Oracle Maximum
Availability Architecture

Oracle Fusion Middleware MAA

Separating Oracle Identity Management Applications Into Multiple Domains

ORACLE WHITE PAPER | FEBRUARY 2019

Table of Contents

Executive Summary

Upgrade to Fusion Middleware 12c requires that Oracle Access Manager and Oracle Identity Governance 11g products reside in separate WebLogic domains using the recommended separated domain topology before you upgrade to 12c. This whitepaper provides the recommended and supported procedure for customers who have deployed Oracle Access Manager and Oracle Identity Governance 11g products in a consolidated WebLogic domain, so that you can separate those components into individual unique domains before upgrading to Oracle 12c. This procedure allows customers to meet Oracle 12c upgrade requirements and avoid known issues that occur when directly upgrading a consolidated domain topology environment. Oracle Fusion Middleware Identity and Access Management 11g have traditionally supported both consolidated and separated domain topologies while historically recommending that customers deploy using the separated domain topology to gain the following benefits:

- Enable independent and less complex patching per individual component
- Accommodate different availability requirements for Oracle Access Manager and Oracle Identity Governance
- Separate the disaster recovery strategies for Oracle Access Management and Oracle Identity Governance

With Oracle Access Manager and Oracle Identity Governance 12c, the separated domain topology is the sole supported topology. Each Oracle Identity Management component must reside in its own domain.

While this document describes the procedure for highly available Oracle Enterprise Deployments of Oracle Identity Governance (OIG) and Oracle Access Manager (OAM), it is also applicable to single instance deployments.

Overview

Oracle Fusion Middleware Identity and Access Management is the suite of applications that facilitate user provisioning and access control to other applications. There are three possible options for separating the OAM and OIG domains. These are:

1. Creating 2 new domains and migrating data
2. Creating a duplicate of the consolidated domain and configuring only OAM within it
3. Creating a duplicate of the consolidated domain and configuring only OIG within it

The third option is presented in this document. It is the preferred method, because it is easier to perform, compared with the other two options. This document provides a review of the scope of Oracle Access Management and Oracle Identity Governance products affected, the consolidated and separated domain reference architecture topologies, the prerequisites and requirements for the domain separation, and a short introduction to the methods used to affect the move and reconfiguration.

A typical Oracle Identity and Access Management (IAM) enterprise deployment includes the following components:

- Oracle HTTP Server
- Oracle Access Manager (OAM)
- Oracle identity Manager (OIG)
- Oracle LDAP (OUD).

The OAM and OIG applications are deployed into Fusion Middleware domains, or a consolidated domain in 11g. The above is not a definitive listing, but rather a listing of the most commonly deployed applications. Each FMW domain is controlled by an Administration Server, either centrally or with an Administration Server per domain.

The separation method presented in this document requires an outage of the IDM environment during the domain duplication process and it continues through the configuration of the newly created OIG domain.

Oracle Fusion Middleware Maximum Availability Architecture

Oracle Maximum Availability Architecture (MAA) is Oracle's best practices blueprint based on proven Oracle high availability technologies, expert recommendations, and customer experiences. The goal of MAA is to achieve optimal high availability for Oracle customers at the lowest cost and complexity. Visit the *"Maximum Availability Architecture Best Practices"* page on the Oracle Technology Network

As part of the MAA Best Practices, Enterprise Deployment Guide documentation is available for Oracle Fusion Middleware products and provides comprehensive, scalable examples for installing, configuring, and maintaining secure, highly available, production-quality deployments. For IAM, the *"Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management"* is available on the Oracle Technology network. For the purpose of this paper, this document will be known as the *"IAM Enterprise Deployment Guide"*.

The resulting environment created from a Deployment Guide is called an enterprise deployment topology. See the Oracle Identity Management MAA Best Practices section of the *"Oracle Fusion Middleware"* page on the Oracle Technology Network website. This document presents configurations that can be implemented on both MAA recommended, high availability environments, as well as configurations that are not configured for high availability.

Oracle 11g Identity and Access Enterprise Deployment Reference Architecture

The diagram below shows the recommended Oracle 11g Enterprise Deployment Architecture for Oracle Identity and Access Management in a distributed architecture.

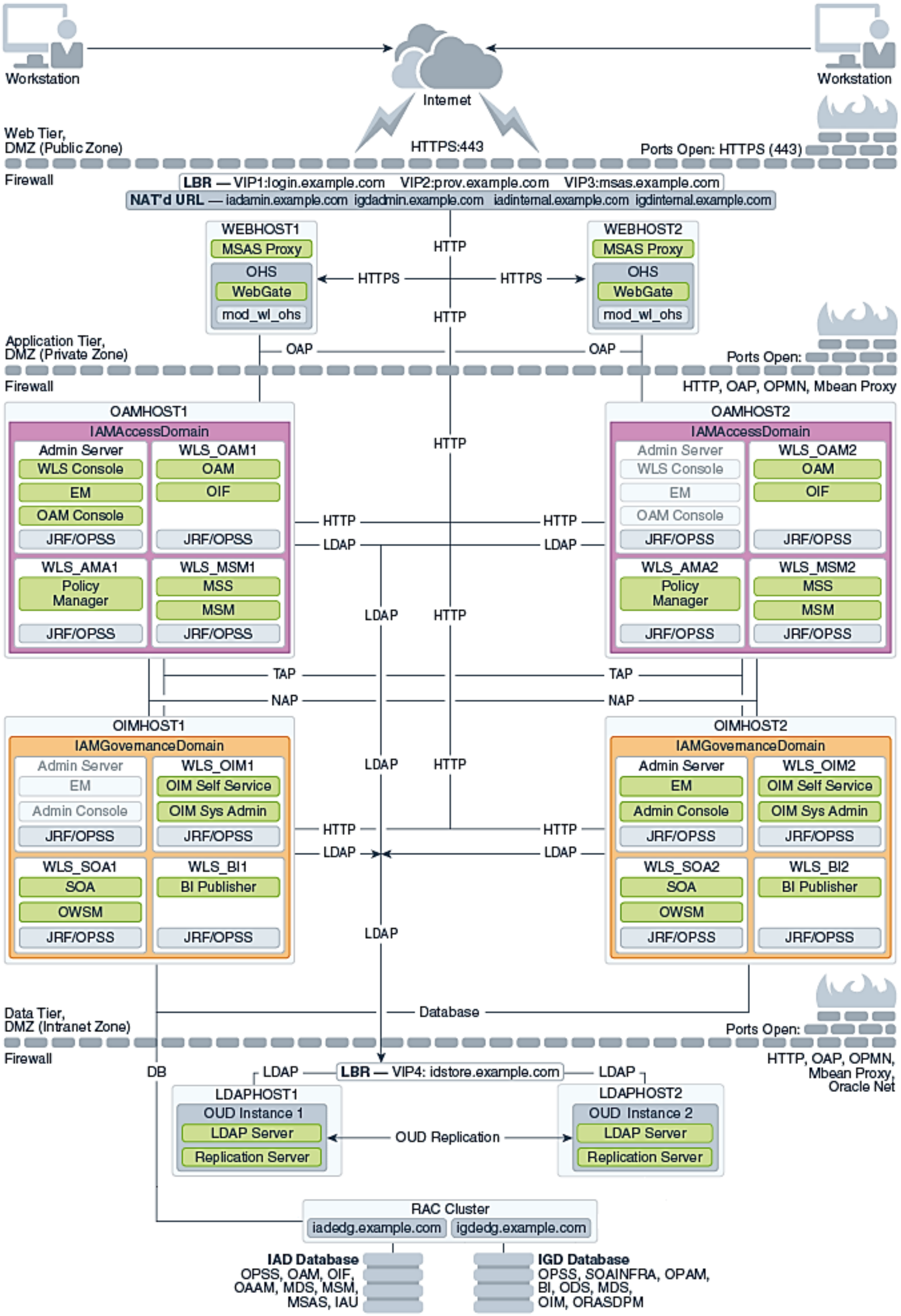

Figure 1: Oracle 11g Identity and Access Management Separated Domain Architecture

Oracle 11g Identity and Access Deployment using a Consolidated Domain

The diagram below shows an alternative Oracle 11g deployment where the components are installed in a consolidated domain.

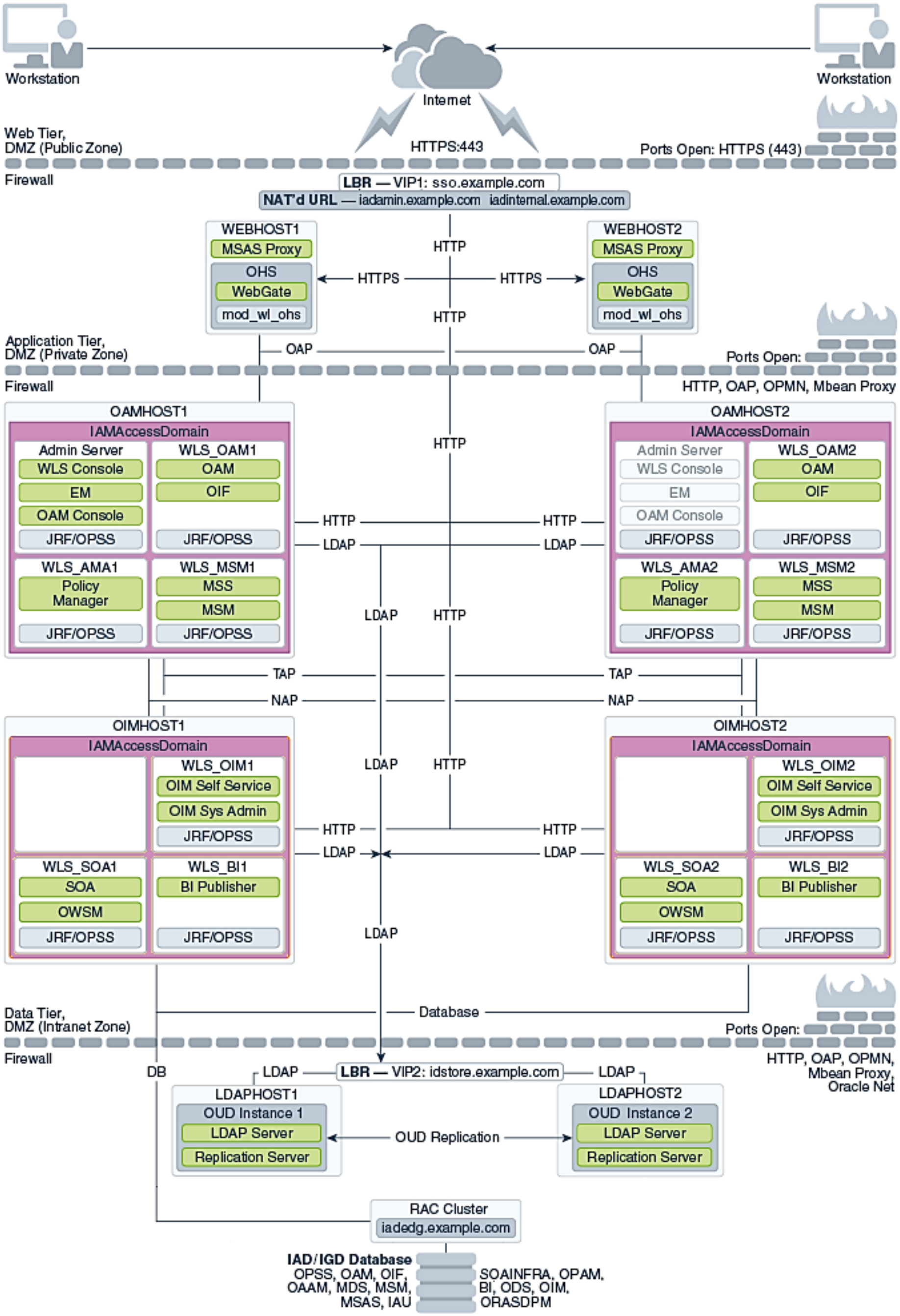

Figure 2: Oracle 11g Identity and Access Management Consolidated Domain Architecture

Key Differences Between Consolidated and Separated Domain Architectures

There are several differences between a consolidated domain configuration and a separated domain configuration. These include:

- Single vs. multiple front end URL endpoints to direct application traffic.
- The ability to perform patching or maintenance on a single type of domain (separated configuration) vs. performing maintenance on all IDM applications in the domain (consolidated configuration).
- The ability to upgrade the environment from version 11g to version 12c.

Separation Method

Details are provided for the recommended method of converting a consolidated OAM/OIG domain topology into separate OAM and OIG domains. The approach is to leave the OAM components in the original domain and then move the OIG components into a new domain using the embedded Fusion Middleware domain movement scripts, better known as Test to Production scripts, or T2P as they are commonly known. The T2P scripts provide a means of replicating the Oracle binaries stored within a Middleware home to a different Middleware home (required to allow independent patching) and to clone the configuration from one Oracle WebLogic domain to another. The script requires that the cloned domain resides in a different database than the source domain, which requires that a new database be set up in advance to provide data isolation and functional independence for the applications in each domain. A cloned domain is created for OIG, then, the OIG domain components are removed from the original OAM domain and the OAM domain components are removed from the new OIG domain. Once the domains are separated and configured, there are two different entry points, once for each domain, and the two domains are connected as shown in Figure 1 above.

