOA server.</td>
<td>See Starting the Servers.</td>
</tr>
<tr>
<td>2. Start the OIM server.</td>
<td></td>
</tr>
<tr>
<td><strong>Procedure to check</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Optional</strong></td>
<td>Perform the post-upgrade tasks for SSL enabled setup.</td>
</tr>
<tr>
<td></td>
<td>See Completing the Post-Upgrade Tasks for SSL Enabled Setup.</td>
</tr>
<tr>
<td><strong>Optional</strong></td>
<td>When you upgrade to Oracle Identity Governance 12c (12.2.1.4.0), the embedded Oracle BI Publisher present in the 11.1.2.3.0 deployment is removed. Therefore, you must install a new standalone Oracle BI Publisher 12c (12.2.1.4.0) on OIMHOST1 and OIMHOST2, post upgrade. After you install, integrate it with Oracle Identity Governance 12c (12.2.1.4.0) to configure the Oracle Identity Governance reports.</td>
</tr>
<tr>
<td></td>
<td>See Installing Standalone Oracle BI Publisher.</td>
</tr>
</tbody>
</table>

**Backing up the 12c (12.2.1.3.0) Middleware Home Folder on OIMHOSTs**

Backup the 12c (12.2.1.3.0) Middleware Home on both OIMHOST1 and OIMHOST2.

As a backup, copy and rename the 12.2.1.3.0 Middleware home folder on OIMHOST1 and OIMHOST2.
For example:

From /scratch/work/u01/mw12c to /scratch/work/u01/mw12c_old

**Stopping Servers and Processes**

Before you upgrade the schemas and configurations, you must shut down all of the pre-upgrade processes and servers, including the Administration Server and any managed servers on OIMHOST.

An Oracle Fusion Middleware environment can consist of an Oracle WebLogic Server domain, an Administration Server, multiple managed servers, Java components, system components such as Identity Management components, and a database used as a repository for metadata. The components may be dependent on each other, so they must be stopped in the correct order.
To stop your pre-upgrade Fusion Middleware environment, navigate to the pre-upgrade domain and follow the steps below.

**Step 1: Stop the Managed Servers**

To stop a WebLogic Server Managed Server, use the `stopManagedWebLogic` script:

- (UNIX) `EXISTING_DOMAIN_HOME/bin/stopManagedWebLogic.sh
  managed_server_name admin_url`
- (Windows) `EXISTING_DOMAIN_HOME\bin\stopManagedWebLogic.cmd
  managed_server_name admin_url`

When prompted, enter your user name and password.

**Step 2: Stop the Administration Server**

When you stop the Administration Server, you also stop the processes running in the Administration Server, including the WebLogic Server Administration Console and Fusion Middleware Control.

To stop the Administration Server, use the `stopWebLogic` script:

- (UNIX) `EXISTING_DOMAIN_HOME/bin/stopWebLogic.sh`
- (Windows) `EXISTING_DOMAIN_HOME\bin\stopWebLogic.cmd`

When prompted, enter your user name, password, and the URL of the Administration Server.

**Step 3: Stop Node Manager**

To stop Node Manager, close the command shell in which it is running.

Alternatively, after having set the `nodemanager.properties` attribute `QuitEnabled` to `true` (the default is `false`), you can use WLST to connect to Node Manager and shut it down. See `stopNodeManager` in *WLST Command Reference for WebLogic Server*. 

---

**Note:**

- The procedures in this section describe how to stop the existing, pre-upgrade servers and processes using the WLST command-line utility or a script. You can also use the Oracle Fusion Middleware Control and the Oracle WebLogic Server Administration Console. See Starting and Stopping Administration and Managed Servers and Node Manager.
- Stop all of the servers in your deployment, except for the Database. The Database must be up during the upgrade process.
Uninstalling the Software on an OIMHOST

Follow the instructions in this section to start the Uninstall Wizard and remove the software.

If you want to uninstall the product in a silent (command-line) mode, see Running the Oracle Universal Installer for Silent Uninstallation in Installing Software with the Oracle Universal Installer.

- Starting the Uninstall Wizard
- Selecting the Product to Uninstall
- Navigating the Uninstall Wizard Screens

Starting the Uninstall Wizard

Start the Uninstall Wizard:

1. Change to the following directory:
   (UNIX) `ORACLE_HOME/oim/bin`
   (Windows) `ORACLE_HOME\oim\bin`

2. Enter the following command:
   (UNIX) `.deinstall.sh`
   (Windows) `deinstall.cmd`

Selecting the Product to Uninstall

Because multiple products exist in the Oracle home, ensure that you are uninstalling the correct product.

After you run the Uninstall Wizard, the Distribution to Uninstall screen opens.

- For OAM or OIM only install: Click Uninstall.
- For OAM or OIM installed with other products: From the dropdown menu, select the Oracle Identity and Access Management 12.2.1.3.0 product and click Uninstall.

The uninstallation program shows the screens listed in Navigating the Uninstall Wizard Screens.

Run the Uninstall Wizard again to uninstall the Oracle Fusion Middleware Infrastructure. For instructions see, Uninstalling Oracle Fusion Middleware Infrastructure in Installing and Configuring the Oracle Fusion Middleware Infrastructure.

Navigating the Uninstall Wizard Screens

The Uninstall Wizard shows a series of screens to confirm the removal of the software.

If you need help on screen listed in the following table, click Help on the screen.
Table 6-2  Uninstall Wizard Screens and Descriptions

<table>
<thead>
<tr>
<th>Screen</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome</td>
<td>Introduces you to the product Uninstall Wizard.</td>
</tr>
<tr>
<td>Uninstall Summary</td>
<td>Shows the Oracle home directory and its contents that are uninstalled. Verify that this is the correct directory.</td>
</tr>
<tr>
<td></td>
<td>If you want to save these options to a response file, click <strong>Save Response File</strong> and enter the response file location and name. You can use the response file later to uninstall the product in silent (command-line) mode. See Running the Oracle Universal Installer for Silent Uninstall in <em>Installing Software with the Oracle Universal Installer</em>.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Deinstall</strong>, to begin removing the software.</td>
</tr>
<tr>
<td>Uninstall Progress</td>
<td>Shows the uninstallation progress.</td>
</tr>
<tr>
<td>Uninstall Complete</td>
<td>Appears when the uninstallation is complete. Review the information on this screen, then click <strong>Finish</strong> to close the Uninstall Wizard.</td>
</tr>
</tbody>
</table>

**Note:**

After the product is uninstalled, ensure that the `ORACLE_HOME` folder exists and it does not contain any files or folders. If there are any remaining files or folders in the `ORACLE_HOME` folder, delete them.

Installing Product Distributions on an OIMHOST

Install the 12c (12.2.1.4.0) binaries on the required OIMHOST.

Install the following products on the required OIMHOST:

Complete the following steps:

1. Install the following products on the required OIMHOST.
   - Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0)
   - Oracle SOA Suite 12c (12.2.1.4.0)
   - Oracle Identity and Access Management 12c (12.2.1.4.0)

For more information, see *Installing Product Distributions*.

Upgrading Schemas on OIMHOST1

Upgrade all of the necessary schemas for Oracle Identity Manager, on OIMHOST1 by using the Upgrade Assistant.

See, *Upgrading Product Schemas*.

**Note:**

Perform schema upgrade on OIMHOST1 only.
Upgrading Domain Component Configurations on OIMHOST1

Use the Upgrade Assistant to upgrade the domain component’s configurations inside the domain to match the updated domain configuration.

Note:
Perform this procedure OIMHOST1 only.

To upgrade the domain configurations in a highly available setup, follow the instructions described in Upgrading Domain Component Configurations on OIMHOST1.

Copying oracle.iam.ui.custom-dev-starter-pack.war to the 12c (12.2.1.4.0) Middleware Home

After you upgrade the domain component configurations on OIMHOST1 by using the upgrade-sharedlibs.sh utility, copy the oracle.iam.ui.custom-dev-starter-pack.war file from backup of 12c (12.2.1.3.0) Middleware home to 12c (12.2.1.4.0) Middleware home manually.

