Oracle® Fusion Middleware

Oracle Identity and Access Management Upgrade Strategies

ORACLE®

Oracle Fusion Middleware Oracle Identity and Access Management Upgrade Strategies,

F33537-04

Contents

Preface

1   About Upgrade Strategies

2   In-Place Upgrade

3   Out-of-Place Upgrade

4   Out-of-Place Cloned Upgrade

A   Additional Information

Preface

This document discusses the recommended upgrade strategies for upgrading Oracle Identity and Access Management, Oracle Internet Directory, and Oracle Unified Directory software.

- Audience
- Documentation Accessibility

Audience

In general, this document is intended for the users of Oracle Fusion Middleware, who need to know different upgrade strategies available for the Oracle Identity and Access Management, Oracle Internet Directory, and Oracle Unified Directory software.

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.

1
About Upgrade Strategies

An Oracle Identity and Access Management deployment consists of a number of different components:

- A database
- An LDAP directory to store user information
- Oracle Access Manager for Authentication
- Oracle Identity Governance (formally Oracle Identity Manager) for provisioning
- Optionally, Oracle HTTP Server and Webgate securing access to Oracle Access Manager and Oracle Identity Governance

There are different upgrade strategies that you can employ for an upgrade of Oracle Internet Directory, Oracle Unified Directory, and Oracle Identity and Access Management. The strategy you choose will depend mainly on your business needs.

> **Note:**
>
> This guide provides you a high-level introduction to the different upgrade strategies. For detailed upgrade steps, see the component-specific upgrade guide for the release you want to upgrade.

This chapter includes the following topics:

- About the In-Place Upgrade Strategy
- About the Out-of-Place Upgrade Strategy
- About the Out-of-Place Upgrade Strategy via Cloning
- Assumptions

About the In-Place Upgrade Strategy

The in-place upgrade allows you to take your existing deployment and upgrade it in situ.

When performing an upgrade, you should make as few changes as possible in each stage to ensure that the upgrade is successful.

For example, it is not recommended to perform multiple upgrade activities such as upgrading Oracle Identity and Access Management, changing the directory, updating the operating system, and so on, all at the same time.

If you want to perform such an upgrade, you must do it in stages. You must validate each stage before moving on to the next. The benefit of this approach is that it helps you to identify precisely where the issue occurred, and correct it or undo it before you continue the exercise.

Following are the topics covered in this section:

- Performing an In-Place Upgrade
- Advantages and Disadvantages of an In-Place Upgrade
- When is In-Place Upgrade Recommended?

Performing an In-Place Upgrade

The in-place upgrade process is similar across all products.

To perform an in-place upgrade:

1. Take a backup of your existing environment.
2. Create a new binary installation.
3. Apply the pre-upgrade patches, if any, to the binaries.
4. Upgrade database objects.
5. Reconfigure the Domain.
6. Re-apply any customizations.
7. Start the component using the new version.
8. Take a backup on the new environment.

Advantages and Disadvantages of an In-Place Upgrade

Following table lists the advantages and disadvantages of an in-place upgrade:

Table 1-1   Advantages and Disadvantages of an In-Place Upgrade

Advantages	Disadvantages
• Lets you perform the upgrade on your existing hardware and requires no additional hardware. • Is highly automated and simplified. • Reduced work compared to other strategies. • Maintains the historical data. • Maintains the existing passwords, policies, and questions/answers. • Ensures no gaps in data. • Requires no reconfiguration of external resources such as DNS or load balancers. • Requires no reconfiguration of external dependencies and other systems utilizing the Identity Management functionality.	• Requires downtime. • Requires reapplication of customizations that may be lost. • Requires you to perform an upgrade more than once if upgrading through multiple versions. • Some components may not work well together in different versions. For example: OHS 12c does not work well with OAM 11g without modifications. • If any issues are encountered, the actual downtime may be higher than the planned downtime.

When is In-Place Upgrade Recommended?

Following scenarios are suitable for an in-place upgrade:

- Single instance deployments.

- Deployments with no or very few customizations.

- Resource constrained deployments (if you have the hardware limitations).

- Non-integrated (loosely connected) environments.

About the Out-of-Place Upgrade Strategy

An out-of-place upgrade creates a second environment on a different hardware at the release you want to go to, and then migrates your data and configuration from your existing system to the new system.

After you migrate data and validate that the new system is working, you switch to the new system, and decommission the existing system.

Following topics are covered in this section:

- Performing an Out-of-Place Upgrade

- Advantages and Disadvantages of an Out-of-Place Upgrade

- When is Out-of-Place Upgrade Recommended?

Performing an Out-of-Place Upgrade

The out-of-place upgrade process is similar across all products.