The high-level steps for the overall approach are:

- Creating new load balancer VIPs for separate domain traffic routing
- Creating and prepare a new database
- Configuring and script the T2P movement
  - Creating the binary archive and domain configuration archive
  - Creating and edit movement plan
  - Cloning the binaries and domain configuration
- Configuring Web tier separation
- Configuring post-T2P movement
  - Configuring OAM login page link redirection
  - Configuring OIG Administration Server
  - Configuring domain using Administration Consoles
    - Removing unnecessary domain components from each domain
    - Adding LDAP groups to the new OIG domain
  - Configuring Domain using the command line interface
    - Configuring the OBI repository
  - Creating the Managed Server domains using pack and unpack scripts
  - Performing post pack and unpack configurations
    - Propagating binary files

  - Enrolling node managers
  - Copying Oracle Service-Oriented Architecture (SOA) composites
  - Starting all SOA and OIM Managed Servers
  - Validating front end URLs
  - Updating OIG Administration Server boot.properties
  - Enabling Single Sign-On (SSO)
  - Validating LDAP users
  - Starting all Oracle Business Intelligence (OBI) Managed Servers
- Validating the application

Points from the Reference Architecture

- Figure 1 above shows an Admin Server on `OIMHOST2` for the OIG domain (*IAMGovernanceDomain*). You can configure the Admin Server to run on either `OIMHOST1` or `OIMHOST2` for the separated OIG domain. The diagram shows that the Admin Server can be run on either host using a movable VIP for redundancy. It is on the host that will initially run the Admin Server that the T2P `pasteBinary` and `pasteConfig` scripts must be run. This will be the target architecture. Refer to *Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management* for information about the architectures and required storage for an enterprise deployment. In this architecture there are two separate AdminSever entry points, one for each of the OAM and OIG domains.
- Figure 2 above shows the domain's Admin Server running on `OAMHOST1`, from where the T2P `copyBinary`, `extractMovePlan`, and `copyConfig` scripts must be run. The scripts are run form the source environment domain.

Domain Separation Requirements

The following are requirements that must be addressed before attempting the domain separation configuration. It is noted whether the requirements are applicable to enterprise deployments or non-enterprise deployments.

Network and Load Balancer Resources

In some consolidated domain configurations, a single front end entry point URL was created. For a separated domain architecture, you must have several new network components created. These include:

- New VIPs, URLs, and corresponding DNS entries for the load balancer to separate the entry points. See *"Summary of Oracle Identity and Access Management Load Balancer Virtual Server Names"* and "*Preparing the Load Balancer and Firewalls for an Enterprise Deployment"* for more information. The entry points that may need to be separated include:
  - The single front end SSO entry point into a *login.example.com* entry point for OAM and *prov.example.com* OIG entry point.
  - The single administrative http entry point into two separate entry points for the OAM Admin Server and OIG Admin Server.
  - VIPs for Exalogic deployments should already be in place if the consolidated domain was created by consulting earlier versions of the *IAM Enterprise Deployment Guide*. See "*Preparing Exalogic for an Oracle Identity and Access Management Deployment"* for more information. Table 1 below lists the required VIPs required for the consolidated and separated domain infrastructures.

TABLE 1: REQUIRED VIPS FOR CONSOLIDATED AND SEPARATED DOMAINS

Entry Point	Targets	Consolidated Domain Purpose	Separated Domain Purpose
sso.example.com	WEBHOST1:7777, WEBHOST2:7777	OAM Login OIM Self Service	N/A
login.example.com	WEBHOST1:7777, WEBHOST2:7777	N/A	OAM Login
prov.example.com	WEBHOST1:7777, WEBHOST2:7777	N/A	OIG Self Service
iadadmin.example.com	WEBHOST1:7777, WEBHOST2:7777	OAM Admin console OAM EM Console OAM Administration OIG Admin console OIG EM Console	OAM Admin console OAM EM Console OAM Administration
igdadmin.example.com	WEBHOST1:7777, WEBHOST2:7777	N/A	OIG Admin console OIG EM Console
iadinternal.example.com	WEBHOST1:7777, WEBHOST2:7777	All internal endpoints	OAM internal endpoints
igdinternal.example.com	WEBHOST1:7777, WEBHOST2:7777	N/A	OIG internal endpoints SOA internal endpoints
idstore.example.com	LDAPHOST1:1389, LDAPHOST2:1389, LDAPHOST1:1636, LDAPHOST2:1636,	OUD front end URL	OUD front end URL

Hardware Acquisition

The same hardware that was used for the OIM Managed Servers in the consolidated domain configuration can be used for the new OIG domain. You do not need to acquire new hardware for the separated domain configuration in either enterprise or non-enterprise deployments. However, you may want to create new file system locations for the new domain. For the purposes of this document we assume that you will be keeping the OAM components on *OAMHOST1* and *OAMHOST2,* and that the OIG components will be moved to *OIMHOST1* and *OIMHOST2*. If you are keeping these components on consolidated hardware, when you see *OIMHOSTn* in the procedures use *OAMHOSTn*. These file systems can either be shared between hosts or local to the respective host. For enterprise deployments, See Preparing Storage for an Enterprise Deployment.

Database Acquisition

The process described in this document requires you to create a second database to separate the OIG domain data from that of the OAM domain data. Therefore, a new database must be created to separate the data. See Creating and Configuring an Oracle Database for more information. The database can be either a dedicated database or a pluggable database. However, for disaster recovery, it is best to create a dedicated database.

Scope

The scope of this document covers Identity Management 11g applications. Table 2: Identity Management Software Scope shows which Identity Management applications are covered by this document in the In Scope column.

TABLE 2: IDENTITY MANAGEMENT SOFTWARE SCOPE

IDM Application	In Scope	T2P Movement[1]	Separate Configuration[2]	Referenced[3]
Oracle Access Manager	Yes	Yes	No	No
Oracle Identity Manager	Yes	Yes	No	No
Oracle Web Services Manager	Yes	Yes	No	No
Oracle Service Oriented Architecture	Yes	Yes	No	No
Oracle Business Intelligence	Yes	Yes	No	No
Oracle HTTP Server	Yes	No	Yes	No
Oracle Unified Directory	No	No	No	Yes
Oracle Internet Directory	No	No	No	No
Oracle Adaptive Access Manager	No	N/A	N/A	N/A
Oracle Entitlements Server	No	N/A	N/A	N/A
Oracle Privileged Account Manager	No	N/A	N/A	N/A
Oracle Mobile Security Suite	No	N/A	N/A	N/A

1: T2P Movement shows which applications will be archived and moved using T2P movement scripts

2: Separate Configuration lists applications that are not moved with T2P movement scripts, but require individual configuration

3: Referenced applications are those that are not configured by either T2P movement scripts or separate configuration, but are referenced by other applications in the domain environments

Oracle Identity Governance Customizations

You can customize Oracle Identity Governance both in the application and by adding custom tables. Migration of these artifacts is outside the scope of this document.

Enterprise Deployment Terminology

This document does not assume that you have configured your environment as an enterprise deployment. However, it does use some terminology found in the Enterprise Deployment Guide. The following are definitions of terms used in this document, which may or may not be relevant for any deployment type.

- **MW_HOME:** This variable and related directory path refers to the location where Oracle Fusion Middleware resides. A *MW_HOME* has a *WL_HOME*, an *ORACLE_COMMON_HOME* and one or more *ORACLE_HOMEs*. In a separated domain architecture, there is a different MW_HOME for each product suite.

  The target architecture will have two separate *MW_HOMEs*, one for OIM applications and one for OIG applications.

  For the target environment, the value of *MW_HOME* may be preceded by a product suite abbreviation, for example: DIR_MW_HOME, IAD_MW_HOME, IGD_MW_HOME, and WEB_MW_HOME.

- **WL_HOME:** This variable and related directory path contains installed files necessary to host a WebLogic Server. The *WL_HOME* directory is a peer of the Oracle home directory and resides in the *MW_HOME*.

- **ORACLE_HOME**: This variable points to the location where an Oracle Fusion Middleware product, such as Oracle HTTP Server or Oracle SOA Suite is installed and the binaries of that product are being used in a current procedure. In this guide, this value might be preceded by a product suite abbreviation, for example: *IAD_ORACLE_HOME*, *IGD_ORACLE_HOME*, *WEB_ORACLE_HOME*, *WEBGATE_ORACLE_HOME*, *SOA_ORACLE_HOME*, and *OUD_ORACLE_HOME*.

- **ORACLE_COMMON_HOME:** This variable and related directory path refer to the location where the Oracle Fusion Middleware Common Java Required Files (JRF) Libraries and Oracle Fusion Middleware Enterprise Manager Libraries are installed. An example is *MW_HOME/oracle_common.*

- **JAVA_HOME:** This is the location where Oracle Java JDK is installed.

- **ASERVER_HOME:** This path refers to the file system location where the Oracle WebLogic domain information (configuration artifacts) are stored. It is where the Admin Server Managed Server runs within.
  - In a non-enterprise deployment, where Fusion Middleware pack and unpack are not used to create a management domain, *ASERVER_HOME* is the domain location on all hosts in the infrastructure.
  - In an enterprise deployment, where Fusion Middleware pack and unpack are used to create a management domain, *ASERVER_HOME* would be the domain location on all hosts where the Admin Server runs.
  - In a consolidated domain architecture, there is a single *ASERVER_HOME* for the entire domain.
  - In a separated domain architecture, there is a different *ASERVER_HOME* for each domain used, specifically: *IGD_ASERVER_HOME* and *IAD_ASERVER_HOME.*

- **MSERVER_HOME:** This path refers to the local file system location where the Oracle WebLogic domain information (configuration artifacts) are stored. This directory is generated by the pack and unpack utilities and is a subset of the *ASERVER_HOME*. It is used to start and stop Managed Servers. The Administration Server is still started from the *ASERVER_HOME* directory.
  - There is a different *MSERVER_HOME* for each domain used. Optionally, it can be used to start and stop Managed Servers.

Oracle Access Management and Identity Governance Applications

The following is a brief description of the applications that are either in scope or referenced by the applications being separated or configured.

Oracle Access Manager

Oracle Access Manager (OAM) provides the Oracle Fusion Middleware 11g single sign-on (SSO) solution. It operates independently, but can also operate with the Access Manager Authentication Provider.

Access Manager SSO allows users and groups to access multiple applications after authentication, eliminating the need for multiple sign-on requests. To enable SSO, a Web server, Application Server, or any third-party application must be protected by a WebGate (or mod_osso instance) that is registered as an agent with Access Manager. Administrators, then define authentication and authorization policies to protect the resource. To enforce these authentication policies, the agent acts as a filter for HTTP requests.

Oracle Access Manager Access

Oracle Access Manager Access provides the infrastructure for enforcing global security and auditing policies in the Service Infrastructure. By securing various endpoints and setting and propagating identity, it secures applications. Oracle Access Manager Access provides a standard mechanism for signing messages, performing encryption, performing authentication, and providing role-based access control. You also can change a policy without having to change the endpoints or clients for this endpoints, providing greater flexibility and security monitoring for your enterprise.

Oracle Identity Manager

Oracle Identity Manager (OIG) is a Governance solution that provides self service, compliance, provisioning, and password management services for applications residing on-premises or on the Cloud.

Oracle Identity Manager makes it possible for enterprises to manage the identities and access privileges of their customers, business partners, and employees, all on a single platform. It allows these users to manage their own identities as well as those of others by using delegated administration. It allows enterprises to set up delegated administrators, who are users empowered to manage the identities, passwords, password policies, and access of other users. Business users can create and manage the lifecycle of enterprise roles, which grant access to end-users. These roles can be granted automatically by using rules. With the help of roles and access policies, organizations can ensure that their users are on-boarded and off-boarded in a timely and automated manner.

Oracle Service Oriented Architecture

Oracle SOA Suite is a middleware component of Oracle Fusion Middleware. Oracle SOA Suite provides a complete set of service infrastructure components for designing, deploying, and managing SOA composite applications. Oracle SOA Suite enables services to be created, managed, and orchestrated into SOA composite applications. Composites enable you to easily assemble multiple technology components into one SOA composite application. Oracle SOA Suite plugs into heterogeneous IT infrastructures and enables enterprises to incrementally adopt SOA.

Oracle Business Intelligence

Oracle Business Intelligence (OBI) is a unique platform that enables customers to uncover new insights and make faster, more informed business decisions by offering agile visual analytics and self-service discovery, together with best-in-class enterprise analytics. Instant mobile, highly interactive dashboards, powerful operational reporting, just-in-time alerts, content and metadata search, strategy management, native access to Big Data sources, sophisticated in-memory computing, and streamlined systems management combine to make OBI a comprehensive solution that reduces the total cost of ownership and increases return on investment for the entire organization.

Oracle Unified Directory

Oracle Unified Directory (OUD) is a comprehensive next generation directory service. It is designed to address large deployments,provides high performance, and is highly extensible. Oracle Unified Directory is easy to deploy, manage, and monitor.

Its components consist of:

- LDAP directory server, used for storing data proxy server
- Oracle Directory Server Enterprise Edition

Oracle HTTP Server

Oracle HTTP Server (OHS) 11g is based on Apache HTTP Server 2.2.22 infrastructure, and includes modules developed specifically by Oracle. In release 11g, Oracle WebGate is installed as component of the OHS server and is used for connectivity to OAM applications for the purpose of single sign-on (SSO).

Assumptions

This document covers the following environment configurations and assumes that the majority of administrators planning to separate Identity Management domains are using similar configurations.

- The applications from the reference architecture were set up as part of an enterprise deployment.
- Although enterprise deployment is typically configured with high availability, the method of domain separation in this document can also be used in an environment that is not configured with high availability.
- The consolidated domain to be separated should contain the in-scope applications listed in Table 1.
- The separated domains can remain on the same hosts as they did when they were configured as a consolidated domain.
- Administrators that have out of scope applications configured in their respective domains should theoretically be able to use the same steps to separate their domains, although additional configurations not covered in this document may need to be performed.
- All command line commands in this document assume a Linux-based operating system.

Fusion Middleware Test to Production (T2P)

Using Fusion Middleware movement scripts, you can move Oracle Fusion Middleware components from a source environment to a target environment.

Moving Oracle Fusion Middleware components minimizes the amount of work that would otherwise be required to reapply all of the customization and configuration changes made in the source environment. You can install, configure, customize, and validate Oracle Fusion Middleware in a source environment. Then, when the system is stable and performs as desired, you can create the target environment by moving a copy of the components and their configurations from the source environment, instead of redoing all the changes that were part of in the source environment.

You can use these scripts to:

- Create a *MW_HOME* that is a copy of your environment. The scripts create a new Middleware home with all patches applied to all of the Oracle homes and the WebLogic Server home in a single step. This is in contrast to separately installing and applying any patches to the WebLogic Server home and separate Oracle homes.

- Move the configuration of a domain or Oracle instance, including the components in the domain or Oracle instance, from one environment to another.