Complete the following steps:

1. From the 12c (12.2.1.3.0) release folder, go to location: 12c_old_Middleware_Home/idm/server/apps/
2. Copy the file: oracle.iam.ui.custom-dev-starter-pack.war
3. For 12c (12.2.1.4.0) release, go to location: 12c_Middleware_Home/idm/server/apps/ and paste the copied .war file.

Starting the Servers on an OIMHOST

After you upgrade Oracle Identity Manager on an OIMHOST, start the server.

You must start the servers in the following order:

1. Start the Administration Server on the OIMHOST.
2. Start the Oracle SOA Suite Managed Server on the OIMHOST with Administration Server URL.
   For example: ./startManagedWebLogic.sh soa_server1 t3://weblogic_admin_host:weblogic_admin_port
3. Once the SOA server is in running state, start the Oracle Identity Governance Managed Server with Administration Server URL, on the OIMHOST.
   This time, OIM bootstrap process will be executed, and after successful bootstrap, OIM Managed Server would restart automatically.
4. Shut down the SOA Managed Server and the Administration Server on the OIMHOST.
5. Start the Node Manager on the OIMHOST.
6. Start the Administration Server on the OIMHOST.
7. Start the Oracle SOA Suite Managed Server (without BPM property) and Oracle Identity Manager Managed Servers on the OIMHOST.

For more information about starting the servers and processes, see Starting the Servers.

For more information about stopping the servers and processes, see Stopping Servers and Processes.

Packing Domain Configurations on OIMHOST1

After upgrading domain component configurations on OIMHOST1, pack the upgraded domain on OIMHOST1. You must unpack it later on OIMHOST2.

To do this, complete the following steps:

1. On OIMHOST1, run the following command from the location $MW_HOME/oracle_common/common/bin to pack the upgraded domain:
   - On UNIX:
     ```bash
     sh pack.sh -domain=<Location_of_OIM_domain> -template=<Location_where_domain_configuration_jar_to_be_created> -template_name=OIM Domain -managed=true
     ```
   - On Windows:
     ```cmd
     pack.cmd -domain=<Location_of_OIM_domain> -template=<Location_where_domain_configuration_jar_to_be_created> -template_name=OIM Domain -managed=true
     ```
2. Copy the domain configuration jar file created by the pack command on OIMHOST1 to any accessible location.

Replicating the Domain Configurations on OIMHOST2

Replicate the domain configurations on OIMHOST2. This involves unpacking the upgraded domain on OIMHOST2, which was packed on OIMHOST1.

To do this, complete the following steps:

1. Earlier in the procedure, you created a copy the domain configuration jar file by using the pack command on OIMHOST1. See Packing Domain Configurations on OIMHOST1.
   Copy the domain configuration jar file created by the pack command on OIMHOST1 to any accessible location on OIMHOST2.
2. On OIMHOST2, rename the existing domain home to <domain_home>_old.
3. On OIMHOST2, run the following command from the location $MW_HOME/oracle_common/common/bin to unpack the domain:
   - On UNIX:
sh unpack.sh -domain=<Location_of_OIM_domain> -template=<Location_where_domain_configuration_jar_to_be_created> -overwrite_domain=true

• On Windows:
unpack.cmd -domain=<Location_of_OIM_domain> -template=<Location_where_domain_configuration_jar_to_be_created> -overwrite_domain=true

Updating the JDK location

When upgrading from 12c (12.2.1.3.0) to 12c (12.2.1.4.0), the reconfiguration wizard is not used. So, the latest JDK version is not automatically updated in the domain home.

After upgrading to 12c (12.2.1.4.0), you must search the references to the current JDK in domain home and replace those instances with the location of the new JDK.

Note:
If you have installed the latest version of the JDK in the same location as the existing JDK, by overwriting the files, then you can skip updating the JDK location.

You must manually search the references to the current JDK in domain home and replace those instances with the location of the new JDK. For information about updating the JDK location, see Updating the JDK Location in an Existing Domain Home.

Updating the setDomainEnv.sh file

For upgrading Oracle Identity Governance (OIG) from 12c (12.2.1.3.0) to 12c (12.2.1.4.0), you need to the delete a property in the setDomainEnv.sh file.

Complete the following steps:

1. Open to the setDomainEnv.sh file in the Oracle_Home/domains/<domain name>/bin/location.
2. Delete the following line:

-Doracle.xdkjava.compatibility.version : 11.1.1

3. Save and close the setDomainEnv.sh file.

Note:
For SOA, you need to add the following entry to the setSOADomainEnv.sh file.

-Doracle.xdkjava.compatibility.version=11.1.1
Upgrading Oracle Access Management Multi-Data Center Environments

You can upgrade Oracle Access Management deployed across multi-data centers (MDC) from 12c (12.2.1.3.0) to 12c (12.2.1.4.0).

Note:

To upgrade Oracle Access Management MDC environments to 12c (12.2.1.4.0), ensure that all of the data centers (DC) are at the same Patch Set level.

When you plan to upgrade to 12c (12.2.1.4.0), you can choose to have zero down time by stopping the data center that needs to be upgraded, and routing all the traffic to the other data centers. Once the upgrade has been completed on one data center, it can start and function as an independent data center. You can then redirect all the traffic to the upgraded data center.

• About the Oracle Access Management Multi-Data Center Topology
  The sample Oracle Access Management Multi-Data Center topology has two data centers — Master data center and Clone data center.

• Roadmap for Upgrading Oracle Access Management MDC Setup
  Use the upgrade roadmap to upgrade your Oracle Access Management multi-data center setup to 12c (12.2.1.4.0).

• Backing Up the Existing MDC Environment
  Before you begin with the upgrade, take a back up of your existing environment.

• Enabling Write Permission to Master and Clones (If Necessary)
  Before you start the upgrade, you must enable modifications to the system and policy configurations on both Master and Clones.

• Disabling and Deleting All Replication Agreements Between Master and Clone
  Disable all replication agreements between the Master and the Clone data centers.

• Redirecting Traffic to Master Data Center
  An in-line upgrade procedure is used to upgrade the Clone data center which requires downtime. Therefore, all traffic must be rerouted to the Master data center.

• Upgrading Oracle Access Management on Clone Data Center
  Upgrade Oracle Access Management on Clone data center to 12c (12.2.1.4.0) after you redirect the traffic to Master data center.

• Redirecting Traffic to Clone Data Center
  An in-line upgrade procedure is used to upgrade the Master data center which requires downtime. Therefore, all traffic must be rerouted to the Clone data center.
centers (also referred to as, the backup data centers or the secondary data centers).

- **Upgrading Oracle Access Management on Master Data Center**
  Upgrade Oracle Access Management on Master data center to 12c (12.2.1.4.0) after you redirect the traffic to clone data center.

- **Freezing all Changes to Clones (if Necessary)**
  After you upgrade Oracle Access Management on all of the Clone data center(s), it is recommended that you freeze the changes to the Clone data center(s). This is to avoid any inadvertent writes.

- **Syncing Access Metadata**
  Oracle Access Management metadata stored in Unified Data Model (UDM) needs to be synced from Master to Clone.

- **Creating Replication Agreement**
  Create the replication agreement again after upgrading the Master and the Clone data centers.

- **Bringing up the Master and Clone Data Centers Online**
  After successful upgrade, both Master and Clone data centers can be brought up online. Traffic can be routed to both data centers based on existing routing rules.

### About the Oracle Access Management Multi-Data Center Topology

The sample Oracle Access Management Multi-Data Center topology has two data centers — Master data center and Clone data center.

The procedure in this chapter describes how to upgrade Oracle Access Management in a MDC setup similar to the reference topology provided in this section. You can use this upgrade procedure to upgrade your environment with any number of data centers.
This figure shows a Master data center and a Clone data center, each of them including a full Access Manager installation. In this topology, GTM refers to the global load balancer, LTM refers to the local load balancer, and WG refers to the WebGate. The S2S OAP is the Oracle Access Protocol.