To perform an out-of-place upgrade:

1. Install your target version of Oracle Identity Management on new hardware.

2. Configure the new system by integrating components as necessary.

3. Apply customizations to the new environment.

4. Export your data from the existing system.

5. Load your data into the new system.

6. Verify the new system.

7. Take a backup on the new environment.

8. Switch over to the new system.

Advantages and Disadvantages of an Out-of-Place Upgrade

Following table lists the advantages and disadvantages of an out-of-place upgrade:

Table 1-2   Advantages and Disadvantages of an Out-of-Place Upgrade

Advantages	Disadvantages

• Reduced downtime.
• Lower risk.
• Upgrade many components at the same time.
• Change the topology.
• Change the architecture.
  For example: Moving from Oracle RAC to Exadata.
• Clean data if required.
• Create customizations ahead of time.
• Update UI or customizations.
• Useful for customers requiring major changes to their system.
• Run old and new system in parallel.
• Resolve issues without affecting production.
	• Requires extra hardware/resources.
	• If you plan to run the new and existing system in parallel, existing external resources will require configuration changes to use the new system.
	  For example: The IDM agents such as webgates which can only point to one system at a time, or OIM reconciling from two different LDAP directories. If you run these systems in parallel, you will have to manually enter details into both systems in parallel until cutover.
	• If you do not run the old and new systems in parallel, existing resources such as DNS and load balancers will need to be reconfigured to use the new environment.
	• If you build the new system ahead of time and transfer the data, then you need a mechanism to keep the data in both systems in sync, until cut over.
	• Time to unload or load data can be significant depending on data volume.

When is Out-of-Place Upgrade Recommended?

Following scenarios are suitable for an out-of-place upgrade:

- Complex installations with many customizations.

- Complex HA installations that are tightly coupled.

- When you want to run an old and new system in parallel.

About the Out-of-Place Upgrade Strategy via Cloning

Upgrading via a cloned environment is a hybrid approach that involves cloning the existing system to a new set of hardware, and then performing an in-place upgrade on the cloned system. This approach can also be used to test the upgrade in a safe environment before doing it on your production environment.

Following are the topics covered in this section:

- Performing an Upgrade via a Cloned Environment

- Advantages and Disadvantages of Upgrading via a Cloned Environment

- Alternatives to Upgrading via a Cloned Environment

Performing an Upgrade via a Cloned Environment

If something goes wrong during the upgrade of your existing deployment, you have to restore that deployment to the point it was prior to beginning the upgrade. An alternative approach is to take a copy of your existing environment, and then upgrade that. If something goes wrong, you have your existing environment as a fallback.

- Host Names
- Cloning the Database
- Cloning the Binaries
- Cloning the Configuration
- Upgrading the Domain

Host Names

The simplest method of cloning involves making no changes to the deployment itself. The easiest way of achieving this is to ensure that your hostnames and site URLs remain unchanged during the cloning process. This process follows the same approach as Oracle recommends for Disaster recovery. Ideally you will have configured your source environment using virtual host names rather than physical host names. For example, `oamhost1` rather than `physhost1`. If you have done this, then when cloning you just add the virtual hostname as an alias of the physical hostname. However, if your source environment has not been configured to use virtual hostnames, then you can can still use the same approach by aliasing your source environment's physical hostname in your target environment.

For example, the goal is to have `oamhost1` resolvable in both your source and target environments but each resolving to an IP address appropriate to the environment you are working. If you do this, then you need make no configuration changes to your clone. If you must change the host names then this can still be achieved but the cloning process becomes more complex and requires you to reconfigure the clone.

Cloning the Database

The following methods are available to clone the database you use to host your application:

Option 1- Database Export Import

See Moving Data Using Data Pump and Export/Import.

Option 2 – Duplicate Database using RMAN

See Database Duplication.

Option 3 – Dataguard Database

See Data Guard Concepts and Administration.

The following table lists the advantages of above three options discussed:

Table 1-3   Advantages of using each method of cloning the database

Option 1	Option 2	Option 3
• Suitable for smaller sized databases. • Allows movement between versions. For example, 12.1.0.3 to 19c. • Allows movement into container databases / private databases. • Is a complete copy. Redoing the exercise requires data to be deleted from the target each time. • No on-going synchronization. • During cut-over, the source system will need to be frozen for updates.	• Suitable for any size of database. • Takes a backup of an entire database. • Database upgrades will need to be performed as a separate task • CDB/PDB migration will have to be done after restoring. • No ongoing synchronization. • During cut-over, the source system will need to be frozen for updates.	• Suitable for any size of database. • Takes a backup of an entire database. • Database upgrades will need to be performed as a separate task • CDP/PDB migration will have to be done as a separate exercise.

Cloning the Binaries

The Oracle binaries must be identical on both the source and target systems. They must be at the same patch level and in the same locations.

Following methods are available to achieve this:

Backup/Restore - Use your preferred backup tool to back up the existing binary installation and restore it to the target system. Do not forget to include the `oraInventory` directory.