Separation Method Configuration Details

This section explains the method with which to separate the consolidated Identity Management domain into two separate domains, and includes additional configurations required prior to and after the separation is accomplished. For the purposes of this document, the original domain is called the *source environment* and the cloned domain is called the *target environment*. This section contains the following topics:

Environment Backup

Target Database Preparation

Application Tier Domain Separation

Web Tier Separation Configuration

Post Domain Cloning Configuration

Environment Backup

Prior to any other preparation, it is a best practice to take full backups of the file systems of all hosts for the consolidated domain, as well as full backups of the back-end database that supports the consolidated domain. This step ensures that a full rollback is possible in the event of issues with any of the following configuration sections.

Load Balancer VIP Creation

Follow the instructions in Preparing the Load Balancer and Firewalls for an Enterprise Deployment and Configuring the Oracle Web Tier to create the required VIPs and OHS virtual hosts configuration files.

Target Database Preparation

OAM and OIG components use a database to store back end data. OAM uses the database to store policy, session, and audit store data. OIG uses the database to store user, role, community, and other self-service application data. For the T2P process, a new database must be created to support the target environment. For more information, see "*Fusion Middleware Administrator's Guide"*, Moving from a Test to a Production Environment - Installing the Database on the Target Environment. The steps to create and populate the database are as follows:

1. Create a complete backup of the database or a Flashback restore point.

2. Create a database for the target environment. Remain consistent with same version as the database for the source environment. For enterprise deployments, refer to IAM Enterprise Deployment Guide chapter 8: Preparing the Database for an Enterprise Deployment.

3. Load the required Fusion Middleware database objects into the target environment database using the Fusion Middleware Repository Creation Utility (RCU), as described in Loading the Identity and Access Management Schemas in the Oracle RAC Database Using RCU.

Note: You must ensure that you use the same version of RCU for creating your database schemas and objects as the currently running version in your source environment. Failure to do so may result in object copying errors or T2P pasteConfig failure during certain phases of the script execution.

4. If using JDBC TLOGs and/or JMS persistent stores, recreate these stores in the target environment database as well. Perform the following steps from IAM Enterprise Deployment Guide chapter 15.4.10: Using JDBC Persistent Stores for TLOGs and JMS in an Enterprise Deployment to create the JDBC stores.

   a. Create TLOGS and JMS tablespaces and schemas:

      TLOGs:

      ```
      create tablespace IAMTLOGS datafile '+DATAC1' size 32m autoextend on next
      32m maxsize 2048m extent management local;
      ```

      JMS:

      ```
      create tablespace IAMJMS datafile '+DATAC1' size 32m autoextend on next
      32m maxsize 2048m extent management local;
      ```

   b. Create users, grant access to created tablespaces, and alter the user’s default tablespace and quota:

      TLOGs:

      ```
      create user IAMTLOGS identified by welcome1;

      grant create table to IAMTLOGS;

      grant create session to IAMTLOGS;

      alter user IAMTLOGS default tablespace IAMTLOGS;

      alter user IAMTLOGS quota unlimited on IAMTLOGS;
      ```

      JMS:

      ```
      create user IAMJMS identified by welcome1;

      grant create table to IAMJMS;

      grant create session to IAMJMS;

      alter user IAMJMS default tablespace IAMJMS;

      alter user IAMJMS quota unlimited on IAMJMS;
      ```

Note: Ensure that the existing stores have been drained of messages.

5. Run these steps to populate the target environment database with the source environment's data. These instructions follow the steps in “*Fusion Middleware Administrator’s Guide”*, Perform Prerequisite Task for Oracle Identity Manager.

6. Create the OIM schema in the target database using RCU, if you have not already done so. See Loading the Database with RCU above.

   a. On the source database host, run the following commands from the database `ORACLE_HOME/bin` to set up your environment:

```
export ORACLE_HOME=ORACLE_HOME_for_source_DB
export PATH=${ORACLE_HOME}/bin:${PATH}
export ORACLE_SID=SID_for_source_DB
```

Note: Domain separation also requires database separation. Using the same database with a different RCU prefix is not an acceptable configuration. If an alternate prefix is configured within the same database, T2p pasteConfig will fail when OIM config.sh runs.

b. On the source database host, use the default dump directory or create a custom dump directory. To create a custom dump directory, run the following SQL command:

```
SQL> create directory [DB_DIR_OBJ] as
'/path_to_directory_on_database_host';
```

Where ***DB_DIR_OBJ*** is a directory object alias to the path specified in the `/path_to_directory_on_database_host` variable.

c. Copy the following file from the source Oracle Identity Manager host to the source database host:

scp *IGD_MW_HOME/iam/clone/data/exp_param.par SRC_DB_HOST:*
/path_to_directory_on_database_host

For example:

```
scp IGD_MW_HOME/iam/clone/data/exp_param.par IDMDBHOST1:/tmp
```

d. If you are running an Oracle RAC database, shut down all but one node on both source and target databases. Failure to perform this step may result in the export failing with "file does not exist" errors.

e. On the source database host, export the configuration data from the source database to a dump file:

```
expdp system/password SCHEMAS=OIM_schema_name DIRECTORY=DB_DIR_OBJ
DUMPFILE=export.dmp LOGFILE=export.log
parfile=directory_containing_file/exp_param.par
```

For example:

```
expdp system/SYSTEM_PASSWORD SCHEMAS=EDG_OIM DIRECTORY=dump_dir
DUMPFILE=export.dmp LOGFILE=export.log parfile=/tmp/exp_param.par
```

f. On the target database host, use the default dump directory or create a custom dump directory. To create a custom dump directory, run the following SQL command:

```
SQL> create directory [DB_DIR_OBJ] as
'/path_to_directory_on_database_host';
```

Where ***DB_DIR_OBJ*** is a directory object alias to the path stated in the `/path_to_directory_on_database_host` variable.

g. If you are using different database hosts for source and target databases, copy the dump file from the source database host system to the dump directory location on the target database host.

For example:

```
scp /tmp/export.dmp IDMDBHOST1:/tmp
```

h. On the target database host, run the following commands from the database `ORACLE_HOME/bin` to set up your environment:

```
export ORACLE_HOME=ORACLE_HOME_for_target_DB
export PATH=${ORACLE_HOME}/bin:${PATH}
export ORACLE_SID=SID_for_target_DB
```

i. On the target database host, for the OIM schema created using RCU, run the following PL/SQL block to drop the OIM schema DB objects:

```
sqlplus EDG_OIM/EDG_OIM _PASSWORD
SQL>BEGIN
  for s in (select object_type,object_name from user_objects
    where object_type not in('TABLE','LOB', 'INDEX','TYPE')
    and not (( object_name = 'OIM_RECON_CHANGES_BY_RES_MV'
    and object_type = 'MATERIALIZED VIEW' )
    or ( object_name = 'OIM_AFTERLOGON_TRIGGER'
    and object_type = 'TRIGGER' )) )
  loop
  BEGIN
    dbms_output.put_line('Drop '|| s.object_type ||' '|| s.object_name);
    execute immediate 'Drop '|| s.object_type ||' '|| s.object_name ;
  EXCEPTION
  WHEN OTHERS THEN
    dbms_output.put_line(SQLERRM);
  END;
  end loop;
END;
/
```

j. On the target database host, import the configuration from the dump file to the target database, as shown here:

```
impdp system/password DIRECTORY=DB_DIR_OBJ DUMPFILE=export.dmp
LOGFILE=import.log remap_schema=src_env_schema_name:tgt_env_schema_name
REMAP_TABLESPACE=src_env_oim_tablespace:tgt_env_oim_tablespace,
src_oim_lob_tablespace_name:tgt_oim_lob_tablespace_name, ...
TABLE_EXISTS_ACTION=REPLACE
```

For example:

```
impdp system/SYSTEM_PASSWORD DIRECTORY=dump_dir DUMPFILE=export.dmp
LOGFILE=import.log remap_schema=EDG_OIM:EDGIGD_OIM
REMAP_TABLESPACE=EDG_OIM:EDGIGD_OIM,EDG_OIM_LOB:EDGIGD_OIM_LOB,EDG_OIM_ARC
H_DATA: EDGIGD_OIM_ARCH_DATA,EDG_OIM_TEMP:EDGIGD_OIM_TEMP
TABLE_EXISTS_ACTION=REPLACE
```

k. Export the Oracle Business Intelligence Publisher data from the BIPLATFORM schema of the source schema, using the following command:

```
expdp system/password DIRECTORY=DB_DIR_OBJ DUMPFILE=bi_export.dmp
PARALLEL=2 LOGFILE=bi_export.log SCHEMAS=src_BIP_schema_name
include:TABLE:"IN ('XMLP_APPINFO', 'XMLP_SCHED_JOB', 'QRIZ_BLOB_TRIGGERS',
'QRIZ_CALENDARS', 'QRIZ_CRON_TRIGGERS',
'QRIZ_FIRED_TRIGGERS','QRIZ_JOB_DETAILS', 'QRIZ_JOB_LISTENERS',
'QRIZ_LOCKS', 'QRIZ_PAUSED_TRIGGERS_GRPS', 'QRIZ_SCHEDULER_STATE',
'QRIZ_SIMPLE_TRIGGERS', 'QRIZ_TRIGGER_LISTENERS', 'QRIZ_LISTENERS',
'QRIZ_TRIGGERS')"
```

For example:

```
expdp system/SYSTEM_PASSWORD DIRECTORY=dump_dir DUMPFILE=bi_export.dmp
PARALLEL=2 LOGFILE=bi_export.log SCHEMAS=EDG_BIPLATFORM include:TABLE:"IN
('XMLP_APPINFO', 'XMLP_SCHED_JOB', 'QRIZ_BLOB_TRIGGERS', 'QRIZ_CALENDARS',
'QRIZ_CRON_TRIGGERS', 'QRIZ_FIRED_TRIGGERS','QRIZ_JOB_DETAILS',
'QRIZ_JOB_LISTENERS', 'QRIZ_LOCKS', 'QRIZ_PAUSED_TRIGGERS_GRPS',
'QRIZ_SCHEDULER_STATE', 'QRIZ_SIMPLE_TRIGGERS', 'QRIZ_TRIGGER_LISTENERS',
'QRIZ_LISTENERS', 'QRIZ_TRIGGERS')"
```

l. Import the Oracle Business Intelligence Publisher data into the target schema, using the following command:

```
impdp system/password DIRECTORY=DB_DIR_OBJ DUMPFILE=bi_export.dmp
PARALLEL=2 LOGFILE=bi_export.log
REMAP_SCHEMA=src_schema_name:target_schema_name
REMAP_TABLESPACE=src_tablespace_name:target_tablespace_name
TABLE_EXISTS_ACTION=REPLACE
```

For example:

```
impdp system/welcome1 DIRECTORY=dump_dir DUMPFILE=bi_export.dmp PARALLEL=2
LOGFILE=bi_export.log REMAP_SCHEMA=EDG_BIPLATFORM:EDGIGD_BIPLATFORM
REMAP_TABLESPACE=EDG_BIPLATFORM:EDGIGD_BIPLATFORM
TABLE_EXISTS_ACTION=REPLACE
```

m. If you are running Oracle RAC databases, restart all nodes on both source and target databases.

7. Create a Flashback restore point or database backup so that you can revert in the event of T2P pasteConfig failure. Creating a restore point is the easier method of reverting the database to a point in time.

The following is a Flashback example, including enabling Flashback on the database:

```
SQL> startup mount

SQL> alter database archivelog;

SQL> alter database flashback on;

SQL> alter database open;

SQL> alter database force logging;

SQL> create restore point RESTORE_POINT guarantee flashback database;
```

Application Tier Domain Separation

This section covers the prerequisites and T2P steps to clone the source domain successfully. This section contains the following topics:

Obtaining Required Patches

Archive Creation Prerequisites

Creating Archives with T2P Copy Scripts

Creating and Editing the T2P Move Plan

Target Environment Binary Creation Prerequisites

Executing the T2P Paste Scripts to Create the Target Domain

Obtaining Required Patches

Prior to starting the prerequisites, acquire patch 20461097, T2P: LIBOVD Issue is Seen in OIM LDAP Topology During pasteConfig from the My Oracle Support site., It must be applied to the OIG binaries Middleware home (*IGD_MW_HOME)* where indicated in the following sections.

Archive Creation Prerequisites

- Create a complete offline backup of your *MW_HOME*, and domain home location (*ASERVER_HOME* and all *MSERVER_HOMEs*, if source environment is an enterprise configuration)
- If new hardware was acquired for the new OIG domain, follow the steps in the appropriate chapters of the IAM Enterprise Deployment Guide that pertain to the particular configuration being used: chapter5: Procuring Resources for an Enterprise Deployment, chapter 6: Preparing the Load Balancer and Firewalls for an Enterprise Deployment, chapter 7: Preparing Storage for an Enterprise Deployment, chapter 8: Preparing Exalogic for an Oracle Identity and Access Management Deployment, and chapter 9: Configuring the Host Computers for an Enterprise Deployment.
- Ensure that all Managed Servers in the source environment using the mds-owsm datasource are running. These include:
  - The Admin Server
  - All OIM Managed Servers (WLS_OIMn from the IAM Enterprise Deployment Guide)
  - All SOA Managed Servers (WLS_SOAn from the IAM Enterprise Deployment Guide)
  - All BI Managed Servers (WLS_BIn from the IAM Enterprise Deployment Guide)

  Failure to have any of the aforementioned Managed Servers running may result in the error noted in MOS article 1456515.1: *Error "oracle.as.t2p.exceptions.FMWT2PCopyConfigException: Error in examining OWSM policies" During 'copyConfig' Phase of Cloning Oracle Fusion Middleware Domain*.
- If possible, use a common share to both the source and target hosts that the T2P scripts will be executed on. This share is used to place the T2P archive files and the move plan files. Using a common share avoids the task of copying files from source to target. For information on how to create a share in an enterprise deployment, refer to IAM Enterprise Deployment Guide chapter 7: Preparing Storage for an Enterprise Deployment.