Roadmap for Upgrading Oracle Access Management MDC Setup

Use the upgrade roadmap to upgrade your Oracle Access Management multi-data center setup to 12c (12.2.1.4.0).

Table 7-1 Oracle Access Management MDC Upgrade Roadmap

<table>
<thead>
<tr>
<th>Task</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review the Oracle Access Management multi-data center topology.</td>
<td>See About the Oracle Access Management Multi-Data Center Topology</td>
</tr>
<tr>
<td>Back up your existing environment.</td>
<td>See Backing Up the Existing MDC Environment</td>
</tr>
<tr>
<td>Enable write permission to Master and Clone data centers, if not already done.</td>
<td>See Enabling Write Permission to Master and Clones (If Necessary)</td>
</tr>
</tbody>
</table>
Table 7-1  (Cont.) Oracle Access Management MDC Upgrade Roadmap

<table>
<thead>
<tr>
<th>Task</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable and delete all replication agreements between Master and Clone data centers.</td>
<td>See Disabling and Deleting All Replication Agreements Between Master and Clone</td>
</tr>
<tr>
<td>Redirect the traffic to the Master data center.</td>
<td>See Redirecting Traffic to Master Data Center</td>
</tr>
<tr>
<td>Upgrade Oracle Access Management on Clone data center.</td>
<td>See Upgrading Oracle Access Management on Clone Data Center</td>
</tr>
<tr>
<td>Redirect the traffic to the Clone data center.</td>
<td>See Redirecting Traffic to Clone Data Center</td>
</tr>
<tr>
<td>Upgrade Oracle Access Management on Master data center.</td>
<td>See Upgrading Oracle Access Management on Master Data Center</td>
</tr>
<tr>
<td>Freeze all changes to the Master and Clones, if required.</td>
<td>See Freezing all Changes to Clones (if Necessary)</td>
</tr>
<tr>
<td>Sync the access UDM data by exporting the access store data from Master data center and importing it on the Clone data center.</td>
<td>See Syncing Access Metadata</td>
</tr>
<tr>
<td>Create the replication agreement again.</td>
<td>See Creating Replication Agreement</td>
</tr>
<tr>
<td>Bring up the Master and Clone data centers online.</td>
<td>See Bringing up the Master and Clone Data Centers Online</td>
</tr>
</tbody>
</table>

Backing Up the Existing MDC Environment

Before you begin with the upgrade, take a back up of your existing environment.

After stopping all the servers, you must back up the following on every data center before proceeding with the upgrade process:

- `MW_HOME` directory (Middleware home directory), including the Oracle Home directories inside Middleware home.
- Oracle Access Management Domain Home directory on all OAM hosts.
- Following Database schemas:
  - Oracle Access Manager schema
  - Audit and any other dependent schema

For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

Enabling Write Permission to Master and Clones (If Necessary)

Before you start the upgrade, you must enable modifications to the system and policy configurations on both Master and Clones.

To do this, run the following command on Master and Clone data centers:
```
setMultiDataCenterWrite(WriteEnableFlag="true")
```
Disabling and Deleting All Replication Agreements Between Master and Clone

Disable all replication agreements between the Master and the Clone data centers.


Redirecting Traffic to Master Data Center

An in-line upgrade procedure is used to upgrade the Clone data center which requires downtime. Therefore, all traffic must be rerouted to the Master data center.

Consult your network infrastructure team or refer to the network infrastructure documentation to accomplish the traffic re-routing.

Upgrading Oracle Access Management on Clone Data Center

Upgrade Oracle Access Management on Clone data center to 12c (12.2.1.4.0) after you redirect the traffic to Master data center.

To upgrade Oracle Access Management on Master data center, follow the instructions described in Upgrading Oracle Access Management Highly Available Environments.

Redirecting Traffic to Clone Data Center

An in-line upgrade procedure is used to upgrade the Master data center which requires downtime. Therefore, all traffic must be rerouted to the Clone data centers (also referred to as, the backup data centers or the secondary data centers).

Consult your network infrastructure team or refer to the network infrastructure documentation to accomplish the traffic re-routing.
For more information, see Updating the JDK After Installing and Configuring an Oracle Fusion Middleware Product.

Upgrading Oracle Access Management on Master Data Center

Upgrade Oracle Access Management on Master data center to 12c (12.2.1.4.0) after you redirect the traffic to clone data center.

To upgrade Oracle Access Management on Master data center, follow the instructions described in Upgrading Oracle Access Management Highly Available Environments.
Freezing all Changes to Clones (if Necessary)

After you upgrade Oracle Access Management on all of the Clone data center(s), it is recommended that you freeze the changes to the Clone data center(s). This is to avoid any inadvertent writes.

To freeze the changes, run the following command on the Clone data center(s):

```
SetMultiDataCenterWrite(WriteEnableFlag="false")
```

Syncing Access Metadata

Oracle Access Management metadata stored in Unified Data Model (UDM) needs to be synced from Master to Clone.

You can sync the access metadata using the WLST commands - `exportAccessStore` and `importAccessStore`. These commands need to be executed after you upgrade all of the data centers and before creating the new replication agreement. This exports the UDM artifacts created till that point, from the Master data center and imports them in the Clone data center(s).

To sync the UDM metadata, complete the following steps:

1. Run the following WLST command on the Master data center to create a ZIP file containing the UDM metadata:
   ```
   exportAccessStore(toFile="/master/location/dc1metadata.zip", namePath="/"
   )
   ```
2. Copy `dc1metadata.zip` to each of the upgraded Clone data centers.
3. Run the following WLST command on the each of the Clone data centers to import the UDM metadata:
   ```
   importAccessStore(fromFile="/clone/location/dc1metadata.zip", namePath="/"
   )
   ```

Creating Replication Agreement

Create the replication agreement again after upgrading the Master and the Clone data centers.

To create the replication agreement, run the following command:

```
curl -u <repluser> -H 'Content-Type: application/json' -X POST 'https://supplier.example.com/oam/services/rest/_replication/setup' -d '{"name":"DC12DC2", "source":"DC1","target":"DC2","documentType":"ENTITY")'
```
For more information about creating a replication agreement, see Creating a Replication Agreement in the *Administrator's Guide for Oracle Access Management*.

**Bringing up the Master and Clone Data Centers Online**

After successful upgrade, both Master and Clone data centers can be brought up online. Traffic can be routed to both data centers based on existing routing rules.

Consult your network infrastructure team or refer to the network infrastructure documentation to accomplish the traffic re-routing.
Part III

Troubleshooting the Oracle Identity and Access Management Upgrade

If you encounter any issue when upgrading the Oracle Identity and Access Management components to 12c (12.2.1.4.0), follow the workaround described in the respective troubleshooting topics.

Topics

• **Troubleshooting the Oracle Access Management Upgrade**
  If you encounter errors while upgrading Oracle Access Management upgrade, review the following troubleshooting procedures.

• **Troubleshooting the Oracle Identity Manager Upgrade**
  If you encounter errors while upgrading Oracle Identity Manager, review the following troubleshooting procedures.
Troubleshooting the Oracle Access Management Upgrade

If you encounter errors while upgrading Oracle Access Management upgrade, review the following troubleshooting procedures.

- **Activation State is set as FAILED when Restarting the Admin Server**
  After you upgrade the domain component configurations and start the Admin server, the activation state is set as FAILED.

- **AMInitServlet Fails to Preload when Restarting OAM Managed Server**
  After you upgrade the domain component configurations and start the OAM managed server, AMInitServlet fails to preload.

- **File Not Found Exception when Starting the OAM Managed Server**
  After you upgrade the domain component configurations and start the server a File Not Found exception is displayed.

- **WADL Generation Does not Show Description**
- **Troubleshooting Security Policy Issues When Upgrading**

**Activation State is set as FAILED when Restarting the Admin Server**

After you upgrade the domain component configurations and start the Admin server, the activation state is set as FAILED.