T2P- If your source environment is an 11g environment, you can use the Oracle Test to Production utility to replicate the binaries to a different set of hosts. For more information, see Moving from a Test to a Production Environment and Using the Movement Scripts in the *Fusion Middleware Administrator's Guide*.

Reinstallation- If you are confident you know all the patches and versions contained in your binary installation, then you can manually install them on your target system. For more information, see the *Installing and Configuring Oracle Identity Management Guide* for the release you are installing.

> ✏️ **Note:**
>
> If you install your binaries locally, ensure that you do the same on your target system. If you use shared storage, then you only need to do the restore once to each shared storage location including any redundant copies you may have.

Chapter 1
About the Out-of-Place Upgrade Strategy via Cloning

Cloning the Configuration

If you have kept your hostnames in sync across the source and target sites, then you can perform a simple backup and restore using your favourite backup and restore tool.

If your source environment is 11g, you can use the T2P utility to clone the configuration. This approach is more complex than a simple backup/restore, but it lets you change some values such as host names.

For more information, see Moving from a Test to a Production Environment and Using the Movement Scripts in the *Fusion Middleware Administrator's Guide*.

OIM also has a utility, which allows you to manually change the hostnames. For more information, see Doc ID 2621548.1.

Upgrading the Domain

After cloning your installation, you can start upgrading the domain using the in-place instructions.

Advantages and Disadvantages of Upgrading via a Cloned Environment

Following table lists the advantages and disadvantages of upgrading via a cloned environment:

Table 1-4   Advantages and Disadvantages of upgrading via a cloned environment

Advantages	Disadvantages
• Reduced downtime. • Lower risk. • Upgrade many components at the same time. • Retain historical data. • Reapply customizations ahead of time. • Migrate to different hardware + (optionally, with newer OS levels). • Do not have to reconfigure external dependent systems. • Use it as a testing ground to get familiar with and validate the procedure before doing it for real as part of an in-place upgrade. • Use it for practising the upgrade if used in a test environment. • Learn about the time taken to perform the upgrade if used in a test environment. • Uncover and provide solutions for any unexpected upgrade issues if used in a test environment.	• Upgrading via a cloned environment requires extra hardware and resources. • The new system must use the same host names and load balancer virtual hosts. • Because the names are the same (unless you used virtual names), you cannot run both systems side by side • Requires the reconfiguration of external resources (DNS/load balancers) to point to the new system when it is available. • If you build the new system ahead of time and transfer the data, then you need a mechanism to keep the data in both systems in sync until the cut over. **✎ Note:** Oracle recommends you to upgrade via a cloned environment only when you have to upgrade multiple components at a time, and have a ready-made fall back.

Alternatives to Upgrading via a Cloned Environment

Following are some alternatives you can use instead of upgrading via a cloned environment:

• If you have a Disaster Recovery (DR) system, you can upgrade the DR system instead of a clone.

• If you are using Oracle Unified Directory (OUD), you can create a replica of the existing site's Oracle Unified Directory instances using Oracle Unified Directory replication, and then upgrade the replica.

• If you are using Oracle Internet Directory (OID), you can create a replica of the existing Oracle Internet Directory using OID replication, and then upgrade the replica.

> **✎ Note:**
>
> If you follow this mechanism when using OIG and OID, you will have to perform a full reconciliation on the new system before use.

- If you are using Oracle Access Manager, you can create a second deployment of Oracle Access Manager and synchronize it with the first using Oracle Access Manager Multi-Data Center technologies, and then upgrade the second site.

Assumptions

Following assumptions are applicable irrespective of which upgrade strategy you adopt:

- Each component directory, OAM, OIG, and Web Tier have dedicated binaries. This allows each product to be upgraded individually.

- Each component requiring a WebLogic domain (OAM, OIG, ODSM, Adaptive Access Manager etc.) has a dedicated domain. For example, Oracle Access Manager and Oracle Identity Governance are in different domains. This allows each product to be upgraded individually.

> **Note:**
>
> If you are upgrading more than one component, you should first upgrade Oracle Internet Directory, Oracle Access Manager, upgrade the Oracle Identity Governance, and then do the reconfiguration.

2

In-Place Upgrade

This chapter contains information about the in-place upgrade strategies for Oracle Internet Directory, Oracle Unified Directory, and Oracle Identity and Access Management.

This chapter includes the following topics:

In-Place Upgrade of Oracle Internet Directory (OID)

Before you begin, review all introductory information to understand the upgrade paths and process for Oracle Internet Directory 12c.

This section describes how to upgrade Oracle Internet Directory 11g Release 2 to 12c.

For intructions, see *Upgrading Oracle Internet Directory* for the release you want to upgrade.

In-Place Upgrade of Oracle Unified Directory (OUD)

You can upgrade an OUD service to the latest version without any service interruption.