Creating Archives with T2P Copy Scripts

The following instructions can be found in the Fusion Middleware Administrator’s Guide in the Moving From Test to Production chapter, the Moving from a Test to a New Production Environment Using Movement Scripts subsection, and the Using the Movement Scripts appendix. The steps to create the archives from the source environment are as follows:

1. Create directories on the share for the archive files, log files, and move plan files.

   For example:

   ```
   mkdir -p SHARED_CONFIG_DIR/T2P
   mkdir -p SHARED_CONFIG_DIR/T2P/logs
   mkdir -p SHARED_CONFIG_DIR/T2P/move
   ```

2. Create a file on the share that contains the password for the source domain’s Admin Server administrative user.

   For example:

   ```
   echo ADMIN_PASSWORD > SHARED_CONFIG_DIR/T2P/adminPassword
   ```

3. Execute the T2P scripts on the source domain’s Admin Server host to create the required archives and domain move plan.

a. Change directory:

```
cd MW_HOME/oracle_common/bin
```

b. Create the binary archive with the T2P `copyBinary` script.

For example:

```
./copyBinary.sh -javaHome ${JAVA_HOME} -al
SHARED_CONFIG_DIR/T2P/T2P_FMW_Binaries -smw MW_HOME -idw true -ipl
/etc/oraInst.loc -silent true -ldl SHARED_CONFIG_DIR/T2P/logs
```

Where the variables shown above are:

javaHome: The location of the Java installation. Binaries will be in the `JAVA_HOME/bin` directory

al: The path and file name where the archive will be created.

smw: The source middleware home

idw: Ignore Disk Warning

ipl: The software inventory location

silent: Tells whether to run with or without interaction

ldl: Log directory location

c. Create the domain configuration archive with the T2P `copyConfig` script.

For example:

```
./copyConfig.sh -javaHome ${JAVA_HOME} -al
SHARED_CONFIG_DIR/T2P/T2P_Domain_Config -sdl ASERVER_HOME -smw MW_HOME -
dhn ASERVER_HOSTNAME -dpn IADADMINVHN_PORT -dau Admin Server_ADMINUSER -
dap SHARED_CONFIG_DIR/T2P/adminPassword -silent true -ldl
SHARED_CONFIG_DIR/T2P/logs
```

Where the variables shown above are:

javaHome: The location of the Java installation. Binaries will be in the `JAVA_HOME/bin` directory

al: The path and file name where the archive will be created.

sdl: The source domain location

smw: The source middleware home

dhn: The domain hostname

dpn: The domain port number

dau: The domain admin username

dap: The domain admin password file

silent: Tells whether to run with or without interaction

ldl: Log directory location

d. Create the T2P move plan files with the T2P `extractMovePlan` script.

For example:

```
./extractMovePlan.sh -javaHome ${JAVA_HOME} -al
SHARED_CONFIG_DIR/T2P/T2P_Domain_Config -pdl SHARED_CONFIG_DIR/T2P/move
```

Where the variables shown above are:

javaHome: The location of the Java installation. Binaries will be in the `JAVA_HOME/bin` directory

al: The path and file name where the archive will be created.

pdl: The move plan directory location

e. Create password file by running the following for the different types of passwords in the moveplan.xml. You will need a separate file every individual password type.

   - JDBC datasource passwords (if there are different passwords, a file for each password will need to be created)
   - LDAP admin user password
   - Other domain passwords

   For example:

```
MW_HOME/oracle_comon/bin/obfuscatePassword.sh -javaHome JAVA_HOME
[Password to obfuscate:] Welcome1
[Path of password file to be
created:]SHARED_CONFIG_DIR/T2P/domainAdminPassword
CLONE-23953-INFO Password file successfully created at
SHARED_CONFIG_DIR/T2P/domainAdminPassword
CLONE-23957-INFO Object persisted successfully
```

Creating and Editing the T2P Move Plan

The moveplan.xml file specifies how objects are created in the target domain. Without any changes, the resulting target domain will be identical to the source domain. The extracted move plan must be edited to be consistent with the target domain configuration.

Further information on modifying the move plan can be found in the "*Fusion Middleware Administrator's Guide*" - Modifying Move Plans appendix.

Changes to the moveplan.xml include:

- Replace the source domain name and *ASERVER_HOME* location with the target values, except for the initial domain name at the beginning of the move plan, as shown here:

```
<movePlan>
  <movableComponent>
    <componentType>J2EEDomain</componentType>
    <componentName>SOURCE_DOMAIN_NAME</componentName>
```

  For example:

```
<configProperty>
  <name>Default File Store Directory</name>
 <value>/u01/oracle/runtime/domains/IAMGovernanceDomain/tlogs/soa_cluster</val
 ue>
 <itemMetadata>
   <dataType>STRING</dataType>
```

```
      <scope>READ_WRITE</scope>
    </itemMetadata>
  </configProperty>
```

- Change VIPs, if the source environment was created as an enterprise deployment.

  Examples:

  ADMINVHN to *IGDADINVHN*

  OAMHOST1VHN1 to *OIMHOST1VHN1*

  OAMHOST1VHN2 to *OIMHOST1VHN2*

  OAMHOST1VHN3 to *OIMHOST1VHN3*

- Validate all URLs and change all of those required from the source domain to those of the target domain.
  - Frontend Hosts

    For example:

    ```
    <configProperty>
      <name>Frontend Host</name>
      <value>igdadmin.example.com</value>
      <itemMetadata>
        <dataType>STRING</dataType>
        <scope>READ_WRITE</scope>
      </itemMetadata>
    </configProperty>
    ```

    - Admin Server with the *igdadmin.example.com* URL
    - SOA cluster with the *igdinternal.example.com* URL
    - External Front End URL for OIM with the *prov.example.com* URL
  - Proxy URL for OIM with the *igdinternal.example.com* URL

    For example:

    ```
    <configProperty>
    <name>Proxy URL for OIM</name>
      <value>igdinternal.example.com:7777</value>
     <Description>Enter OIM Proxy URL in
     'http://&lt;hostname&gt;:&lt;portnumber&gt;' Format</Description>
      <itemMetadata>
        <dataType>STRING</dataType>
        <scope>READ_WRITE</scope>
      </itemMetadata>
    </configProperty>
    ```

  - LDAP Host with the shared *idstore.example.com* URL

For example:

```
<configProperty>
  <name>LDAP Url</name>
  <value>ldap://idstore.example.com:1389</value>
  <itemMetadata>
    <dataType>STRING</dataType>
    <scope>READ_WRITE</scope>
  </itemMetadata>
</configProperty>
```

- UMS Web Service with the *igdinternal.example.com* URL

For example:

```
<configProperty>
  <name>UMS Web Service URL</name>
  <value>http://igdinternal.example.com:7777/ucs/messaging/webservice</value>
  <itemMetadata>
    <dataType>STRING</dataType>
    <scope>READ_WRITE</scope>
  </itemMetadata>
</configProperty>
```

- OIM Server Config with the *prov.example.com* URL

For example:

```
<configProperty id="OIM Server Configuration">
  <configProperty>
    <name>Host</name>
    <value>prov.example.com</value>
    <itemMetadata>
      <dataType>STRING</dataType>
      <scope>READ_WRITE</scope>
    </itemMetadata>
  </configProperty>
```

- If using full Oracle RAC connect strings for JDBC data sources, for example:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=scan.exam
ple.com)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=SERVICE_NAME)))
```

they must be reformatted to a simpler version, or the `pasteConfig` script will fail.

For example:

```
jdbc:oracle:thin:@scan.example.com:1521/SERVICE_NAME
```

- Change every instance of a blank value for name/value pairs where Name="Password File" and Value=[BLANK]:

For example:

```
<name>Password File</name>
<value/>
```

Or for every instance of a name/value pairs where the Value="Password File":

For example:

```
<value>Password File</value>
```

Substitute the value in the <value> tags with the full path and name of one of the password files created in Step 3e in the above Creating Archives with T2P Archive Scripts, depending on the password file type (JDBC, Domain Accounts, JDBC admin, etc…)

For example:

```
<value>SHARED_CONFIG_DIR/T2P/domainAdminPassword</value>
```

- Change every instance of a blank value for name/value pairs where Name="LDAP Url" and Value=[BLANK]:

  For example:

  ```
  <name>LDAP Url</name>
  <value/>
  ```

  Substitute the value in the <value> tags with of the value of the LDAP server to be shared with both the source and target domains

  For example:

  ```
  <name>LDAP Url</name>
  <value>ldap://idstore.example.com:1389</value>
  ```

- Every instance of a blank value for name/value pairs where Name="Directory Server Type" and Value=[BLANK]:

  ```
  <name>Directory Server Type</name>
  <value/>
  ```

  Substitute the value in the <value> tags with of the value of the directory server type (OUD, etc…) to be shared with both the source and target domains

  For example:

  ```
  <name>Directory Server Type</name>
  <value>OUD</value>
  ```

Target Environment Binary Creation Prerequisites

Perform the following tasks before running the `pasteBinary` script.

1. Create any additional NFS mounts and/or shares in the target environment for the new domain. See IAM Enterprise Deployment Guide chapter 7: Preparing Storage for an Enterprise Deployment for information.

Note: If the domain is an enterprise deployment and MW_HOME is shared across every application host in the domain, there should be a separation of MW_HOMEs to provide for zero-downtime patching after the domain separation, to adhere to the recommended share configuration in the IAM Enterprise Deployment Guide. Refer to IAM Enterprise Deployment Guide chapter 7: Preparing Storage for an Enterprise Deployment for details about setting up the storage resources for your target environment.

2. Install or copy the JDK from the source domain onto the target host where the T2P cloning scripts will be executed, and set the environment variables. If you are installing a new JDK, the version should match the version in the source domain, and the load balancer certificate(s) must be added to the JDK trust store. See IAM Enterprise Deployment Guide chapter 15.4.13: Adding a Load Balancer Certificate to JDK Trust Stores for more information.

   For example:

   Install the JDK in */u01/oracle/products/jdk*

   Set environment variable examples:

   ```
   export JAVA_HOME=/u01/oracle/products/jdk
   export PATH=${JAVA_HOME}/bin:${PATH}
   ```

Note: Do not install the JDK in the location where you intend to install either the binaries or the domain configuration, because this causes the T2P scripts to fail when run. The T2P scripts require that directories that are to be created by the script do not exist before running the script.

3. Create a temporary directory on the target environment hosts, in which to run the `pasteBinary` script. Create the directory on all hosts that require a new *MW_HOME* to be created, including those that require a new *IAD_MW_HOME* or a new *IGD_MW_HOME*. A new *IAD_MW_HOME* is required if you are creating an enterprise deployment and require a redundant *IAD_MW_HOME* for upgrading purposes. For more information, see IAM Enterprise Deployment Guide appendix A: Creating a Redundant Middleware Home. If the target environment has a common share between hosts, a single location on that share can be used.

   For example:

   ```
   mkdir -p SHARED_CONFIG_DIR/T2P/pasteBinary
   ```

4. Copy `MW_HOME/oracle_common/bin/pasteBinary.sh` and `MW_HOME/oracle_common/jlib/cloningclient.jar` from the source host to the temporary directory(ies) created in the previous task.

   For example:

   ```
   cp IAD_MW_HOME/oracle_common/bin/pasteBinary.sh
   SHARED_CONFIG_DIR/T2P/pasteBinary

   cp IAD_MW_HOME/oracle_common/jlib/cloningclient.jar
   SHARED_CONFIG_DIR/T2P/pasteBinary
   ```

5. If there is no share between hosts, the binary archive file previously created must be copied to every host where you will run the `pasteBinary` script.

6. If there is no common share between all hosts, you must copy the archive created in Creating Archives with T2P Copy Scripts, step 3b to the hosts, where you will run the `pasteBinary` script.

Running the T2P pasteBinary Script to Create the Target Binaries

Create the new target domain binaries using the following steps. The variables shown on all of the `pasteBinary` script examples are:

javaHome: The location of the Java installation. Binaries will be in the `JAVA_HOME/bin` directory

al: The path and file name where the archive will be created.

tmw: The target middleware home

idw: Ignore Disk Warning

ipl: The software inventory location

silent: Tells whether to run with or without interaction

ldl: Log directory location

Creating the Target Binaries for an Enterprise Deployment:

1. On *OAMHOST2*, change directory to the temporary location where you previously copied the pasteBinary.sh script, then, run the following to create the *IAD_MW_HOME.*

   ```
   ./pasteBinary.sh -javaHome JAVA_HOME -al BINARY_ARCHIVE_LOCATION -tmw
   IAD_MW_HOME -idw true -esp true -ipl /etc/oraInst.loc -ldl
   SHARED_CONFIG_DIR/T2P/logs -silent true
   ```

   For example:

   ```
   ./pasteBinary.sh -javaHome ${JAVA_HOME} -al
   SHARED_CONFIG_DIR/T2P/T2P_FMW_Binaries -tmw /u01/oracle/products/access -idw
   true -esp true -ipl /etc/oraInst.loc -ldl SHARED_CONFIG_DIR/T2P/logs -silent
   true
   ```

2. On *OIMHOST1* and *OIMHOST2*, change directory to the temporary location where you previously copied the pasteBinary.sh script, then, run the following to create the *IGD_MW_HOME.*

   ```
   ./pasteBinary.sh -javaHome JAVA_HOME -al BINARY_ARCHIVE_LOCATION -tmw
   IAD_MW_HOME -idw true -esp true -ipl /etc/oraInst.loc -ldl
   SHARED_CONFIG_DIR/T2P/logs -silent true
   ```

   For example:

   ```
   ./pasteBinary.sh -javaHome ${JAVA_HOME} -al
   SHARED_CONFIG_DIR/T2P/T2P_FMW_Binaries -tmw /u01/oracle/products/identity -
   idw true -esp true -ipl /etc/oraInst.loc -ldl SHARED_CONFIG_DIR/T2P/logs -
   silent true
   ```

Creating the Target Binaries for a Non-Enterprise Deployment:

1. On all hosts that do not have the original *MW_HOME*, change directory to the temporary location where you previously copied the pasteBinary.sh script, then, run the following to create the *IAD_MW_HOME*:

   ```
   ./pasteBinary.sh -javaHome JAVA_HOME -al BINARY_ARCHIVE_LOCATION -tmw
   IAD_MW_HOME -idw true -esp true -ipl /etc/oraInst.loc -ldl
   SHARED_CONFIG_DIR/T2P/logs -silent true
   ```

   For example:

```
./pasteBinary.sh -javaHome ${JAVA_HOME} -al
SHARED_CONFIG_DIR/T2P/T2P_FMW_Binaries -tmw /u01/oracle/products/access -idw
true -esp true -ipl /etc/oraInst.loc -ldl SHARED_CONFIG_DIR/T2P/logs -silent
true
```

2. On all hosts that do not have the original *MW_HOME*, change directory to the temporary location where you previously copied the pasteBinary.sh script, then, run the following to create the *IGD_MW_HOME*:

```
./pasteBinary.sh -javaHome JAVA_HOME -al BINARY_ARCHIVE_LOCATION -tmw
IGD_MW_HOME -idw true -esp true -ipl /etc/oraInst.loc -ldl
SHARED_CONFIG_DIR/T2P/logs -silent true
```

   For example:

```
./pasteBinary.sh -javaHome ${JAVA_HOME} -al
SHARED_CONFIG_DIR/T2P/T2P_FMW_Binaries -tmw /u01/oracle/products/identity -
idw true -esp true -ipl /etc/oraInst.loc -ldl SHARED_CONFIG_DIR/T2P/logs -
silent true
```

   After running the script, you should have two separate *MW_HOMEs* on each host:one for the OIG domain and one for the OAM domain. In the examples above, they are:

   IAD_MW_HOME = /u01/oracle/products/access

   IGD_MW_HOME = /u01/oracle/products/identity

Target Environment Domain Configuration Creation Prerequisites

Perform the following tasks before running the `pasteConfig` script.

1. Create and populate the target database before running the T2P pasteConfig script. See Target Database Preparation.
2. If the source domain is set up with multiple hosts in a high availability configuration with more than one OIM or SOA Managed Servers, modify the /etc/host file on the host where the T2P pasteConfig script will be executed.
   a. Create a backup copy of the */etc/hosts* file as */etc/hosts.orig.*
   b. Create one new host entry on a single line for the *IGDADMINVHN* VIP IP address that includes all of the values for each Listen Address found in the *moveplan.xml* file. Enter all hostname values separated by spaces or tabs. The values should be the fully-qualified domain names (FQDN) or host aliases, not IP addresses, of the VIPs or hosts where the OIM and SOA servers are located.

      Using IAM Enterprise Deployment Guide host aliases:

```
192.168.10.20 IGDADMINVHN.example.com OIMHOST1 OIMHOST2 OIMHOST1VHN1
OIMHOST1VHN2 OIMHOST1VHN3 OIMHOST2VHN1 OIMHOST2VHN2 OIMHOST2VHN3
SOAHOST1VHN1 SOAHOST1VHN2 SOAHOST1VHN3 SOAHOST2VHN1 SOAHOST2VHN2
SOAHOST2VHN3
```

      Using FQDN values:

```
192.168.10.20 IGDADMINVHN.example.com OIMHOST1.example.com
OIMHOST2.example.com OIMHOST1VHN1.example.com OIMHOST1VHN2.example.com
OIMHOST1VHN3.example.com OIMHOST2VHN1.example.com OIMHOST2VHN2.example.com
OIMHOST2VHN3.example.com
```

   c. Comment out any other entries in this file pertaining to any hosts you have added to this line.

Note: Failure to create the host entry may result in the pasteConfig script failing at the OIM configuration step.

3. Stop all Managed Servers and the Admin Server in the source environment.
4. Install patch 20461097 to the target binary installations created in *Executing T2P* `pasteBinary` *Script to Create the Target Binaries steps* 2b *and* 3b above to avoid LibOVDPasteonfig plug-in issues. See MOS Article 2193594.1: *Pasteconfig.sh Encounters Exception at AMSuiteT2PPasteConfigException*.
5. Copy the following JAR file to the *`IGD_MW_HOME/iam/inventory/Scripts/ext/lib`* location in order for the OIM configuration to succeed:

   For example:

```
cp ${IGD_MW_HOME}/iam/server/ext/jakarta-commons/commons-collections-
3.2.2.jar ${IGD_MW_HOME}/iam/inventory/Scripts/ext/jlib
```

Failure to copy this JAR file will result in failure during the OIM configuration step.

Running T2P pasteConfig Script to Create Target Domain Configuration

Create the new target environment domain configurations using the steps below. The `pasteConfig` script creates the *IGD_ASERVER_HOME*, which is the domain location where the OIG domain's Admin Server is run from.

Unlike the `pasteBinary` script where it is run on each host or share that it needs to reside on, the `pasteConfig` script is only run once for the entire domain.

For a non-enterprise domain, the *IGD_ASERVER_HOME* is also where the Managed Servers run. For an enterprise domain, the *IGD_ASERVER_HOME* is only where the Admin Server run. There are further steps shown later in this document to create the Managed Server domain home or *IGD_MSERVER_HOME*.

1. Change directory to the newly created `IGD_MW_HOME/oracle_common/bin` directory

   For example:

```
cd /u01/oracle/products/identity/oracle/oracle_common/bin
```

2. Set up your environment:

```
unset IGD_MW_HOME
unset IGD_ASERVER_HOME
unset ORACLE_HOME
unset CONFIG_JVM_ARGS
unset T2P_JAVA_OPTIONS
unset LD_LIBRARY_PATH
export IGD_MW_HOME=/u01/oracle/products/identity (or your IGD_MW_HOME
location)
export IGD_ASERVER_HOME=/u01/oracle/config/domains/IAMGovernanceDomain (or
where your IGD_ASERVER_HOME location will be cloned to)
export ORACLE_HOME=${IGD_MW_HOME}/iam
export CONFIG_JVM_ARGS="-d64 -XX:PermSize=1024m -XX:MaxPermSize=1024m"
export T2P_JAVA_OPTIONS="-d64 -XX:PermSize=1024m -XX:MaxPermSize=1024m -
Dt2p.logging.level=ALL"
```

Note: For the last two values above, ensure that you have enough memory to accommodate your specific environment. Adjust accordingly.

3. Create the cloned domain.

```
./pasteConfig.sh -javaHome ${JAVA_HOME} -al
SHARED_CONFIG_DIR/T2P/T2P_Domain_Config -tdl ${IGD_ASERVER_HOME} -tmw
${MW_HOME} -mpl SHARED_CONFIG_DIR/T2P/move/moveplan.xml -dau weblogic -dap
SHARED_CONFIG_DIR/T2P/domainAdminPassword -ad
/u01/oracle/config/applications/IGD_APP_DIR -silent true -ldl
SHARED_CONFIG_DIR/T2P/logs
```

The variables shown above are:

javaHome: The location of the Java installation. Binaries will be in the `JAVA_HOME/bin` directory

al: The path and file name where the archive will be created.

tdl: The target domain location

tmw: The source middleware home

mpl: The move plan location

dau: The domain admin username1

dap: The domain admin password file

ad: The target application directory2

silent: Tells whether to run with or without interaction

ldl: Log directory location

1:. Make sure to specify the "weblogic" user for the -dau parameter (or the default user configured during the original domain configuration wizard process). Only this default local administrative user is available to the T2P scripts during its execution. Any other users from the identity store are not yet accessible to the cloned domain until the post-T2P configurations are performed.

2: If the source application directory (ad) was embedded inside of ASERVER_HOME, it needs to be moved to a location on the target host that is outside of the IGD_ASERVER_HOME that is being created. pasteConfig would fail if the application directory is inside the domain directory. The pasteConfig script checks to make sure, that the directories that it creates are empty.

3: The following error may be seen in the OIM config.sh install log during the pasteConfig process, which can be ignored: Tue Nov 27 10:40:24 PST 2018 - ERROR - oracle.xdo.servlet.ui.admin.AdminException: DUPLICATE_DATA_SOURCE_EXCEPTION

Depending on the source domain configuration, the `pasteConfig` script may take upwards of an hour or more to complete. Upon completion, the script may leave multiple Java processes running on the server, which need to be stopped in order to proceed with the post-T2P configurations. Use the following commands to find and stop these processes:

```
ps –fu `whoami` | grep java
```

```
kill -9 [PIDs_FROM_PREVIOUS_COMMAND]
```

Failure of the pasteConfig Script

Because the `pasteConfig` script sets up an entirely new domain, it is susceptible to failure if configurations are not set properly. See Troubleshooting for information about several possible issues that may occur if these configurstions are not set properly. If the `pasteConfig` script fails at any point, the target environment must be completely reset. This reset includes the following:

- Database
  - Flashback the database or restore from database backup.

    For example:

    ```
    SQL> flashback database to restore point RESTORE_POINT;
    ```

    or
  - Run RCU to drop and recreate the OAM and OIM schemas and objects.
- File system
  - Remove the following directories.
    - The directory created as the target domain location (-*tdl*) in the `pasteConfig` script
    - The directory created as the application directory (-*ad*) in the `pasteConfig` script
    - The runtime domain found in the modified move plan
  - Kill any Java processes that the `pasteConfig` script may have started.

Web Tier Separation Configuration

In the consolidated domain configuration, there may be only a single front-end (SSO) URL virtual hosts configuration file, a single admin virtual hosts configuration file, and a single internal virtual hosts configuration file. With the domain separation on the application tier, there will be two Admin Servers, two front-end entry point URLs, and two internal entry point URLs, one for each of the source and target domains. This requires the separation of the web tier configurations :

- One virtual host file for the OAM login URLs
- One virtual host file for the OIG URLs
- One admin virtual host file for each of the two Admin Server's URL redirection
- One internal virtual hosts file to cover the OIM and SOA internal URL redirection

As described in IAM Enterprise Deployment Guide chapter 14: Configuring the Oracle Web Tier, you can use the same web servers for both of the OAM and OIG domains, using multiple load balancer VIPs. The VIPs to be used are:

- Convert sso.example.com:443 to login.example.com:443
- Current VIP: iadadmin.example.com:80
- Current VIP: iadinternal.example.com:7777
- New VIP: prov.example.com:443
- New VIP: igdadmin.example.com:80
- New VIP: igdinternal.example.com:7777

In a consolidated configuration, several of the above VIPs would be consolidated in the source environment. Examples are:

- login.example,com and prov.example.com may be combined as a single VIP.
- iadadmin.example,com and igdadmin.example.com may be combined as a single VIP for the single Admin Server.

These combined VIPs must be separated to accommodate the separation of domains in the target environment. Table 3: Virtual Hosts Files and Their Respective Configurations below lists the virtual host files to be created and their respective directives. See IAM Enterprise Deployment Guide chapter 14.1.2: Configuring Virtual Hosts for more information. *WebLogicHost* and *WebLogicCluster* host names configured in the virtual host files must match the hostnames of the Managed Servers on which they reside. These are:

- login_vh.conf
  - *OAMHOST1:OIM_PORT, OAMHOST2:OIM_PORT*
- iadadmin_vh.conf
  - *IADADMINVHN:IAD_ADMIN_PORT*
  - *OAMHOST1:AMA_PORT, OAMHOST2:AMA_PORT*
  - *OAMHOST1:MSM_PORT, OAMHOST2:MSM_PORT (if MSM is being used)*
- iadinternal_vh.conf
  - *OAMHOST1:MSM_PORT, OAMHOST2:MSM_PORT (if MSM is being used)*
- prov_vh.conf
  - *OIMHOST1VHN1:OIM_PORT, OIMHOST2VHN1:OIM_PORT*
- igdadmin_vh.conf
  - *IGDADMINVHN:IGD_ADMIN_PORT*
  - *OIMHOST1VHN1:OIM_PORT, OIMHOST2VHN1:OIM_PORT*
- igdinternal_vh.conf
  - *OIMHOST1VHN1:OIM_PORT, OIMHOST2VHN1:OIM_PORT*
  - *OIMHOST1VHN2:SOA_PORT, OIMHOST2VHN2:SOA_PORT*
  - *OIMHOST1VHN3:BI_PORT, OIMHOST2VHN3:BI_PORT*

TABLE 3: VIRTUAL HOST FILES AND THEIR RESPECTIVE CONFIGURATIONS

Virtual Host Filename	ServerName Directive	Location Directives
iadadmin_vh.conf	http://*iadadmin.example.com:80*	/console /consolehelp /em /oamconsole /apm /access /gms-rest /msm-mgmt

Virtual Host Filename	ServerName Directive	Location Directives
igdadmin_vh.conf	http://*igdadmin.example.com:80*	/console /consolehelp /em /apm /oim /sysadmin /xlWebApp /identity /Nexaweb /SchedulerService-web /xmlpserver
iadinternal_vh.conf	http://*iadinternal.example.com:7777*	/msm /ecp /mfm /gms-rest /msm-mgmt
igdinternal_vh.conf	http://*igdinternal.example.com:7777*	/sodcheck /role-sod /workflowservice /callbackResponseService /spml-xsd /spmlws /reqsvc /integration /soa-infra /ucs /provisioning-callback /CertificationCallbackService /sdpmessaging /Deployment
login_vh.conf	https://*login.example.com:443*	/oam /oamfed /ms_oauth
prov_vh.conf	*https://prov.example.com:443*	/identity /xlWebApp /HTTPClnt /reqsvc

Post Domain Cloning Configuration

Before starting the Admin Server or any of the Managed Servers in the cloned target domain, there are several configurations and validations that need to be performed. The following sections cover the required tasks.

OIG Admin Server Pre-Start Configurations

Perform the following required domain file system configurations.

1. Disable SSO from the web tier by commenting out the following line from the `WEB_ORACLE_INSTANCE/config/OHS/INSTANCE_NAME/httpd.conf` file, and restart the OHS instance(s):

   ```
   #Include "${WEB_ORACLE_INSTANCE}/config/OHS/${INSTANCE_NAME}/webgate.conf"
   ```

2. On the target domain administrative server host, for example, *OIMHOST1*, revert the `/etc/hosts` changes from step 2 of the Target Environment Domain Configuration Creation Prerequisites section above by renaming the new file to `/etc/hosts.edited` and renaming the original file `/etc/hosts`.

   ```
   mv /etc/hosts /etc/hosts.edited
   mv /etc/hosts.orig /etc/hosts
   ```

3. Remove the contents of the following directories in the new Admin Server:

   ```
   IGD_ASERVER_HOME/servers/Admin Server/tmp
   IGD_ASERVER_HOME/servers/Admin Server/cache
   IGD_ASERVER_HOME/servers/Admin Server/logs
   ```

4. Create a new `boot.properties` for the Admin Server. See IAM Enterprise Deployment Guide Chapter 15.4.4: Creating boot.properties for the WebLogic Administration Servers

   a. Create the following directory structure.

      ```
      mkdir -p IGD_ASERVER_HOME/servers/Admin Server/security
      ```

   b. In a text editor, create a file called `boot.properties` in the last directory created in the previous step, and enter the username and password in the file. For example:

      ```
      username=weblogic
      password=password for weblogic user
      ```

      The clear text username and password are encrypted by the Admin Server at first server startup.

5. Edit the following file in the cloned *IGD_ASERVER_HOME*, replacing values of the previous domain name with those of the new domain name, or with the new target domain Admin Server VIP:

   » `IGD_ASERVER_HOME/sysman/state/targets.xml`

   For example:

   ```
   <Target TYPE="oracle_ias_farm" NAME="Farm_IAMGovernanceDomain"
   DISPLAY_NAME="Farm_IAMGovernanceDomain">
   ```

6. If any of the following files were customized before the T2P copy/paste process, they must be reapplied to their counterpart files in the cloned *IGD_ASERVER_HOME*:

   » `IAD_ASERVER_HOME/bin/setDomainEnv.sh`

   » `IAD_ASERVER_HOME/bin/startWebLogic.sh`

   a. Copy the OAM Domain scripts from the OAM Admin Server host to the OIG Admin Server host:

      ```
      scp OAMHOST1:IAD_ASERVER_HOME/bin/setDomainEnv.sh
      OIMHOST1:/tmp/iad_setDomainEnv.sh

      scp OAMHOST1:IAD_ASERVER_HOME/bin/startWebLogic.sh
      OIMHOST1/tmp/iad_startWebLogic.sh
      ```

   b. Compare the copied files to the current environment and create patch files.