Caused By: oracle.security.am.install.AMInstallException: Invalid Simple Mode Artifacts at oracle.security.am.install.startup.AMKeyStoreValidator.execute(AMKeyStoreValidator.java:70) at oracle.security.am.install.startup.OamInstallTopologyConfigListener.doMandatoryValidations(OamInstallTopologyConfigListener.java:114)

To solve the error, complete the following steps:

1. In the 11g environment, open to the oam-config.xml file and copy the value of sslGlobalPassphrase.
2. In the 12c environment, open to the oam-config.xml file and replace the value of sslGlobalPassphrase with the value that you copied from the 11g environment.

For more information about how to import or export oam-config.xml from database, see Doc ID 2310234.1.
AMInitServlet Fails to Preload when Restarting OAM Managed Server

After you upgrade the domain component configurations and start the OAM managed server, AMInitServlet fails to preload.

The following error message is displayed:

Caused By:
oracle.security.am.common.utilities.exception.AmRuntimeException:
Fail to decrypt oamkeystore data with cipher key from OAM config
(/DeployedComponent/Server/NGAMServer/Profile/ssoengine/CipherKey)
at oracle.security.am.engines.sso.adapter.OAMSessionConfiguration$Config
Listener.configurationChanged(OAMSes...)

To solve the error, complete the following steps:

1. In the 11g environment, open to the oam-config.xml file and copy the value of cipherKey.
2. In the 12c environment, open to the oam-config.xml file and replace the value of cipherKey with the value that you copied from the 11g environment.

For more information about how to import or export oam-config.xml from database, see Doc ID 2310234.1.

File Not Found Exception when Starting the OAM Managed Server

After you upgrade the domain component configurations and start the server a File Not Found exception is displayed.

This is a known issue. Ignore the following File Not Found exception:

[2019-09-04T05:52:24.349+00:00] [wls_oam1] [WARNING] [J2EE JMX-46714]
[oracle.as.jmx.framework.wls.spi.ComponentMBeans] [tid: [ACTIVE].ExecuteThread: '4' for queue: 'weblogic.kernel.Default (self-tuning)'] [userId: <WLS Kernel>] [ecid: ab946520-e98c-498c-5e9e0f055f40-00000007,0] [partition-name: DOMAIN] [tenant-name: GLOBAL] Error parsing MBean descriptor file "fmwconfig/mbeans/oamconfig_mbeans.xml".['[java.io.FileNotFoundException: The Config MBean jar file "C:\Oracle\Middleware_IAM\user_projects\domains\oam_domain\config\fmwconfig \mb eans\${OAM_ORACLE_HOME}\server\lib\jmx\configmgmt.jar" does not exist.

[2019-09-04T05:52:26.693+00:00] [wls_oam1] [WARNING] [J2EE JMX-46714]
[oracle.as.jmx.framework.wls.spi.ComponentMBeans] [tid: [ACTIVE].ExecuteThread: '4' for queue: 'weblogic.kernel.Default (self-tuning)'] [userId: <WLS Kernel>] [ecid: ab946520-e98c-498c-5e9e0f055f40-00000007,0] [partition-name: DOMAIN]
Error parsing MBean descriptor file "fmwconfig/mbeans/t2p_mbeans.xml". [java.io.FileNotFoundException: The Config MBean jar file "C:\Oracle\Middleware_IAM\user_projects\domains\oam_domain\config\fmwconfig\mb\eans\${OAM_ORACLE_HOME}\server\lib\jmx\was-t2p.jar" does not exist.]

WADL Generation Does not Show Description

Issue

WADL generation fails and a java.lang.IllegalStateException: ServiceLocatorImpl is returned.

Exception thrown when provider class org.glassfish.jersey.server.internal.monitoring.MonitoringFeature$Statistic$Listener was processing MonitoringStatistics. Removing provider from further processing. java.lang.IllegalStateException: ServiceLocatorImpl(__HK2_Generated_6,9,221656053) has been shut down at org.jvnet.hk2.internal.ServiceLocatorImpl.checkState(ServiceLocatorImpl.java:2393)

Also, when the WADL generation fails, the description field shows Root Resource, instead of a proper description in the following URLs.

http://<Host>:<AdminServerPort>/oam/services/rest/11.1.2.0.0/ssa/policyadmin/application.wadl
http://<Host>:<ManagedServerPort>/iam/access/api/v1/health/application.wadl

Resolution

Restart the Admin server and managed servers to resolve the wadl issue.

Troubleshooting Security Policy Issues When Upgrading

OAM 12c (12.2.1.4.0) has an improved security posture and leverages the capabilities added in the underlying infrastructure. OAM 12c (12.2.1.4.0) is certified with JDK 8, and based on the JDK 8 update used, its behavior may vary. More details about specific JDK 8 updates and their corresponding Java policies can be found in Release Notes for JDK 8 and JDK 8 Update Releases.

Oracle Access Protocol (OAP) version 5 has improved security for WebGate and server communication. OAP version 5 is used for communication between 12c (12.2.1.4.0) WebGates and 12c (12.2.1.4.0) OAM Servers.

- Modifying the Java Security Posture
Modifying the Java Security Posture

OAM Server 12c (12.2.1.4.0) supports TLS1.2 and SHA-2. For compatibility with older products (including Webgate, OIM, and OAAM), relax the OAM security posture by making the following changes to the java.security policy:

1. Remove TLSv1, TLSv1.1, MD5withRSA from the following key:
   
   key - jdk.tls.disabledAlgorithms

2. Remove MD5 from the following key:

   key - jdk.certpath.disabledAlgorithms

Upgrade Scenarios for OAM

An upgraded OAM environment can result in the following cases:

- If WebGate is upgraded and the OAM Server is not, then SSL communication between them uses TLSv1 with MD5 certificates.
- If OAM Server is upgraded and WebGate is not, then SSL communication between them fails, as the OAM Server rejects MD5 certificates and doesn't support TLSv1. In this case, you need to modify the Java security policy to enable TLSv1, TLSv1.1 and MD5.
- If both OAM Server and WebGate are upgraded, edit the WebGate profile and copy the WebGate artifacts to the WebGate config folder. SSL communication between the OAM Server and WebGates will use TLSv1.2 with SHA-2 certificates.

WebGates

12c (12.2.1.4.0) WebGates that employ version 4 of the OAP protocol will continue to work with OAM 12c (12.2.1.4.0). However, these WebGates must be upgraded to leverage the full capability of 12c (12.2.1.4.0). To upgrade the WebGates:

1. Stop the WebGates (OHS/OTD)
2. Upgrade WebGate binaries to 12c (12.2.1.4.0)
3. Edit WebGate profile and register the updated profile
4. Copy the WebGate artifacts to the WebGate config folder
5. Start the WebGates (OHS/OTD)

Multi-Data Center

If an upgrade results in a 12c (12.2.1.4.0) Master server and an 12c (12.2.1.3.0) clone server (or vice versa), then SSL communication between the servers fails. To enable communication between these servers, modify the java.security policy to enable TLSv1, TLSv1.1, and MD5 as suggested above.
Client Certificates

OAM Server 12c (12.2.1.4.0) rejects older client/user X.509 certificates that don't adhere to JDK 8 security requirements. See Release Notes for JDK 8 and JDK 8 Update Releases for MD5- and TLS-related restrictions for the JDK 8 update specific to the system. This behavior is governed by the JDK 8 java.security policy. To ensure acceptance of older client/user X.509 certificates, modify the java.security policy to enable TLSv1, TLSv1.1, and MD5 as described above.

Federation

For scenarios that involve Service Provider (SP) or Identity Provider (IDP) registration, the certificates used may undergo the same limitations as that for Client Certificates listed above.

Note that federation agreements will break if the Token Signing Certificate is changed. As a result, the 12c (12.2.1.3.0) security posture is carried forward after upgrading, which may require enabling the legacy algorithms (TLSv1, TLSv1.1, and MD5), as described above. The use of SHA-2 certificates is supported.