This section describes the in-place upgrade of OUD 11g Release 2 to 12c. It also describes how to update an individual directory server instance and provides considerations for upgrading OUD Services Manager on Oracle Weblogic Server.

For instructions, see *Installing Oracle Unified Directory* for the release you want to upgrade.

In-Place Upgrade of Oracle Identity Manager (OIM)

This section describes the in-place upgrade of OIM 11g Release 2 to 12c.

For instructions, see *Upgrading Oracle Identity Manager* for the release you want to upgrade.

In-Place Upgrade of Oracle Access Manager (OAM)

Before you begin, review all introductory information to understand the standard upgrade topologies and upgrade paths for OAM 12c.

This section describes the in-place upgrade of OAM 11g (11.1.2.3) to 12c.

If your domain contains other components, you will have to upgrade those components as well.

For instructions, see *Upgrading Oracle Access Manager* for the release you want to upgrade.

In-Place Upgrade of Oracle HTTP Server (OHS)

Before you begin, review all introductory information to understand the standard upgrade topologies and upgrade paths for OHS 12c.

This section describes the in-place upgrade of OHS 11g (11.1.2.3) to 12c.

For instructions, see *Upgrading Oracle HTTP Server* for the release you are upgrading.

For details about OHS/OTD WebGate upgrade, see *Installing WebGates for Oracle Access Manager* for the release you want to upgrade.

3
Out-of-Place Upgrade

An out-of-place upgrade is described as creating a new system and migrating the data from your existing system to the new system.

The new system may have different host names and different application URLs.

This chapter contains information about the out-of-place upgrade strategies for Oracle Identity Management, Oracle Internet Directory, and Oracle Unified Directory.

The sections below show the high level steps to perform an out-of-place upgrade. For detailed instructions, see the product-specific upgrade guides for the version you are upgrading.

This chapter includes the following topics:

- Planning the Out-of-Place Upgrade
- Out-of-Place Upgrade Considerations
- Performing an Out-of-Place Upgrade of Oracle Internet Directory
- Performing an Out-of-Place Upgrade of Oracle Unified Directory
- Out-of-Place Upgrade of Oracle Access Manager
- Performing an Out-of-Place Upgrade of Oracle Identity Manager
- Performing an Out-of-Place Upgrade of Oracle HTTP Server
- Interfaces

Planning the Out-of-Place Upgrade

Before you start the out-of-place upgrade of OIG, OAM, OID, or OUD, you must do the following:

- Verify that you are running the supported hardware and software versions. For more information, see Oracle Fusion Middleware 12c Certifications.
- Ensure that the database and JDK versions are up-to-date. You must have the latest JDK version installed in the source environment. For more information, see Oracle Fusion Middleware 12c Certifications.
- Upgrade timelines and resources should also factor in topology complexities such as high availability configuration, SSL, firewalls, and so on.
- Ensure that the upgrade does not compromise functionalities such as OAM Administration console, OAM SSO login, Identity Federation SSO, session management, custom OAM authentication plug-in, OAM custom page configurations (login, error, logout), Custom API solutions, and performance.
- Plan for system downtime during the upgrade process.

Out-of-Place Upgrade Considerations

When performing an out-of-place upgrade, you are creating an entirely new system based on existing data. You may choose to keep your existing application URLs, or create new ones. If you choose to have the same URLs, then migrating your existing system interfaces will be easier. However having different URLs means that you can run both your installations in parallel and can phase your cutover.

Because you have an entirely new system, you will have different host names. As a best practice, Oracle recommends that you use virtual host names rather than physical host names. Using virtual host names makes it easier for disaster recovery, transportability, and deployment into virtual environments.

Performing an Out-of-Place Upgrade of Oracle Internet Directory

When using an out-of-place upgrade of Oracle Internet Directory, it is possible to perform the upgrade in one step. You can have a source system based on OID 11g (11.1.1.9), export the data from it, and import it directly into OID 12c.

To perform an out-of-place upgrade of OID:

1. Complete the pre-upgrade assessment check to ensure the environment is ready for an upgrade.

2. Install OID 12c in your target environment.

3. Place the source directory in read-only mode.

4. Export the data from the existing directory to an LDIF file.

5. Perform a bulk load of the data from the LDIF file.

   You new directory is now available for use.

6. Validate that OID is functioning correctly using in-house tests.

> ✏️ **Note:**
>
> Complete these steps as a one-time operation. There is no ongoing data synchronization, at this time.

For instructions, see *Upgrading Oracle Internet Directory* for the release you want to upgrade.

Performing an Out-of-Place Upgrade of Oracle Unified Directory

When using an out-of-place upgrade of Oracle Unified Directory, it is possible to perform the upgrade in one step. You can have a source system based on OUD 11g (11.1.2.3), export the data from it, and import it directly into OUD 12c.

To perform an out-of-place upgrade of OUD:

1. Install OUD 12c in your target environment.

2. Create a replication agreement between your source system and the destination system. OUD supports replication across releases.