OIC

Similar to Federation, changing the OAuth Token Signing Certificate breaks existing trust relationships. As a result, the 12c (12.2.1.3.0) security posture is carried forward after upgrading, which may require enabling the legacy algorithms (TLSv1, TLSv1.1, and MD5), as described above. The use of SHA-2 certificates is supported.
Troubleshooting the Oracle Identity Manager Upgrade

If you encounter errors while upgrading Oracle Identity Manager, review the following troubleshooting procedures.

**Note:**

The product Oracle Identity Manager is referred to as Oracle Identity Manager (OIM) and Oracle Identity Governance (OIG) interchangeably in the guide.

- **Reading CSF Key Fails when Running Upgrade Assistance (UA)**
  During OIM upgrade to 12c (12.1.2.3.0), when you run Upgrade Assistance (UA) in readiness mode, OIM tries to read the CSF key and fails.

- **Access Denied Error when running the upgrade-sharedlibs.sh utility**
  If running the `upgrade-sharedlibs.sh` file displays an access denied error then verify and update where the 12c (12.2.1.4.0) binaries are stored.

- **KeystoreService Exception in the Logs After Reconfiguring the OIM Domain**
  After you reconfigure the Oracle Identity Manager (OIM) domain, the logs show some exceptions which can be ignored.

- **Warning when Generating the Pre-Upgrade Report for OIM**
  When you run the pre-upgrade report utility to generate the pre-upgrade report for Oracle Identity Manager, the audit store instantiation failure warning is seen on the console, which can be ignored.

- **OIM Bootstrap for DEPLOYSOACOMPOSITES Task Fails After Upgrade**
  After you complete the Oracle Identity Manager upgrade, when you start the Oracle Identity Manager Managed Servers for the first time, bootstrapping happens. If the OIM bootstrap fails for `DEPLOYSOACOMPOSITES` task, use the workaround described in this section to resolve the issue.

- **Authorization Policy Merge Issue**

- **MAR Update or Metadata Merge Issue**
  When you start the Oracle Identity Manager Managed Servers for the first time after upgrade, if you encounter any error during the bootstrap process which is related to `MARUPDATE` bootstrap task, run the external utility `mergeMDSDataAfterUpgrade.sh` from the 12c Middleware Home to re-trigger the Metadata Services (MDS) merge process.

- **Error When Opening ADF DI Excel Sheet After Upgrade**
  The ADFDI functionality will not work after you upgrade Oracle Identity Manager to 12c (12.2.1.4.0).
• **Compilation Error When Starting the SOA Server After Upgrade**
  When you start the Oracle SOA Suite for the first time after upgrade, you may see the compilation error in the SOA server logs.

• **Warning in Oracle Identity Manager Server Logs After Upgrade**
  After upgrade, the Oracle Identity Manager (OIM) Server logs show NPE warning, which can be ignored.

• **Default Challenges Questions are not Updated After Upgrade**
  After you upgrade Oracle Identity Manager 12c (12.2.1.3.0) to 12c (12.2.1.4.0), the default challenge questions are not updated. It still shows the old or existing challenge questions.

• **EditFailedException When Releasing Configuration From WebLogic Console**
  After you upgrade Oracle Identity Manager to 12c (12.2.1.4.0), when you click **Release Configuration** on Oracle WebLogic Console, the following error is seen:

• **OIM Application Deployment Fails Intermittently**
  After you upgrade Oracle Identity Manager to 12c (12.2.1.4.0), the oim application deployment may fail with the following error:

• **Oracle Identity Manager Server Throws OutOfMemoryError**
  When you start the servers post upgrade, OutOfMemoryError is thrown.

• **LDAP User Create and Update Reconciliation Job Fails**
  LDAP User Create and Update Reconciliation job fails to run with the following exception:

• **BI Managed Server is Seen on WebLogic Console After Upgrade**
  If your 12c domain had a custom name for BI Managed Server, that is, the name other than bi_server1, then this Managed Server will not be deleted during the upgrade.

• **Empty Pages or Panels After Upgrade**
  After you complete the upgrade, the Applications tile in the OIM Self Service console and the Import/Export links in the Admin console may be rendered as empty pages or panels.

---

**Reading CSF Key Fails when Running Upgrade Assistance (UA)**

During OIM upgrade to 12c (12.1.2.3.0), when you run Upgrade Assistance (UA) in readiness mode, OIM tries to read the CSF key and fails.

To solve the issue, complete the following steps:

1. **Open the Update jps-config-jse.xml file at location $DOMAIN/config/fmwconfig.**

2. **Go to the section** `<serviceInstance name="audit.db" provider="audit.provider">`

3. **In the serviceInstance section, add the following as the first entry.**
  `<property name="server.type" value="DB_ORACLE"/>

Sample serviceInstance section:

```
<serviceInstance name="audit.db" provider="audit.provider">
  <property name="server.type" value="DB_ORACLE"/>
```

Access Denied Error when running the upgrade-sharedlibs.sh utility

If running the upgrade-sharedlibs.sh file displays an access denied error then verify and update where the 12c (12.2.1.4.0) binaries are stored.

There might be a scenario where you run the upgrade-sharedlibs.sh file for updating the library oracle.idm.ipf#1.0@12.2.1.3.0 and view an access denied error.

**Solution:** Ensure that the 12c (12.2.1.4.0) binaries are installed directly in the new 12c Middleware home folder and not copied from any other folder.

To identify if the binaries are installed directly in the new 12c Middleware home folder, complete the following steps:

1. **Open the** weblogic.policy **file located in the** `$<12c_Middleware_Home>/wlserver/server/lib/` **directory.**

2. **Verify that** `<12c_Middleware_Home>` **path used for individual grants is correct.** For example: In the following entry the location /SomeBase/12c_upg_prov/12cMW should be same as your $12cMWH and the directory should exist.

```java
grant codeBase
"file:/SomeBase/12c_upg_prov/12cMW/wlserver/..:/oracle_common/modules/thirdparty/-";
{ permission java.security.AllPermission; };
```

KeystoreService Exception in the Logs After Reconfiguring the OIM Domain

After you reconfigure the Oracle Identity Manager (OIM) domain, the logs show some exceptions which can be ignored.

The following exceptions are seen in the logs after you reconfigure the OIM domain:

```java
oracle.security.jps.upgrade.tools.KeyStoreUpgrade - Exception in checking
```
jdk cacert store
oracle.security.jps.service.keystore.KeyStoreServiceException: Failed to load
the keystore.
at
oracle.security.jps.internal.keystore.ldap.KeyStoreDataManager.getKeyStore(
Key
StoreDataManager.java:987)
at
oracle.security.jps.internal.keystore.ldap.LdapKeyStoreServiceImpl.getKeySt
ore
(LdapKeyStoreServiceImpl.java:279)
at
oracle.security.jps.upgrade.tools.KeyStoreUpgrade.importJdkCacerts(KeyStore
Upgrade.java:313)
at
oracle.security.jps.upgrade.tools.KeyStoreUpgrade.upgradeDITAndData(KeyStor
eUpgrade.java:266)
at
oracle.security.jps.upgrade.tools.utility.Upgrade.upgradeOPSSDITAndData(Upg
rade.java:1078)
at
oracle.security.jps.upgrade-tools.utility.Upgrade.upgradeOPSS(Upgrade.java:
772)
at
oracle.security.opss.tools.lifecycle.OpssDomainConfigImpl.reconfigSubsyste
m(Op
ssDomainConfigImpl.java:359)
at
oracle.security.opss.tools.lifecycle.OpssDomainConfigImpl.initializeSubsyste
m(Op
ssDomainConfigImpl.java:271)
at
oracle.security.opss.tools.lifecycle.cie.OpssSecurityConfiguration.initiali
zeS
ubsystem(OpssSecurityConfiguration.java:188)
at
com.oracle.cie.domain.progress.template.importer.ImporterOPSSProcessingPhas
e.i
itiate(ImporterOPSSProcessingPhase.java:36)
at
com.oracle.cie.domain.progress.domain.generation.OPSSProcessingPhase.proces
OPSS(OPSSProcessingPhase.java:154)
at
com.oracle.cie.domain.progress.domain.generation.OPSSProcessingPhase.execut
e(OPSSProcessingPhase.java:54)
at
com.oracle.cie.domain.progress.AbstractProgressGenerator.run(AbstractProgre
ssG
enerator.java:94)
Warning when Generating the Pre-Upgrade Report for OIM

When you run the pre-upgrade report utility to generate the pre-upgrade report for Oracle Identity Manager, the audit store instantiation failure warning is seen on the console, which can be ignored.

The following warning is seen on the console when generating the pre-upgrade report for OIM:

WARNING: Audit store instantiation failure, type: db reason: java.lang.ClassNotFoundException: oracle.security.audit.config.dynamic.persistence.internal.ldap.LdapAuditStore
Jul 28, 2016 10:26:05 PM oracle.security.jps.az.internal.runtime.service.PDPServiceImpl SEVERE: Cannot read the default policy store.
oracle.security.jps.service.policystore.PolicyStoreException: oracle.security.jps.az.internal.management.pd.PD at
oracle.security.jps.az.common.pd.service.PDServiceFinder.getPolicyDistributionService(PDServiceFinder.java:65) at
oracle.security.jps.az.internal.runtime.service.PDPServiceImpl.initializeMixedMode(PDPServiceImpl.java:714) at
oracle.security.jps.az.internal.runtime.service.PDPServiceImpl.initialize(PDPServiceImpl.java:685)

Ignore this warning and proceed.
OIM Bootstrap for DEPLOYSOACOMPOSITES Task Fails After Upgrade

After you complete the Oracle Identity Manager upgrade, when you start the Oracle Identity Manager Managed Servers for the first time, bootstrapping happens. If the OIM bootstrap fails for DEPLOYSOACOMPOSITES task, use the workaround described in this section to resolve the issue.

The following error is seen in the OIM server logs:

The following error is seen in the Oracle SOA Suite (SOA) server logs:

To resolve this issue, start the Oracle SOA Suite server with the following property:

-Dbpm.enabled=true

This completes the OIM bootstrap tasks successfully. After the successful completion of OIM bootstrap tasks, restart all of the servers. This time, do not use the property -Dbpm.enabled=true for starting the SOA server. When you start the Managed Servers for the first time after upgrade, start them with the Administration Server URL.

Authorization Policy Merge Issue

Oracle Identity Manager 11.1.2.3.0 has two Oracle Platform Security Services (OPSS) application policy stripes namely oim and OracleIdentityManager, whereas Oracle Identity Governance 12.2.1.3 has only one OPSS application policy stripe named oim.
The 12c upgrade process handles the merging of application stripes into one along with all the customization, at various phases. If you encounter any error or issue related to OPSS application policies after upgrade, or if you find the policies in inconsistent state, complete the following steps to restore the OPSS application policies:

1. The Authorization policy backup for OIM lying in OPSS schema is taken by the 12c pre-upgrade utility. This backup folder is located at oim.outputreportfolder/Auth-Policy-Backup.

   oim.outputreportfolder is the name of the pre-upgrade report output folder specified by you in the preupgrade_report_input.properties file when you ran the pre-upgrade utility.

The backup folder contains the following files:

   • oim.outputreportfolder/Auth-Policy-Backup/oim.xml — This is for oim application policy stripe of 11.1.2.3.0.
   • oim.outputreportfolder/Auth-Policy-Backup/OracleIdentityManager.xml — This is for OracleIdentityManager application policy stripe of 11.1.2.3.0.

   Restore these stripes data in OIM database using the following WLST offline commands:

   • migrateSecurityStore(type="appPolicies", srcApp="OracleIdentityManager ", configFile="DOMAIN_HOME/config/fmwconfig/jps-config_temp.xml", src="desContextOracle", dst="migrateStripe", overWrite="true")
   • migrateSecurityStore(type="appPolicies", srcApp="oim", configFile="DOMAIN_HOME/config/fmwconfig/jps-config_temp.xml", src="desContextOIM", dst="migrateStripe", overWrite="true")

   In the above commands, DOMAIN_HOME/config/fmwconfig/jps-config_temp.xml file is a copy of the DOMAIN_HOME/config/fmwconfig/jps-config.xml file. The following service instances and JPS contexts are added in this file:

   <serviceInstance name="serviceInsOracle" provider="policystore.xml.provider" location="<oim.outputreportfolder>/Auth-Policy-Backup/OracleIdentityManager.xml"/>
   <serviceInstance name="serviceInsOIM" provider="policystore.xml.provider" location="<oim.outputreportfolder>/Auth-Policy-Backup/oim.xml"/>

   <jpsContext name="desContextOracle">
   <serviceInstanceRef ref="serviceInsOracle"/>
   </jpsContext>
   <jpsContext name="desContextOIM">
   <serviceInstanceRef ref="serviceInsOIM"/>
   </jpsContext>
   <jpsContext name="migrateStripe">
   <serviceInstanceRef ref="policystore.db"/>
   </jpsContext>

2. Migrate the OracleIdentityManager stripe to oim stripe using the following WLST offline command:
migrateSecurityStore(type="appPolicies", srcApp="OracleIdentityManager", dstApp="oim", configFile=DOMAIN_HOME/config/fmwconfig/jps-config_temp.xml, src="migrateStripe", dst="migrateStripe", overWrite="false")

3. Merge the 12c Out Of The Box application policies on OIM 11.1.2.3.0 application policy stripe named as oim by doing the following:
   a. Unzip the 12c_Middleware_Home/idm/common/templates/wls/oracle.OIM.reconfig.template_1 2.2.1.2.0.jar file to any temporary location. This temporary location is referred to as unzip_location.
   b. Verify that the file unzip_location/security/authorization/jazn-data.xml exists.
   c. Run the following WLST offline command:

   ```
migrateSecurityStore(type="appPolicies", srcApp="oim", configFile=DOMAIN_HOME/config/fmwconfig/jps-config_temp.xml, src="12c_context", dst="migrateStripe", overWrite="false")
   ```

   The following service instances and JPS contexts are added in the DOMAIN_HOME/config/fmwconfig/jps-config_temp.xml file:

   ```
<serviceInstance name="serviceIns12c_context" provider="policystore.xml.provider" location="unzip_location/security/authorization/jazn-data.xml"/>
<serviceInstance name="oim"><jpsContext name="12c_context"> <serviceInstanceRef ref="service12c_context"/></jpsContext>
   ```

   d. Delete the OracleIdentityManager stripe using the following WLST command:

   ```
deleteAppPolicies(appStripe="OracleIdentityManager")
   ```

## MAR Update or Metadata Merge Issue

When you start the Oracle Identity Manager Managed Server for the first time after upgrade, if you encounter any error during the bootstrap process which is related to MARUPDATE bootstrap task, run the external utility mergeMDSDataAfterUpgrade.sh from the 12c Middleware Home to re-trigger the Metadata Services (MDS) merge process. The upgrade utility merges the existing MDS data with 12c Out of the Box (OOTB) to preserve the customization. When you start the OIM Managed Server for the first time, if you encounter errors for MARUPDATE bootstrap task, check if the issue is occurring during the MDS merge process. If so, run an external utility to re-trigger the MDS merge process as described in this section.

To check if the issue is occurring during the MDS merge process, do the following:

1. Connect to the Oracle Identity Manager database.
2. Use the following SQL query to check the status of the MARUPDATE bootstrap task:

   ```
   select State from OIMBootState where FEATURENAME='MARUPDATE';
   ```
3. If the query returns **VALID** or **COMPLETE**, the issue is not because of the MDS merge failure. Therefore, no action is required. If the query returns any other result, run the merge utility to re-trigger the MDS merge process.

To re-trigger the MDS merge process using the merge utility, complete the following steps:

1. The OIM pre-upgrade reports folder must exist on the same machine from which the MDS merge utility is going to be triggered. If the pre-upgrade reports are on a different machine, copy them to the machine from which you wish to run the merge utility. The pre-upgrade report utility takes a back up of the MDS data and saves it in the pre-upgrade reports folder.