3. Create any indexes on your destination system that are not covered in the replication.

4. Create any global ACIs on your destination system that are not covered in the replication.

   You new directory is now available for use and changes made on the source system will continue to be propagated to the destination system.

5. Validate that OUD is functioning correctly using in-house tests.

6. When ready for cutover, remove the source directory from the replication agreement.

> **Note:**
>
> The OUD replication does not replicate global ACIs or local indexes, so these need to be created manually.

Out-of-Place Upgrade of Oracle Access Manager

Oracle does not support an out-of-place upgrade for Oracle Access Manager. Oracle recommends that you perform an out-of-place upgrades of Oracle Access Manager using the cloned approach. For instructions, see *Upgrading Oracle Access Manager* for the release you want to upgrade.

Performing an Out-of-Place Upgrade of Oracle Identity Manager

When using an out-of-place upgrade of Oracle Identity Manager (Oracle Identity Governance) it is possible to perform the upgrade in one step. That is to say, you can have a source system based on OIM 11g (11.1.2.3), export the data from it, and import it directly into OIG 12c.

To perform an out-of-place upgrade of OIG:

1. Complete the pre-upgrade assessment check to ensure the environment is ready for an upgrade.

2. Install Oracle Identity Governance 12c in your target environment.

3. Migrate your Data from 11g to 12c. Data migration includes: Organizations, Connectors, Accounts, Roles, Users, and Customizations.

4. Tune the database / Application Server

5. Validate your installation including, interactions with Dependent Directories, Oracle Access Manager (if used), and any other connected systems.

For instructions, see *Upgrading Oracle Identity Manager* for the release you want to upgrade.

- Migration Considerations
  After you have installed the OIG 12c environment as per your requirements, migrate the following entities from 11g to 12c environment:

- Tuning Considerations

Migration Considerations

After you have installed the OIG 12c environment as per your requirements, migrate the following entities from 11g to 12c environment:

- Organizations

- Connectors

- Accounts

- Roles (Role, Role Membership, and Categories)

- User Records

- User Customizations

- Others

Organizations

Following options are available to migrate Organization records from the current OIM 11g (11.1.2.3) environment to 12c:

Option 1- Organization Bulk Load Utility

This option involves creating a source database table or a CSV file that contains the data you want to migrate.

For more information on using CSV files or creating database tables, see Creating the Input Source for the Bulk Load Operation in *Developing and Customizing Applications for Oracle Identity Governance*.

Option 2- Export And Import Feature In Sysadmin Console

After you have created your source data, you need to import the source data into the new 12c target system. For more information, see Migrating Incrementally Using the Deployment Manager.

Connectors

You should review the latest version of the connector available for 12c and use Application on Boarding (AoB) to create such connectors.

A new installation enables you to upgrade your targets to newer versions that are certified with 12c connectors.

If 12c connectors are not available, you can export or import existing user data as long as those connectors are supported in the 12c OIM server.

For more information, see Oracle Identity Governance 12c Connectors documentation.

For downloading connectors, see the Oracle Identity Governance Connector Downloads page.

For certification information for Oracle Identity Manager Connectors, see Oracle Identity Governance Connectors Certification.

> **Note:**
>
> If the connectors installed on 11g (11.1.2.3) have no 12c version, you must check the certification, and then upgrade the existing connector to make it compatible with OIG 12c.

Accounts

After you set up the connectors as applications, you should start loading the account data from the target systems.

> **Note:**
>
> Target systems are applications such as database, LDAP, and so on, which OIM connects to using the OIM connectors.

Following options are available to load your accounts:

*   **Option 1**: If the target system has account data, you can bulk load the account details (or data) by using the Bulk Load Utility. See Loading Account Data in *Developing and Customizing Applications for Oracle Identity Governance* guide.

*   **Option 2**: You can load the target system account data into the new environment by using connector the reconciliation jobs.

Roles (Role, Role Membership, and Categories)

You can use the OIM Bulk Load Utility to import roles, role membership, and categories from a table or a CSV file. Export the relevant data files from the source OIM database.

For information on how to export and import this data, see Loading Role, Role Hierarchy, Role Membership, and Role Category Data in *Developing and Customizing Applications for Oracle Identity Governance*.

User Records

Following options are available to migrate user records from current OIM 11g (11.1.2.3) environment to 12c:

Option 1 - User Bulk Load Utility

This option includes exporting the user records to a table or a CSV file that will act as a source. See Loading OIM User Data in *Developing and Customizing Applications for Oracle Identity Governance* guide.

Option 2- Trusted Recon of Users from 11g to 12c

This option includes using the Database User Management (DBUM) connector or a flat file connector to migrate the user records.

> **Note:**
>
> You cannot migrate user passwords by using the above options. You can set up SSO or LDAP as an authentication provider.

User Customizations

If you have added the custom User Defined Fields (UDF) in OIM 11g (11.1.2.3), you must create those UDFs in 12c as well.

> **WARNING:**
>
> Oracle does not support UDF migration (Deployment Manager and ADF Sandboxes).

> **Note:**
>
> To check if import or export from 11g (11.1.2.3) to 12c works, export the user metadata from the 11g (11.1.2.3) environment and import it to 12c, get the corresponding ADF sandbox, and then import it to 12c.

Others

You can also migrate the following items from your 11g (11.1.2.3) environmen to 12c environment by using the Export/Import option in the sysadmin console:

- Access policies
- Admin roles
- Application instances
- Approval policies
- Catalog UDFs
- Certification configurations
- Certification definitions
- Custom resource bundles
- E-mail definitions
- Error codes
- Event handlers

- Identity Audit configuration
- Identity Audit rules
- Identity Audit scan definitions
- IT resource definition
- IT resources
- JAR files
- Lookup definitions
- Notification templates
- Organization metadata
- Organizations
- Password policies
- Policies
- Plug-ins
- Prepopulation adapters
- Process definitions
- Process forms
- Provisioning workflows and process task adapters
- Request datasets
- Resource objects
- Risk configuration
- Role metadata
- Roles
- Scheduled jobs
- Scheduled tasks
- System properties
- User metadata

For more information, see Moving from a Test to a Production Environment and Using the Movement Scripts in the *Fusion Middleware Administrator's Guide*.

Tuning Considerations

As a post-upgrade step, you must follow the performance tuning guidelines provided in the tuning documentation. See Oracle Identity Governance Performance Tuning.

Also, you should check the existing 11g (11.1.2.3) system for custom indexes and create them in the 12c system.

Performing an Out-of-Place Upgrade of Oracle HTTP Server

You can perform an out-of-place upgrade of Oracle HTTP Server in one step. Export the configuration from the source system that is based on OHS 11g (11.1.2.3) and import it directly into the OHS 12c (12.2.1.4).

To perform an out-of-place upgrade of OHS:

1. Install Oracle HTTP Server 12.2.1.4 in your target environment.
2. Migrate your configuration from the source environment to the destination environment.
3. Disable Webgate.
4. Validate the configuration using in-house tests.
5. Copy the 12c Webgate Artifacts from your OAM 12c deployment to your Oracle HTTP 12c server installation.
6. Enable Webgate.
7. Validate your installation using in-house tests.

> **Note:**
>
> Oracle HTTP Server 12c comes with an embedded webgate. This webgate will not work out-of-the box with Oracle Access Manager 11g. It is possible to make it work but it is recommended that you do not enable Webgate until you have upgraded to Oracle Access Manager 12c. If you are using an SSL enabled Oracle HTTP server, you will need to either create a new certificate or copy your existing certificate to the new Oracle HTTP installation.

Interfaces

If you have any external applications, which interact with Oracle Identity Manager, then you need to ensure that they work with the new installation. This may include:

- Changing URLs if your URLs have changed.
- Upgrading any third party agents, if you are using any. For example, BIG-IP.
- Changing any load balancers/DNS servers to point to the new application.

4

Out-of-Place Cloned Upgrade

An out-of-place cloned upgrade is described as creating a copy of your existing system on new hardware, and then performing an in-place upgrade on the clone.

This chapter includes the following topics:

- Considerations for an Out-of-Place Cloned Upgrade
- Performing an Out-of-Place Cloned Upgrade of Oracle Internet Directory
- Performing an Out-of-Place Cloned Upgrade of Oracle Unified Directory
- Performing an Out-of-Place Cloned Upgrade of Oracle Access Manager
- Performing an Out-of-Place Cloned Upgrade of Oracle Identity Manager
- Performing an Out-of-Place Cloned Upgrade of Oracle HTTP Server

Considerations for an Out-of-Place Cloned Upgrade

This section lists the consideration for an out-of-place cloned upgrade:

- Symmetry
- Load Balancer
- Databases
- Cloning Application Binaries
- Cloning Configuration Information
- Separate Domains

Symmetry

It is recommended that the cloned environment be identical to the source environment. The less you change, the less you have to re-configure during the cloning process.

This includes the following:

- **Application URLS** – If you access your application using `login.example.com`, then your cloned environment should use `login.example.com` as well.
- **Host Names** – Host names should be identical on both the source and clone. As a best practice, Oracle recommends to use virtual host names rather than physical hostnames. For example, instead of using `mhost.example.com`, you use `OAMHOST1.example.com`. If you are using virtual host names, then simply alias those to the physical host names in your local hosts file. If you are not using virtual host names, then the same can be achieved by aliasing your source physical host names to your cloned host name in your local hosts file.

  This will include database as well as middle ware host names.

Whilst this is the desired approach, which ensures that no reconfiguration is required using the cloning process it is possible to change host names, if required. But, this adds complexity to the solution.