   The MDS backup data is located at `<oim.outputreportfolder>/MDS-Backup` folder. `<oim.outputreportfolder>` is the path that you specified for the property `oim.outputreportfolder` in the `preupgrade_report_input.properties` file, when generating the pre-upgrade reports for OIM.

2. Run the following command from the location `12c_Middleware_Home/idm/server/bin/mergeMDSDataAfterUpgrade.sh`

   You must specify the location of the OIM pre-upgrade reports folder. The MDS merge utility that you triggered merges the MDS backup data from the pre-upgrade reports folder with the 12c data OOTB.

3. After the successful completion of the MDS merge process, connect to the OIM database and run the following query:
   ```sql
   update OIMBootState set State='COMPLETE' where FEATURENAME='MARUPDATE';
   ```

4. Restart the OIM Managed Server.

(Optional) Enter the result of the procedure here.

---

**Error When Opening ADF DI Excel Sheet After Upgrade**

The ADFDI functionality will not work after you upgrade Oracle Identity Manager to 12c (12.2.1.4.0).

After upgrade, when you open the ADF DI spreadsheet in Excel, the following error is displayed:

ADFDI-05587: The client and server versions do not match. Using this version of the client may result in unexpected behavior or errors. The client version is 12.2.1.3.0 (6882) but the server at http://host.example.com:22925/identity/adfdiRemoteServlet expects version 12.2.1.4.0 (16546) using precision 3.

To resolve this, uninstall and reinstall the ADF DI Excel plug-in, and then re-download the Excel.
Compilation Error When Starting the SOA Server After Upgrade

When you start the Oracle SOA Suite for the first time after upgrade, you may see the compilation error in the SOA server logs.

The following error is displayed in the SOA server logs:

```
[2016-07-01T02:04:18.239-07:00] [soa_server1] [ERROR] [oracle.soa.bpel.system] [tid: DaemonWorkThread: '8' of WorkManager: 'wm/SOAWorkManager'] [userId: ] [ecid: 4f969dd2-853a-4ddf-be01-0ac2ca0d2210-00000009,0:11854] [APP: soa-infra] [partition-name: DOMAIN] [tenant-name: GLOBAL] Error while loading process.
```

The process domain is encountering the following errors while loading the process "ApprovalProcess" (composite "default/DefaultRequestApproval!5.0*soa_c9c16746-016e-40c4-aaea-6ccd2d685cb4")

| : BPEL 1.1 compilation failed.  
This error contained an exception thrown by the underlying process loader module.  
Check the exception trace in the log (with logging level set to debug mode).  
If there is a patch installed on the server, verify that the bpelcClasspath domain property includes the patch classes.

Check the SOA composites status from Oracle Enterprise Manager console after successful start of the Oracle Identity Manager Managed Server.

If the Enterprise Manager console shows DefaultRequestApproval!5.0 composite status as actively deployed, ignore this one time error.

If you have upgraded your 11g Release 2 (11.1.2.2.0) environments to 11g Release 2 (11.1.2.3.0), and then to 12c (12.2.1.4.0), you will see the compilation error for DefaultRequestApproval!3.0 composite. This composite was in use in 11g Release 2 (11.1.2.2.0). Before you upgraded to 11.1.2.3.0, this composite processed all of the inflight requests. After upgrading to 11.1.2.3.0, all of the new requests go via DefaultRequestApproval!5.0 composite.

DefaultRequestApproval!3.0 is irrelevant when upgrading from 11.1.2.3.0 to 12c (12.2.1.4.0). Therefore, this compilation error can be ignored.
Warning in Oracle Identity Manager Server Logs After Upgrade

After upgrade, the Oracle Identity Manager (OIM) Server logs show NPE warning, which can be ignored.

After you upgrade Oracle Identity Manager, the following warning is seen in the OIM Server logs for once:

```java
<Warning> <oracle.iam.platform.entitymgr.impl> <BEA-000000> <EntityManagerConfigImpl.getEntityConfig().Can throw NPE with
providerType:
RDBMSChildDataProviderProvider Definition: type: RDBMSChildDataProvider
className:
oracle.iam.platform.entitymgr.provider.rdbms.RDBMSChildDataProvider
m_params:
parent_id_column : name:parent_id_column type:string required:true
multiValued:false id_sequence : name:id_sequence type:string required:false
multiValued:false table : name:table type:string required:true multiValued:false
data_level_column : name:data_level_column type:string required:false
multiValued:false modify_timestamp_column : name:modify_timestamp_column
type:string required:false multiValued:false id_column : name:id_column type:string required:true
multiValued:false optimistic_locking : name:optimistic_locking type:boolean required:true
multiValued:false

 paramName: id_type>
Apr 18, 2017 9:52:54,122 AM PDT> <Warning>
<oracle.iam.platform.entitymgr.impl> <IAM-0040000> <Cannot load entity
definition - java.lang.NullPointerException at
oracle.iam.platform.entitymgr.impl.EntityManagerConfigImpl.getEntityConfig(Ent
ityManagerConfigImpl.java:1164) at
oracle.iam.platform.entitymgr.impl.EntityManagerConfigImpl.getEntityConfig(Ent
ityManagerConfigImpl.java:1242)
```

This warning can be ignored.

Default Challenges Questions are not Updated After Upgrade

After you upgrade Oracle Identity Manager 12c (12.2.1.3.0) to 12c (12.2.1.4.0), the default challenge questions are not updated. It still shows the old or existing challenge questions.

If you are using default password policy with default challenge questions, you must modify them manually post upgrade per your organization needs to have a better security.
EditFailedException When Releasing Configuration From WebLogic Console

After you upgrade Oracle Identity Manager to 12c (12.2.1.4.0), when you click **Release Configuration** on Oracle WebLogic Console, the following error is seen:

```
weblogic.management.provider.EditFailedException: Error loading jdbc/OIMMDS-jdbc.xml
```

This error does not have any functional impact on the WebLogic configuration. To resolve this, open the following DataSource configurations, make any changes, save, and activate the changes:

- ApplicationDB
- mds-oim
- OIMJMSStoreDS
- OIMOperationsDB
- soaOIMLookupDB

OIM Application Deployment Fails Intermittently

After you upgrade Oracle Identity Manager to 12c (12.2.1.4.0), the oim application deployment may fail with the following error:

```
<Error> <Deployer> <BEA-149231> <Unable to set the activation state to true for the application "oim".
weblogic.application.ModuleException: java.lang.NoClassDefFoundError: Could not initialize class oracle.iam.platform.utils.cache.Cache
```

To resolve this, restart the Oracle Identity Manager Server.

Oracle Identity Manager Server Throws OutOfMemoryError

When you start the servers post upgrade, OutOfMemoryError is thrown.

The following error is seen in the OIM server logs for this issue:

```
[oim_server1] [NOTIFICATION] []
[oracle.iam.oimdataproviders.impl] [tid: [ACTIVE].ExecuteThread: '9' for queue: 'weblogic.kernel.Default (self-tuning)'] [userId: xelsysadm] [ecid: 5679ce10-f0df-457f-88f1-6bc04e10a13-000013b1,0] [APP: oim-runtime] [partition-name: DOMAIN] [tenant-name: GLOBAL] [DSID: 0000Lg0PPYTBd5I_Ipt1if1OpGGi00000U] RM_DEBUG_PERF - 2017-03-24 06:09:51.087 - search criteria = arg1 = (usr_key) EQUAL arg2 = (1)[[ query = Select usr.usr_key, usr.usr_status from usr where usr.usr_key = ?
```
LDAP User Create and Update Reconciliation Job Fails

LDAP User Create and Update Reconciliation job fails to run with the following exception:

java.lang.Exception: Full resync required. Reason: The provided cookie is older than the start of historical in the server for the replicated domain : dc=us,dc=oracle,dc=com

To resolve this issue, you must update the parameter Last Change Number of the job. To do this, complete the following steps:

1. Get the value from Oracle Unified Directory using the following command:
   
   ```
   ./ldapsearch -h <OUDHOST> -p 1389 -D "cn=oudadmin" -w Fusionapps1 --control "1.3.6.1.4.1.26027.1.5.4:false;" -b "cn=changelog" "(objectclass=*)" *** +
   ```

2. Search for the following line in the output of the above command:
changeLogCookie: dc=us,dc=oracle,dc=com:0000015dcefd65a3000100000102;

3. Fill in dc=us,dc=oracle,dc=com:0000015dcefd65a3000100000102; in to the Last Change Number parameter of the job.

BI Managed Server is Seen on WebLogic Console After Upgrade

If your 12c domain had a custom name for BI Managed Server, that is, the name other than bi_server1, then this Managed Server will not be deleted during the upgrade.