- **File System Paths**– File system paths should be identical on both your source and primary systems.

Load Balancer

In a high availability configuration, Oracle Identity and Access Management will reside behind an Oracle HTTP server,which will be used to route requests to the Oracle Weblogic components. Access to the Oracle HTTP servers will be through a load balancer. In an Out of Place cloned environment, you can either utilise your existing Load Balancer or use a different one. If you are using a different load balancer, then you will need to ensure that you copy your SSL certificates across.

Databases

The strategy involves cloning your database objects from the source system to the destination system. There are multiple ways of cloning a database and each has its merits.

> **Note:**
>
> Oracle Identity and Access Management 12c does not support Oracle Access Manager and Oracle Identity Manager configured to use the same database schema prefix. Before you upgrade, if both products co-exist and share the same database schemas, you must first split the database into two different prefixes and schema sets.

You can use the following options to clone the database:

Option 1 – Database Export Import

- Suitable for smaller sized databases.
- Allows movement between versions. For example, 12.1.0.3 to 19c.
- Allows movement into Container Databases/Private Databases.
- Is a complete copy; redoing the exercise requires data to be deleted from the target each time.
- No ongoing synchronization.
- During cut-over the source system will need to be frozen for updates.

Option 2 – Duplicate Database using RMAN

- Suitable for databases of any size.
- Takes a back up of an entire database.
- The database version and patch level should be the same on both the source and destination.
- Database upgrades will need to be performed as a separate task.

- CDP/PDB migration will have to be done as a separate exercise.

- No ongoing synchronization.

- During cut-over, you should freeze the source system for updates.

Option 3 – Dataguard Database

- Suitable for databases of any size.

- Takes a back up of an entire database.

- Database upgrades will need to be performed as a separate task.

- CDP/PDB migration will have to be done as a separate exercise.

- Ongoing synchronisation; Database can be opened to test the upgrade and closed again to keep data synchronized with the source system.

> **Note:**
>
> You should choose the solution based on your requirements.

Cloning Application Binaries

Your source and destination systems must have identical binary installations with the same patches installed on both systems. There are several mechanisms that can be used to clone the application binaries:

- **Backup/Restore** – You can use a backup and restore tool of your choice to copy the middleware homes from the source to the target system.

- **T2P** – If your source environment is 11g, you can use the Oracle Test to Production utility (T2P) to copy the middleware homes from the source to the target system.

- **Manual Install** – If you are certain of the binary installation contents, then you can perform a manual installation/patch application on the destination system.

> **Note:**
>
> You should choose an option based on your requirements. Oracle recommends that you choose the first option to ensure that both systems are identical.

Cloning Configuration Information

Your source and destination systems must have an identical configuration. There are two mechanisms that can be used to clone the configuration information:

- **Backup/Restore** – You can use your preferred backup and restore tool to copy the domain/instance configuration from the source to the target system. This will ensure an exact copy and will not let any changes in the configuration (for example, host names remain as that are).

- **T2P** – You can use the Oracle Test to Production (T2P) utility to copy the configuration from the source to the target system. This is a more complicated approach, but lets you make host name changes.

You should choose option based on your requirements.

Separate Domains

Oracle Identity and Access Management 12c does not support Oracle Access Manager and Oracle Identity Manager running in the same domain. Before you upgrade a domain where both products co-exist, you must first split the domain into two different domains. For more information, see Separating Oracle Identity Management Applications Into Multiple Domains.

Performing an Out-of-Place Cloned Upgrade of Oracle Internet Directory

To perform a cloned upgrade of Oracle Internet Directory:

1. Place the source directory into read-only mode.
2. Back up the database that hosts your OID database schemas.
3. Back up your Oracle Internet binary installation.
4. Back up Oracle Internet Directory instance configuration.
5. Back up ODSM/DIP domain directory, if used.
6. Copy backup files to the destination system.
7. Restore the database on the destination system.
8. Restore binaries on destination system.
9. Restore the Oracle Internet Directory instances on the destination system.
10. Restore the ODSM/DIP domain directory, if used.
11. Make any host name changes you require.
12. Start the Oracle Internet Directory instances.
13. Start the Oracle OUDSM/DIP domain.
14. Validate that OID is functioning correctly using in-house tests.
15. Upgrade the OID installation using the in-place upgrade steps to reach your desired version.

Performing an Out-of-Place Cloned Upgrade of Oracle Unified Directory

To perform a cloned upgrade of Oracle Unified Directory:

1. Place your source directory into read-only mode.
2. Back up your Oracle Unified Directory binary installation.
3. Back up your Oracle Unified Directory instance configuration.