Post upgrade, the BI managed server lying in Oracle Identity Governance domain is of no use. You can delete this BI server manually by doing the following:

1. Log in to the WebLogic Administration Console using the following URL:

   http://weblogic_admin_host:weblogic_admin_port/console

2. Click Environments on the left navigation pane.

3. Click Servers.

4. Select the check box against BI Managed Server, and click Delete.

Empty Pages or Panels After Upgrade

After you complete the upgrade, the Applications tile in the OIM Self Service console and the Import/Export links in the Admin console may be rendered as empty pages or panels.

This can occur if the following URIs are being filtered by a proxy:

- /OIGUI/
- /FacadeWebApp/
- /iam/

To avoid this issue, update your proxy rules to allow access to these URIs.
Updating the JDK After Installing and Configuring an Oracle Fusion Middleware Product

Consider that you have a JDK version jdk1.8.0_191 installed on your machine. When you install and configure an Oracle Fusion Middleware product, the utilities, such as Configuration Wizard (config.sh|exe), OPatch, or RCU point to a default JDK, for example, jdk1.8.0_191. After some time, Oracle releases a new version of the JDK, say jdk1.8.0_211 that carries security enhancements and bug fixes. From 12c (12.2.1.4.0) onwards, you can upgrade the existing JDK to a newer version, and can have the complete product stack point to the newer version of the JDK.

You can maintain multiple versions of JDK and switch to the required version on need basis.

• About Updating the JDK Location After Installing an Oracle Fusion Middleware Product

The binaries and other metadata and utility scripts in the Oracle home and Domain home, such as RCU or Configuration Wizard, use a JDK version that was used while installing the software and continue to refer to the same version of the JDK. The JDK path is stored in a variable called JAVA_HOME which is centrally located in .globalEnv.properties file inside the ORACLE_HOME/oui directory.

About Updating the JDK Location After Installing an Oracle Fusion Middleware Product

The binaries and other metadata and utility scripts in the Oracle home and Domain home, such as RCU or Configuration Wizard, use a JDK version that was used while installing the software and continue to refer to the same version of the JDK. The JDK path is stored in a variable called JAVA_HOME which is centrally located in .globalEnv.properties file inside the ORACLE_HOME/oui directory.

The utility scripts such as config.sh|cmd, launch.sh, or opatch reside in the ORACLE_HOME, and when you invoke them, they refer to the JAVA_HOME variable located in .globalEnv.properties file. To point these scripts and utilities to the newer version of JDK, you must update the value of the JAVA_HOME variable in the .globalEnv.properties file by following the directions listed in Updating the JDK Location in an Existing Oracle Home.

To make the scripts and files in your Domain home directory point to the newer version of the JDK, you can follow one of the following approaches:

• Specify the path to the newer JDK on the Domain Mode and JDK screen while running the Configuration Wizard.

For example, consider that you installed Oracle Fusion Middleware Infrastructure with the JDK version 8u191. So while configuring the WebLogic domain with the Configuration Assistant, you can select the path to the newer JDK on the Domain
Mode and JDK screen of the Configuration Wizard. Example: /scratch/jdk/jdk1.8.0_211.

- Manually locate the files that have references to the JDK using `grep` (UNIX) or `findstr` (Windows) commands and update each reference. See Updating the JDK Location in an Existing Oracle Home.

Note: If you install the newer version of the JDK in the same location as the existing JDK by overwriting the files, then you don’t need to take any action.

- Updating the JDK Location in an Existing Oracle Home
  The `getProperty.sh|cmd` script displays the value of a variable, such as `JAVA_HOME`, from the `.globalEnv.properties` file. The `setProperty.sh|cmd` script is used to set the value of variables, such as `OLD_JAVA_HOME` or `JAVA_HOME` that contain the locations of old and new JDKs in the `.globalEnv.properties` file.

- Updating the JDK Location in an Existing Domain Home
  You must search the references to the current JDK, for example 1.8.0_191 manually, and replace those instances with the location of the new JDK.

Updating the JDK Location in an Existing Oracle Home

The `getProperty.sh|cmd` script displays the value of a variable, such as `JAVA_HOME`, from the `.globalEnv.properties` file. The `setProperty.sh|cmd` script is used to set the value of variables, such as `OLD_JAVA_HOME` or `JAVA_HOME` that contain the locations of old and new JDKs in the `.globalEnv.properties` file.

The `getProperty.sh|cmd` and `setProperty.sh|cmd` scripts are located in the following location:

(UNIX) `ORACLE_HOME/oui/bin`
(Windows) `ORACLE_HOME\oui\bin`

Where, `ORACLE_HOME` is the directory that contains the products using the current version of the JDK, such as 1.8.0_191.

To update the JDK location in the `.globalEnv.properties` file:

1. Use the `getProperty.sh|cmd` script to display the path of the current JDK from the `JAVA_HOME` variable. For example:

   (UNIX) `ORACLE_HOME/oui/bin/getProperty.sh JAVA_HOME`
   (Windows) `ORACLE_HOME\oui\bin\getProperty.cmd JAVA_HOME`
   `echo JAVA_HOME`

   Where `JAVA_HOME` is the variable in the `.globalEnv.properties` file that contains the location of the JDK.

2. Back up the path of the current JDK to another variable such as `OLD_JAVA_HOME` in the `.globalEnv.properties` file by entering the following commands:

   (UNIX) `ORACLE_HOME/oui/bin/setProperty.sh -name OLD_JAVA_HOME -value specify_the_path_of_current_JDK`
   (Windows) `ORACLE_HOME\oui\bin\setProperty.cmd -name OLD_JAVA_HOME -value specify_the_path_of_current_JDK`
This command creates a new variable called OLD_JAVA_HOME in the .globalEnv.properties file, with a value that you have specified.

3. Set the new location of the JDK in the JAVA_HOME variable of the .globalEnv.properties file, by entering the following commands:

   (UNIX) `ORACLE_HOME/oui/bin/setProperty.sh -name JAVA_HOME -value specify_the_location_of_new_JDK`
   (Windows) `ORACLE_HOME\oui\bin\setProperty.cmd -name JAVA_HOME -value specify_the_location_of_new_JDK`

   After you run this command, the JAVA_HOME variable in the .globalEnv.properties file now contains the path to the new JDK, such as jdk1.8.0_211.

### Updating the JDK Location in an Existing Domain Home

You must search the references to the current JDK, for example 1.8.0_191 manually, and replace those instances with the location of the new JDK.

You can use the `grep` (UNIX) or `findstr` (Windows) commands to search for the jdk-related references.

You'll likely be required to update the location of JDK in the following three files:

   (UNIX) `DOMAIN_HOME/bin/setNMJavaHome.sh`
   (Windows) `DOMAIN_HOME\bin\setNMJavaHome.cmd`

   (UNIX) `DOMAIN_HOME/nodemanager/nodemanager.properties`
   (Windows) `DOMAIN_HOME\nodemanager\nodemanager.properties`

   (UNIX) `DOMAIN_HOME/bin/setDomainEnv.sh`
   (Windows) `DOMAIN_HOME\bin\setDomainEnv.cmd`