4. Back up your ODSM/DIP domain directory, if used.

5. Copy your backup files to the destination system.

6. Restore the binaries on your destination system.

7. Restore the Oracle Unified directory instances on your destination system.

8. Restore the ODSM/DIP domain directory, if used.

9. Make any host name changes you require.

10. Start your Oracle Unified Directory instances.

11. Start your Oracle OUDSM/DIP domain.

12. Validate that OUD is functioning correctly using in-house tests.

13. Upgrade your OUD installation using the in-place upgrade steps to reach your desired version.

Performing an Out-of-Place Cloned Upgrade of Oracle Access Manager

To perform a cloned upgrade of Oracle Access Manager:

1. Perform a pre-upgrade assessment to ensure that any deprecated products are not used or alternatives are put into place for them.

2. Place your source system into read-only mode.

3. Back up your database hosting your OAM database schemas.

4. Back up your Oracle Access Manager binary installation.

5. Back up your Oracle Access Manager instance configuration.

6. Back up your Oracle Access Manager domain directory.

7. Copy the backup files to the destination system.

8. Restore the binaries on your destination system.

9. Restore your Database hosting your OAM database schemas.

10. Restore the Oracle Access Manager domain directory.

11. Make any host name changes you require, this can be achieved using T2P.

12. Start your Oracle Access Manager domain.

13. Validate that OAM is functioning correctly using in-house tests, including:

    • Ensuring that you can see your external directory users in the WebLogic console.

    • Ensuring that you can log in to your console using an external directory user.

    • Using the AccessManager Test tool.

14. Upgrade your OAM installation using the in-place upgrade steps to reach your desired version.

> **Note:**
>
> To ensure that you are using your new directory, temporarily shutdown the existing directory so that you do not access it accidentally.

For instructions, see *Upgrading Oracle Access Manager* for the release you want to upgrade.

Performing an Out-of-Place Cloned Upgrade of Oracle Identity Manager

To perform a cloned upgrade of Oracle Identity Manager:

1. Perform a pre-upgrade assessment.

2. Place your source system into read-only mode.

3. Back up your database hosting your OIM database schemas.

4. Back up your Oracle Identity Manager binary installation.

5. Back up the Oracle Identity Manager configuration.

6. Back up the Oracle Identity Manager domain directory.

7. Copy your backup files to the destination system.

8. Restore your binaries on your destination system.

9. Restore your database to the destination system.

10. Restore the Oracle Identity Manager domain directory.

11. Make any host name changes you require by using T2P or the OIM host change utility.

12. Start your Oracle Identity Manager domain.

13. Validate that OIM is functioning correctly using in-house tests, including:

    - Ensuring you can see your external directory users in the OIM console.

    - Running the reconciliation jobs.

    - Creating a user or role in OIM and ensuring that it gets created in your LDAP directory.

    - Marking the end date of an employee and ensuring that any OIM sessions (if using OIM).

    - Checking if any Connectors are still functioning.

14. Upgrade your OIM installation using the in-place upgrade steps to reach your desired version.

15. If moving from Oracle Identity Manager 11g to 12c, Oracle recomends that you migrate your directory interface from LDAPSYNC to Connector.

16. Upgrade SOA composites.

17. Upgrade OIM design console.

18. Install External BI publisher and install OIM reports.

19. Tune the application module for user interface.

For instructions, see *Upgrading Oracle Identity Manager* for the release you want to upgrade.

Performing an Out-of-Place Cloned Upgrade of Oracle HTTP Server

To perform a cloned upgrade of Oracle HTTP Server:

1. Back up your Oracle HTTP Server binary installation.

2. Back up your Oracle HTTP Server instance configuration.

3. Copy your backup files to the destination system.

4. Restore your binaries on your destination system.

5. Restore the Oracle HTTP Sever instances on your destination system.

6. Make any host name changes you require.

7. Start your Oracle HTTP Server instances.

8. Validate that OHS is functioning correctly using in-house tests, including accessing protected resources.

9. Upgrade your Oracle HTTP Server installation using the in-place upgrade steps to reach your desired version.

A
Additional Information

This section of the document provides additional information and case studies of the procedures for moving Oracle Identity and Access Management (IDM) from an existing deployment into Oracle Cloud Infrastructure (OCI), and upgrading Oracle Identity and Access Management.

For more inforamtion, see:

- Migrating Oracle Identity and Access Management to Oracle Cloud Infrastructure (OCI)
- Oracle Access Manager (OAM) - Clone and Upgrade Case Study
- Oracle Internet Directory (OID) - Clone and Upgrade Case Study
- Upgrading Oracle Internet Directory to 12.2.1.3
- Upgrading Oracle Internet Directory to 12.2.1.4
- Upgrading Oracle Unified Directory to 12.2.1.3
- Upgrading Oracle Unified Directory to 12.2.1.4
- Upgrading Oracle Access Manager to 12.2.1.3
- Upgrading Oracle Access Manager to 12.2.1.4
- Upgrading Oracle Identity Manager to 12.2.1.3
- Upgrading Oracle Identity Manager to 12.2.1.4