```
diff -u /tmp/iad_setDomainEnv.sh IGD_ASERVER_HOME/bin/setDomainEnv.sh >
/tmp/iad_setDomainEnv.patch
```

```
diff -u /tmp/iad_startWebLogic.sh IGD_ASERVER_HOME/bin/startWebLogic.sh >
/tmp/iad_startWebLogic.patch
```

c. Manually review patch output files for changes.

```
* /tmp/iad_setDomainEnv.patch
```

```
* /tmp/iad_startWebLogic.patch
```

d. If necessary, back up the scripts and apply the patches in the target environment.

```
cp IGD_ASERVER_HOME/bin/setDomainEnv.sh
IGD_ASERVER_HOME/bin/setDomainEnv.sh.orig
```

```
cp IGD_ASERVER_HOME/bin/startWebLogic.sh
IGD_ASERVER_HOME/bin/startWebLogic.sh.orig
```

```
patch IGD_ASERVER_HOME/bin/setDomainEnv.sh < /tmp/iad_setDomainEnv.patch
```

```
patch IGD_ASERVER_HOME/bin/startWebLogic.sh < /tmp/iad_startWebLogic.patch
```

e. Clean up the temporary files.

```
rm -f /tmp/iad_setDomainEnv.* /tmp/iad_startWebLogic.*
```

7. Validate that all application deployment paths are inside of the new domain. These are listed in the `IGD_ASERVER_HOME/config/config.xml` file inside `<app-deployment>` tags, specifically:

» em

» NonJ2EEManagement#11.1.1

8. Edit the `IGD_ASERVER_HOME/config/config.xml` file and remove the following lines, so that the oam_admin deployment does not start on the OIG domain Admin Server:

```
<app-deployment>

    <name>oam_admin#11.1.2.0.0</name>

    <target>Admin Server</target>

    <module-type>ear</module-type>

    <source-path>/u01/oracle/products/access/iam/oam/server/apps/oam-
admin.ear</source-path>

    <deployment-order>400</deployment-order>

    <security-dd-model>DDOnly</security-dd-model>

    <staging-mode>nostage</staging-mode>

  </app-deployment>
```

Note: If any edits to the IGD_ASERVER_HOME/config/config.xml file are made, you must remove the IGD_ASERVER_HOME/edit.lok and the IGD_ASERVER_HOME/config/config.lok files, or your to the file are automatically reverted. It is also a good practice to create a backup version of the file before editing it.

9. Follow the instructions in IAM Enterprise Deployment Guide chapter 15.4.5: Perform Initial Node Manager Configuration, and if you are setting up an enterprise deployment, follow the instructions in chapter16: Setting Up Node Manager for an Enterprise Deployment to configure and start the node managers on your hosts.

For an enterprise deployment, if you are using the same OIG hosts for the separated domain as you were for the consolidated domain, you can use the same node managers. You must replace the nm_data.properties file with that in the new *WL_HOME*. You also need to change the *MW_HOME* location in the nodemanager.domains and startNodeManagerWrapper.sh files, and re-enroll the node managers to the new OIG domain's Admin Server. The Enrolling Node Managers Into Their Respective Domains section provides details for this procedure. You only need to set up a new node manager for the Admin Server VIP. Enrolling the node managers is described in the next section of the document.

If you run OIG and OAM node managers on the same hosts, they must be running at different VIPs, at different IPs, or different ports.

10. Start the OIG Admin Server using *IGD_ASERVER_HOME*/bin/startWeblogic.sh and change the node manager credentials. See IAM Enterprise Deployment Guide chapter 15.4.5.2: Updating the Node Manager Credentials. Attempting to start using WLST before completing the above steps will fail, because the node manager credentials are not yet synched.
    a. Start the Administration Server using the start script in the domain directory:

    ```
    cd IGD_ASERVER_HOME/bin

    ./startWebLogic.sh
    ```

    b. Use the Administration Console to update the Node Manager credentials for the domain.
        i. In a browser, access the WebLogic Administration console. For example:
        `http://IGDADMINVHN.example.com:7100/console`
        ii. Log in as the weblogic user, using the password you specified in the boot-properties file.
        iii. Click **Lock & Edit**.
        iv. Click **domain_name**.
        v. Select **Security** tab, and then **General** tab.
        vi. Expand **Advanced Options**.
        vii. Enter a username for **Node Manager**.
        viii. Click **Save**.
        ix. Click **Activate Changes**.

11. Follow the instruction in IAM Enterprise Deployment Guide chapter 15.4.5.3: Disabling Host Name Verification using the WebLogic Administration Console.
    a. Log in to the Oracle WebLogic Server Administration Console.
    b. Log in as the user **weblogic**, using the password you specified during the installation.
    c. Click **Lock & Edit**.
    d. Expand the **Environment node** in the **Domain Structure** window.
    e. Click **Servers**.
    f. The Summary of Servers page appears.
    g. Select **Admin Server(admin)** in the Name column of the table. The Settings page for Admin Server(admin) appears.
    h. Click the **SSL** tab.
    i. Click **Advanced**.
    j. Set **Hostname Verification** to None.
    k. Click **Save**.
    l. Click **Activate Changes**.

12. Restart the OIG Admin Server by following the steps in IAM Enterprise Deployment Guide chapter 15.4.5.4: Restart the Administration Server via Node Manager. This step assumes that the node manager for the Admin Server host or VIP from step 10 above is already running.
    a. Stop the WebLogic Administration Server by running stopWebLogic.sh, located in the *IGD_ASERVER_HOME*/bin directory, or, if the server is running in the foreground of a command line window, press CTRL+C to stop the Admin Server.
    b. Start WLST and connect to the Node Manager with nmconnect and the credentials set as previously described. Then start the Administration Server using nmStart.

```
cd ${ORACLE_COMMON_HOME}/common/bin

./wlst.sh

nmConnect('ADMIN_USER','PASSWORD','IGDADMINVHN','IGDADMINPORT',
'IAMGovernanceDomain','IGD_ASERVER_HOME')

nmStart('Admin Server')
```

Replace the value of:

ADMIN_USER with the OIG domain node manager user set in step 11 above.

PASSWORD with the OIG domain node manager password set in step 11 above.

IGD_ADMIN_VIP with the listen address that the node manager runs at

IGD_ADMIN_PORT with the port that the node manager runs at

13. Start the OAM node managers and the OAM Admin Server as you would before executing the T2P scripts.

Domain Configurations Using the Adminstration Console

Removing Unnecessary Domain Components from Each Domain

After cloning the original consolidated domain, each domain has a specialized purpose but still contains the identical configuration for all product features. Clean up both domains by removing the components that are no longer needed for each domain's respective purposes, following the instructions below. Table 4: Listing of Objects to be Removed from Domains Via Admin Consoles lists the objects that should be removed from each domain. Remove each object in thetop-down order listed in the table to avoid any dependency issues.

TABLE 4: OBJECTS TO BE REMOVED FROM DOMAINS USING ADMINISTRATION CONSOLE

Configuration Object Type	OAM Domain (*IAD_ASERVER_HOME*)	OIG Domain (*IGD_ASERVER_HOME*)
JMS Modules	SOA, OIM, and BI JMS Modules	N/A
JMS Servers	SOA, OIM, and BI JMS Servers	N/A
Persistent Stores	SOA, OIM, and BI Persistent Stores	N/A
Clusters	OIM Cluster, SOA Cluster, BI Cluster	OAM Cluster, AMA Cluster, MSM Cluster
Work Managers	All targeted to OIM, SOA, or BI Managed Servers	N/A
Managed Servers	All OIM, SOA, and BI	All OAM, AMA, and MSM
Machines	All OIMHOSTs	All OAMHOSTs

Remove all of the objects listed in Table 4 above following this process. The objects must be removed in the order listed above.

1. Access the Admin Console for the appropriate domain.
2. Click **Lock & Edit** in the upper-left **Change Center** section.
3. Expand **Domain and Services** elements of the **Domain Structure** tree, and select a configuration object type. Follow the list in Table 4. in a top-down sequence. The order of removal is specific and required to avoid errors.
   - DOMAIN_NAME (Examples: *IAMAccessDomain* or *IAMGovernanceDomain*)
     - Environment
       - Servers
       - Clusters
       - Machines
       - Work Managers
     - Services
       - Messaging
         - JMS Modules
         - JMS Servers
       - Persistent Stores
4. In the subsequent screen, check the box next to each item to be deleted. Select the objects as listed in Table 4 for the current domain and current object type you're working on.
5. Click **Delete**.
6. Repeat steps 3-5 for each set of objects in Table 4 for the current domain.
7. Once all required changes have been made, click **Activate Changes** in the **Change Center** section.
8. Repeat this process for the each domain listed in Table 4.

Adding LDAP Groups to the New OIG Domain

When you run the `pasteConfig` script, it does not create the configuration to add the directory server groups to the WebLogic administrators group. Follow the instructions in IAM Enterprise Deployment Guide Chapter 17.2.3.3: Adding LDAP Groups to WebLogic Administrators to add the LDAP Groups *OAMAdministrators* and *IDM Administrators* to the WebLogic Administrators:

1. Log in to the WebLogic Administration Server Console.
2. In the left pane of the console, click **Security Realms**.
3. On the **Summary of Security Realms** page, click **myrealm** under the **Realms** table.
4. On the Settings page for **myrealm**, click the **Roles & Policies** tab.
5. On the **Realm Roles** page, expand the **Global Roles** entry under the **Roles** table.
6. Click the **Roles** link to go to the **Global Roles** page.

   ``On the Global Roles page, click the **Admin** role to go to the Edit Global Roles page.
7. On the **Edit Global Roles** page, under the **Role Conditions** table, click **Add Conditions**.
8. On the **Choose a Predicate** page, select **Group** from the drop down list for predicates and click **Next**.
9. On the Edit Arguments Page, Specify **OAMAdministrators** in the Group Argument field and click **Add**.
10. Repeat for the Group **IDM Administrators**.

11. Click **Finish** to return to the **Edit Global Roles** page.
12. The **Role Conditions** table now shows the groups **OAMAdministrators** and **IDM Administrators** as role conditions.
13. Click **Save** to finish adding the **Admin** role to the **OAMAdministrators** and **IDM Administrators** Groups.

Domain Configurations Using the Command Line Interface

Copy the OBI Repository

So that the Oracle Business Intelligence functionality works as it previously did in the consolidated domain, the repository must be copied from the source environment to the target environment before starting the BI Managed Servers. Follow the below steps to accomplish this.

1. Create an archive of the BI repository.

   For example

   ```
   cd IAD_ASERVER_HOME/config
   ```

   ```
   tar zcvf bipublisher.tgz bipublisher/repository/*
   ```

2. Copy the archive to the target host.

   For example:

   ```
   scp IAD_ASERVER_HOME/config/bipublisher.tgz OIMHOST1:IGD_ASERVER_HOME/config
   ```

3. Decompress the archive into the *IGD_ASERVER_HOME* host.

   For example:

   ```
   cd IGD_ASERVER_HOME/config
   ```

   ```
   tar zxvf bipublisher.tgz
   ```

4. Edit the following files in the *IGD_ASERVER_HOME*, replacing values of the previous domain name with those of the new domain name, or with the new target domain Admin Server VIP.

   - `IGD_ASERVER_HOME/config/bipublisher/repository/Admin/Scheduler/jms_cluster_config.properties`
   - `IGD_ASERVER_HOME/config/bipublisher/repository/Admin/DataSource/datasources.xml`

5. Create the `jms/sharedtemp` location directory that was configured in the `IGD_ASERVER_HOME/config/bipublisher/repository/Admin/Scheduler/jms_cluster_config.properties` file.

Creating the Managed Server Domains Using Pack and Unpack

In enterprise deployments, multiple domain home folders are segregated based on functionality and high-availability requirements. Additional steps are needed in these types of deployments to replicate the domain configuration properly.

The primary domain home for the Admin Server, referred to as: *ASERVER_HOME*, contains the complete domain configuration and server folder for the Admin Server. This directory structure is typically stored on a shared file system to allow Admin Server runtime failover. The domain home folder for the rest of the domain's Managed Servers, known as *MSERVER_HOME*, is stored in a common location on each host, typically on a local storage volume. The *MSERVER_HOME* is created and populated with data from the *ASERVER_HOME* by the Fusion Middleware utilities: `pack` and `unpack`.

Pack is used to create an archive that can be used to create a Managed Server domain home from an administrative domain home. Unpack is used to deploy the packed domain configuration into a machine's Managed Server domain home location. Perform the following steps on all hosts assigned as machines to run Managed Servers in the target OIG domain.

Use these steps to pack the configuration from the OAM and OIG administrative domain homes and unpack into their respective Managed Server domain homes per host. Refer to IAM Enterprise Deployment Guide chapter 15.4.6: Creating a Separate Domain Directory for Managed Servers in the Same Node as the Administration Server for the pack command and to unpack to the same hosts as the administrative domain was packed. Also, refer to IAM Enterprise Deployment Guide chapter 15.4.7: *Propagating Changes to Remote Servers* for instructions about unpacking the Managed Server domain into remote servers.

From this point forward, the source domain isknown as the OAM domain, and the target domain is known as the OIG domain.

OAM Domain (IAD_ASERVER_HOME)

1. Execute the `pack` command from *OAMHOST1*:

   ```
   IAD_MW_HOME/oracle_common/common/bin/pack.sh -managed=true –
   domain=IAD_ASERVER_HOME –template=/tmp/
   IAD_SplitDomain_Whitepaper_Template.jar -template_name=IAD_TEMPLATE -
   log=/tmp/pack.log -log_priority=debug
   ```

   Where the variables shown above are:

   managed: Specifies whether the template is to be used to create Managed Servers on remote machines.

   domain: The full or relative path for the *IAD_ASERVER_HOME* from which the template is to be created.

   template: The full or relative path and file name of the template to be created. The template filename must include the *.jar* extension.

   template_name: Descriptive name for the template. Quotes are required only if the value contains spaces.

   log: Path and name of the log file.

   log_priority: Sets the logging level.

2. Copy the Created template jar file to `/tmp` on *OAMHOST1* and *OAMHOST2*:

3. Run the `unpack` command on *OAMHOST1* and *OAMHOST2*:

   ```
   IAD_MW_HOME/oracle_common/common/bin/unpack.sh -domain=IAD_MSERVER_HOME -
   overwrite_domain=true -template=/tmp/ IAD_SplitDomain_Whitepaper_Template.jar
   -log=/tmp/unpack.log -log_priority=debug -app_dir=IAD_MSERVER_HOME
   ```

   Where the variables shown above are:

   domain: The full or relative path of the *IAD_MSERVER_HOME* to be created.

   overwrite_domain: If the specified domain directory already exists and is not empty, no warnings to that effect are displayed, and the files in the directory are automatically overwritten.

   template: The full or relative path and filename of the template from which the WebLogic domain is to be created.

   log: Path and name of the log file.

   log_priority: Sets the logging level.

app_dir: The full path to the directory used to store the applications defined in the template. This parameter is applicable only if the template supports a separate applications directory.

4. Start all OAM domain node managers and Managed Servers as previously performed before domain separation, and validate successful startups.

OIG Domain (IGD_ASERVER_HOME)

1. Run the `pack` command from *OIMHOST1*:

```
IGD_MW_HOME/oracle_common/common/bin/pack.sh -managed=true –
domain=IGD_ASERVER_HOME -template=/tmp/
IGD_SplitDomain_Whitepaper_Template.jar -template_name=IGD_TEMPLATE -
log=/tmp/pack.log -log_priority=debug
```

   Where the variables shown above are:

   managed: Specifies whether the template is to be used to create Managed Servers on remote machines.

   domain: The full or relative path for the *IGD_ASERVER_HOME* from which the template is to be created.

   template: The full or relative path and file name of the template to be created. The template filename must include the *.jar* extension.

   template_name: Descriptive name for the template. Quotes are required only if the value contains spaces.

   log: Path and name of the log file.

   log_priority: Sets the logging level.

2. Copy the template JAR file to `/tmp` on *OIMHOST1* and *OIMHOST2.*
3. Run the `unpack` command on *OIMHOST1* and *OIMHOST2*:

```
IGD_MW_HOME/oracle_common/common/bin/unpack.sh -domain=IGD_MSERVER_HOME -
overwrite_domain=true -template=/tmp/ IGD_SplitDomain_Whitepaper_Template.jar
-log=/tmp/unpack.log -log_priority=debug -app_dir=IGD_MSERVER_HOME
```

   Where the variables shown above are:

   domain: The full or relative path of the *IGD_MSERVER_HOME* to be created.

   overwrite_domain: If the specified domain directory already exists and is not empty, no warnings to that effect are displayed, and the files in the directory are automatically overwritten. No attempt is made to merge or preserve local customizations.

   template: The full or relative path and filename of the template from which the WebLogic domain is to be created.

   log: Path and name of the log file.

   log_priority: Sets the logging level.

   app_dir: The full path to the directory used to store the applications defined in the template. This parameter is applicable only if the template supports a separate applications directory.

Note: For non-enterprise deployments, where a Managed Server domain was not configured originally, copying the administrative domain to each host is sufficient.

Post-Pack/Unpack Configurations

Now that the domains have been separated and deployed into administrative and Managed Server domains, there are a few additional configurations that need to be performed before the OIG Managed Servers can be started and validated. The following sections explain these configurations.

Propagate Changes to `ASERVER_HOME/bin` files to `MSERVER_HOME/bin`

As previously required in OIG Admin Server Pre-Start Configurations, step 8, when pack and unpack utilities are used, they do not propagate changes to the domain home binary files in `MSERVER_HOME/bin`. The following steps show a method to change and deploy them.

OAM Domain (IAD_MSERVER_HOME)

1. On the *OAMHOST1*, run the following:

```
cd IAD_MSERVER_HOME/bin
cp IAD_ASERVER_HOME/bin/startWebLogic.sh .
cp IAD_ASERVER_HOME/bin/setDomainEnv.sh .
vi setDomainEnv.sh and remove DemoTrust.jks reference
for f in `find IAD_MSERVER_HOME/bin -type f `; do sed -i
"s|IAD_ASERVER_HOME|IAD_MSERVER_HOME|g" $f ;done
```

2. Copy the edited files to the rest of the OAM domain hosts.

For example:

```
scp startWebLogic.sh [OAMHOST1/OAMHOST2]:`pwd`
scp setDomainEnv.sh [OAMHOST1/OAMHOST2]:`pwd`
```

Where ***ALL_OAMHOSTs*** are the hosts where all OAM *MSERVER_HOMEs* reside.

OIG Domain (IGD_MSERVER_HOME)

1. On the *OIMHOST1*, run the following:

```
cd IGD_MSERVER_HOME/bin
cp IGD_ASERVER_HOME/bin/startWebLogic.sh .
cp IGD_ASERVER_HOME/bin/setDomainEnv.sh .
vi setDomainEnv.sh and remove DemoTrust.jks reference
for f in `find IGD_MSERVER_HOME/bin -type f `; do sed -i
"s|IGD_ASERVER_HOME|IGD_MSERVER_HOME|g" $f ;done
```

2. Copy the edited files to the rest of the OIG domain hosts.

For example:

```
scp startWebLogic.sh [OIMHOST1/OIMHOST2]:`pwd`
scp setDomainEnv.sh [OIMHOST1/OIMHOST2]:`pwd`
```

Where ***ALL_OIMHOSTs*** are the hosts where all OIG *MSERVER_HOMEs* reside.

Enrolling Node Managers in Their Respective Domains

Because the *IGD_ASERVER_HOME* and *IGD_MSERVER_HOME* domain home locations have been created as part of the T2P cloning, the node managers that reside on these `OIMHOSTs` will need to be enrolled in the *IGD_ASERVER_HOME* Admin Server. Please refer to IAM Enterprise Deployment Guide chapter 15.4.6: Creating a Separate Domain Directory for Managed Servers in the Same Node as the Administration Server, Steps 3a-3c. Run the following procedure on each of the OIMHOSTs to enroll the node managers on that specific host. After all of the node managers are enrolled, start all of the node managers.

```
"IGD_ORACLE_COMMON_HOME/common/bin/wlst.sh"
```

```
connect('USERNAME','PASSWORD','t3://IGDADMINVHN:IGDADMINPORT')
```

Replacing the value of:

USERNAME with the username of the OIG domain admin user

PASSWORD with the password of the OIG domain admin user

IGDADMINVHN with the listen address that the Admin Server runs at

IGDADMINPORT with the port that the Admin Server runs at

Examples for all hosts are listed below, where the variables shown for the below are:

domainDir: The full path of the WebLogic domain operated by this node manager.

nmHome: The full path to the directory where the node manager configuration files reside

- For *OIMHOST1*:

1. Enroll the node manager for the Admin Server's domain home (*IGD_ASERVER_HOME*).

```
nmEnroll(domainDir='IGD_ASERVER_HOME',nmHome='/u01/oracle/config/nodemanager/
IGDADMINVHN')
```

2. Enroll the node manager for the Managed Servers domain home (*IGD_MSERVER_HOME*).

```
nmEnroll(domainDir='IGD_MSERVER_HOME',nmHome='/u01/oracle/config/nodemanager/
OIMHOST1')
```

- For *OIMHOST2*:

1. Enroll the node manager for the Managed Servers domain home (*IGD_MSERVER_HOME*).

```
nmEnroll(domainDir='IGD_MSERVER_HOME',nmHome='/u01/oracle/config/nodemanager/
OIMHOST2')
```

Copying SOA Composites Into the New OIG Domain

For SOA to work properly, it needs to access the required composite JAR files at Managed Server startup. These files were not replicated using T2P and must be replicated manually from the OAM domain in the `IAD_ASERVER_HOME/soa` directory. This entire directory must be copied over to the new OIG domain into both the *IGD_SERVER_HOME* and *IGD_MSERVER_HOMEs* on all OIG hosts. This is shown in IAM Enterprise Deployment Guide chapter 19.3: Copying SOA Composites to Managed Server Directory.

1. On *OAMHOST1*, navigate to *IAD_ASERVER_HOME.*
2. Run: `tar zcvf composites.tgz soa/*.`
3. Copy the `composites.tgz` file to *IGD_ASERVER_HOME* and all *IGD_MSERVER_HOMEs.*
4. Run: `tar zxvf composites.tgz` in all locations where the `composites.tgz` file was copied.

Start all SOA and OIM Managed Servers

Start all SOA and OIM Managed Servers in the new OIG domain by following the steps provided in the following IAM Enterprise Deployment Guide documentation sections:

1. IAM Enterprise Deployment Guide chapter 31.1.6.2: Starting and Stopping Oracle SOA Suite Weblogic Managed Servers
2. IAM Enterprise Deployment Guide chapter 31.1.6.3: Starting and Stopping Oracle Identity Manager Weblogic Managed Servers

> *All node manager processes must be enrolled in the OIG domain and started before starting any Managed Servers.*

Validating the OIM Front End URL Configurations in the Enterprise Manager Console

The T2P `pasteConfig` steps earlier should have set the internal and external OIM URL configurations correctly as customized in the move plan. Validate that the values configured in the OIM application MBeans are set consistently with the ServerName value of the IGD internal VirtualHost configurations on the web tier.

1. Verify the values of *ServerName* in the web tier VirtualHost configurations of the `prov_vh.conf` and `igdinternal_vh.conf` files on all Web Servers. For more information, see IAM Enterprise Deployment Guide chapter 14: Configuring the Oracle Web Tier.
2. Access the OIG domain’s Enterprise Manager application at http://igdadmin.example.com/em.
3. Navigate to **Identity and Access** > **OIM.**
4. Right-click **oim(11.1.2.0.0)**, and select **System MBean Browser.**
5. Under **Application Defined MBeans**, navigate to **oracle.iam** > **Server:[SERVER_NAME]** > **Application:oim** > **XMLConfig** > **Config** > **XMLConfig.DiscoveryConfig** > **Discovery.**
6. Validate the values for the **OimFrontEndURL** and **OimExternalFrontEndURL** attributes. If they match the above mentioned web tier file, no further configuration is required. If they do not match:
   a. Enter the matching value from the `prov_vh.conf` or `igdinternal_vh.conf` files.
   b. Click **Apply** to save the changes.
   c. Restart the OIM Managed Servers.

Updating the OIG Admin Server boot.properties File

Now that the domains have been successfully separated, SSO needs to be re-enabled on the domain. The first step is to set the OIG Admin Server’s credentials to that of the WebLogic admin user set up in the identity store. Follow the instructions in IAM Enterprise Deployment Guide chapter 22.3: Updating the boot.properties File.

1. On the *IGD_ASERVER_HOME* host, go to the directory: `ASERVER_HOME/servers/serverName/security.`
2. Make a pre-SSO backup copy of the `boot.properties` file, in case you need to revert for any reason.
3. Use a text editor to create a file called `boot.properties` under the security directory. Enter the following lines in the file:

   ```
   username=adminUser
   password=adminUserPassword
   ```

   For example:

```
username=weblogic_idm
password=Password for weblogic_idm user
```

Enable SSO

Re-enable SSO by reverting the changes previously performed on the web server in step 1 of the OIG Admin Server Pre-Start Configurations section.

1. If not already started, start the OAM and AMA Managed Servers using the OAM Admin Server. See IAM Enterprise Deployment Guide chapters 31.1.5.2: Starting and Stopping Oracle Access Manager Weblogic Managed Servers and 31.1.5.3: Starting and Stopping Policy Manager Weblogic Managed Servers for more information.
2. Uncomment the following line from the `WEB_ORACLE_INSTANCE/config/OHS/INSTANCE_NAME/httpd.conf` file and restart the OHS instance(s):

   ```
   Include "${WEB_ORACLE_INSTANCE}/config/OHS/${INSTANCE_NAME}/webgate.conf"
   ```

3. Validate that SSO is working properly with all applications in both the OAM and OIG domain applications by accessing several OAM and OIG domain applications with the same login. As expected, a single login should be prompted at the first application access and subsequent application access should not require a login. Ensure that the user that is being used to test SSO has access to all applications that are being tested.

OAM Login Page Link Redirection

In some consolidated domain configurations, a single URL is used for the SSO front-end entry point. When you separate the domains, this configuration must also separated. Once separated, one entry point will point to login.example.com URL and one will point to prov.example.com URL. See IAM Enterprise Deployment Guide chapter 2.3.4: Summary of Oracle Identity and Access Management Load Balancer Virtual Server Names and IAM Enterprise Deployment Guide chapter 14: Configuring the Oracle Web Tier for more information. After enabling SSO, configure a redirection of the links on the OAM login page to the prov.example.com URL. The file that is changed as a result of this configuration is *IAD_ASERVER_HOME/config/fmmconfig/oam-config.xml*. The following steps show how to accomplish the link URL change o the OAM domain:

1. Start the OAM Admin Server, as you would before you ran the T2P script.
2. Run the following from the OAM *ADMINHOST*:
   a. `IAD_ORACLE_HOME/common/bin/wlst.sh`

   WLST must be run from IAD_ORACLE_HOME, as the command to be run is not found in WLST from IAD_MW_HOME/oracle_common.

   b. `connect('USERNAME','PASSWORD','t3://IADADMINVHN:IADADMINPORT')`

   Replacing the value of:

   USERNAME with the username of the OAM domain admin user

   PASSWORD with the password of the OAM domain admin user

   IADADMINVHN with the listen address that the Admin Server runs at

   IADADMINPORT with the port that the Admin Server runs at

   c.
   ```
   updateOIMHostPort(hostName="<HOST_NAME>", port="<PORT_NUMBER>",
   secureProtocol="true")
   ```

Replacing the value of:

HOST_NAME with the OIG prov.example.com URL

PORT_NUMBER with the OIG prov.example.com port (usually 443)

For example:

```
updateOIMHostPort(hostName="prov.example.com", port="443",
secureProtocol="true")
```

3. Validate the change by viewing the following section in the *IAD_ASERVER_HOME/config/fmmconfig/oam-config.xml* file :

   For example:

   ```
   <Setting Name="ServerConfiguration" Type="htf:map">
     <Setting Name="OIM-SERVER-1" Type="htf:map">
       <Setting Name="Host" Type="xsd:string">prov.example.com</Setting>
       <Setting Name="Port" Type="xsd:integer">443</Setting>
       <Setting Name="SecureMode" Type="xsd:boolean">true</Setting>
     </Setting>
   </Setting>
   ```

4. Restart the OAM domain Admin Server, the OAM Managed Servers, and AMA Managed Servers. Once started, validate that the OAM login page link points to the prov.example.com entry point by hovering over the links. Proper functionality validation will occur as part of the overall separated configuration validation.

Validate LDAP Users and Roles in the OIM Self Service Application

As with the admin users in the Admin Server, T2P does not re-configure the LDAP connectivity from OIM to SOA. This can be accomplished by following the instructions in IAM Enterprise Deployment Guide chapter 19.14: Enabling OIM to Connect to SOA Using LDAP User.

At least one OIM Managed Server must be running to complete this procedure.

1. Log in to Enterprise Manager Fusion Middleware Control of the IAMGovernanceDomain, as the **weblogic** user.
2. Select **Farm_IAMGovernanceDomain**, **WebLogic Domain**, and then **IAMGovernanceDomain**.
3. Right-click and Select **System MBean Browser** from the menu, or right-click to select it.
4. Select **Search**, enter **SOAConfig**, then click **Search**.
5. Change the username attribute to the Oracle WebLogic Server administrator username provisioned in Preparing the Identity Store. For example:

   ```
   weblogic_idm
   ```

   Click **Apply**.
6. Select **Weblogic Domain**, and then **IAMGovernanceDomain**.

7. Select **Security** and then **Credentials** from the dropdown menu.

8. Expand the key **oim**.

9. Click **SOAAdminPassword** and click **Edit**.

10. Change the username to `weblogic_idm` and set the password, then click **OK**.

11. From the navigator, click **Farm_IAMGovernanceDomain** and then click **WebLogic Domain**. Right-click on **IAMGovernanceDomain**, and select **Application Roles** from the Security menu.

12. Set the application stripe to `soa-infra` by selecting from the drop-down list. Click **Search**.

13. Click **SOAAdmin**. Ensure that you see **Administrators** in the membership box.

14. Click **Edit**. The Edit page is displayed.

15. Click **Add** in the Members box. The Add principal search box is displayed.

    Enter the following:

    Type: Group

    Principal Name: starts with: IDM

    Click **Search**.

16. Select **IDM Administrators** from the results box, then click **OK**.

    You will be redirected to the Edit screen. Ensure that the members are Administrators and IDM Administrators.

    Click **Ok**.

17. Run the reconciliation process to enable the Oracle WebLogic Server administrator, `weblogic_idm`, to be visible in the OIM Identity Console.

    a. Log in to the OIM System Administration Console as the user `xelsysadm`.

    b. Click **Scheduler** under **System Configuration**.

    c. Enter `LDAP*` in the search box.

    d. Click the arrow for the **Search Scheduled Jobs** to list all the schedulers.

    e. Select **LDAP User Create and Update Full Reconciliation**.

    f. Click **Run Now** to run the job.

    g. Repeat for the job **LDAP Role Create and Update Full Reconciliation**.

    h. Log in to the OIM Identity Console and verify that the user `weblogic_idm` is visible.

18. Log in to the OIM Self Service Console as the user `xelsysadm`.

    If prompted, set up challenge questions. This happens on your first login to Oracle Identity Manager Identity Console.

19. Click on the **Roles** tab under the **Manage** tab.

20. Search for the Administrators role.

    Enter `Administrators` into the **Display Name** search box and click **Search**.

    Click the **Administrators Role** to view the **Role's Properties** page.

21. Click on the **Organizations** tab.

22. Click **Add**. Search and select the organization to which **xelsysadm** belongs, example, **Xellerate Users.**

23. Click **Add Selected**, then click **Select**.

24. Click the **Members** tab and click **Add**.

25. Search for the user **weblogic_idm** . Select the **weblogic_idm** user.

26. Click **Add Selected**.

27. Click **Select**, and then click **Apply**.

Start All OBI Managed Servers

The following assumes that all node managers have been started as part of the Enrolling Node Managers Into Their Respective Domains section above. Follow the instructions in IAM Enterprise Deployment Guide chapter 31.1.6.2: Starting and Stopping Oracle BI Publisher Weblogic Managed Servers to start all of the Oracle BI Publisher Managed Servers.

Note: All node manager processes must be properly enrolled in the domain and started before starting any Managed Servers.

Validate All OAM and OIG Functionality

As your final task, validate functionality and data on the new separated topology. Run any test cases that may exist for your specific environments. A set of generic test cases can be found in IAM Enterprise Deployment Guide Appendix B: Sanity Checks.

Appendix A: Issues and Troubleshooting

Potential issues that you might encounter in the domain separation process and references to possible solutions from Oracle documentation, My Oracle Support articles, and software patches is provided in Table 5: OAM/OIG Domain Separation Troubleshooting, arranged by step or topic.

TABLE 5: OAM/OIG DOMAIN SEPARATION TROUBLESHOOTING

Troubleshooting Item #1: Enabling debug log level in T2P/Cloning scripts

```
T2P_JAVA_OPTIONS="-Dt2p.logging.level=ALL"

export T2P_JAVA_OPTIONS
```

Step	Reference	URL	Solution
All T2P scripting steps	MOS article 662633.1	https://support.oracle.com/epmos/faces/DocumentDisplay?id=1662633.1	N/A

Troubleshooting Item #2: Error in copyConfig log or at command line:

```
Problem invoking WLST - Traceback (innermost last):

File "/tmp/CLONINGCLIENT3620601331018991586/tmp1538497921953.py", line 22, in ?

File "/u01/oracle/products/oracle_common/common/wlst/wsmManage.py", line 712, in
exportRepository

File "/u01/oracle/products/oracle_common/common/wlst/lib/ora_util.py", line 51, in
raiseScriptingException

OracleScriptingException: The MBean oracle.wsm:*,name=WSMDocumentManager,type=Repository was
not found.

FINE : [WLSTCommandUtil:executePyScript] Error while executing the wlst script
/tmp/CLONINGCLIENT3620601331018991586/tmp1538497921953.py

FINE : [OWSMMigrationUtility:exportOWSMMetadata] Error in examining OWSM policies.

FINE : [GenericCopyConfigSteps:addOWSMExportMetadataToArchive] Error in examining OWSM
policies.

FINE : [GenericCopyConfigSteps:introspectGenericJ2EEComps] Error in examining OWSM
policies.Error in examining OWSM policies.

oracle.as.t2p.exceptions.FMWT2PCopyConfigException: Error in examining OWSM policies.Error in
examining OWSM policies.
```

Step	Reference	URL	Solution
T2P copyConfig	MOS article 1456515.1	https://support.oracle.com/epmos/faces/DocumentDisplay?id=1456515.1	Make sure ALL Managed Servers using the mds-owsm datasource (Admin Server, SOA, OIM, BI) are running

Troubleshooting Item #3: Error in pasteConfig log or at command line:

```
SEVERE : ERROR - CLONE-20643 Move plan comparison failed.

SEVERE : CAUSE - CLONE-20643 The move plan xml passed in the argument does not contain the same
meta data as the one present in archive

Meta data property "componentName" from argument move plan is "TARGET_DOMAIN_NAME"

Meta data property "componentName" from archive move plan is "SOURCE_DOMAIN_NAME"

SEVERE : ACTION - CLONE-20643 Make sure the move plan is actually generated from the archive
passed in the argument.

INFO : CLONE-23534 The move plan - SHARED_CONFIG_DIR/T2P/move/moveplan.xml was not extracted
using the archive - SHARED_CONFIG_DIR/T2P/T2P_Domain_Config.

Please extract the move plan once again using the archive -
SHARED_CONFIG_DIR/T2P/T2P_Domain_Config and re-run the script.
```

Step	Reference	URL	Solution
T2P pasteConfig	Error in log	N/A	Ensure that you use the target domain’s DOMAIN_NAME in the top <componentName> of the moveplan.xml file.

Troubleshooting Item #4: Error in pasteConfig log or at command line:

```
ERROR - CLONE-20327   Invalid password file.

CAUSE - CLONE-20327   The DataSource1 password file did not exist or first line did not contain
password.

ACTION - CLONE-20327   Provide a valid password file.
```

Step	Reference	URL	Solution
T2P pasteConfig	MOS article 1609041.1	https://support.oracle.com/epmos/faces/DocumentDisplay?id=1609041.1	Edit moveplan.xml, replacing the values in the </value> XML tags for the "Password File" XML tags

Troubleshooting Item #5: Error in pasteConfig log or at command line:

```
Error Message :1 [PLUGIN][LIBOVD] Error executing LibOVDPasteonfig plug-in

Error Message :2 [PLUGIN][LIBOVD] - ERROR - Specified host already configured in adapter
ldap.example.com:1389

[PLUGIN][LIBOVD] - CAUSE - Specified host already configured in adapter ldap.example.com:1389

Error Message :3 SEVERE - CLONE-20936 "pasteConfig" operation failed for
oracle.ods.virtualization.t2p.LibOVDPasteConfigImpl plugin. Check clone log and error files for
more details.
```

Step	Reference	URL	Solution
T2P pasteConfig	MOS Article 2193594.1	https://support.oracle.com/epmos/faces/DocumentDisplay?id=2193594.1	Apply patch 20461097 to OIG MW_HOME

Troubleshooting Item #6: Out of Memory while running pasteConfig.sh

```
Exception in thread "Thread-1041" SEVERE : SEVERE - CLONE-20936 "pasteConfig" operation failed
for oracle.as.clone.soa.impl.SOAPasteConfigImpl plugin. Check clone log and error files for
more details.

SEVERE : ERROR - CLONE-20218   Cloning is not successful.

SEVERE : CAUSE - CLONE-20218   An internal operation failed.

SEVERE : ACTION - CLONE-20218   Provide the clone log and error file for investigation.

java.lang.OutOfMemoryError: PermGen space
```

Step	Reference	URL	Solution
T2P pasteConfig	T2P Docs	https://docs.oracle.com/cd/E52734_01/core/ASADM/testprod.htm#CACDJDHI	Set PermGen memory to a higher value prior to executing pasteConfig. IE: export T2P_JAVA_OPTIONS="- -XX:PermSize=1024m -XX:MaxPermSize=1024m

Troubleshooting Item #7: LDAP directory server type missing:

```
SEVERE : [PLUGIN][OIM] - ERROR - CLONE-73030  LDAP directory server type value is empty

SEVERE : [PLUGIN][OIM] - CAUSE - CLONE-73030  LDAP directory server type value is not provided
in moveplan.

SEVERE : [PLUGIN][OIM] - ACTION - CLONE-73030  Please provide a proper LDAP directory server
type in moveplan out of following
```

Step	Reference	URL	Solution
T2P pasteConfig	T2P Docs	N/A	Edit moveplan.xml, adding the type of directory server (OUD, etc...)

Troubleshooting Item #8: Database credential issue:

```
[PLUGIN][OIM] - ERROR - CLONE-71000  configuration Failed. Exiting configuration due to data
validation failure.

[PLUGIN][OIM] - CAUSE CLONE-71000  [VALIDATION] [ERROR]:INST-6104: Unable to connect to the
Database with the given credentials. Listener could be down

[PLUGIN][OIM] - ACTION - CLONE-71000  [VALIDATION] [SUGGESTION]:Check the values. Make sure the
Database is up and running and connect string, user name and password are correct.
```

Step	Reference	URL	Solution
T2P pasteConfig	T2P Docs	N/A	Make sure JDBC URLs are in the following format in the moveplan.xml: <value>jdbc:oracle:thin:@scan.example.com:1521/SERVICE_NAME</value>

Troubleshooting Item #9: LDAP Connection Error:

```
[PLUGIN][OIM] - ERROR - CLONE-71000  configuration Failed. Exiting configuration due to data
validation failure.
```

```
[PLUGIN][OIM] - CAUSE - CLONE-71000  [VALIDATION] [ERROR]:INST-6127: Error in connecting to
LDAP.
```

```
[PLUGIN][OIM] - ACTION - CLONE-71000  [VALIDATION] [SUGGESTION]:Enter LDAP URL in proper
format.
```

Step	Reference	URL	Solution
T2P pasteConfig	T2P Docs	N/A	Use the proper LDAP URL format: ldap://ldap.example.com:1389

Troubleshooting Item #10: In OIM Config log (ORACLE_INVENTORY/logs):

```
[2018-11-14T11:48:56.040-08:00] [as] [ERROR] [] [oracle.as.provisioning] [tid: 42] [ecid:
0000MSJkhym8XrS_QDs1yd1Rv7iO000005,0] Exception[[org.quartz.SchedulerConfigException: Failure
occured during job recovery. [See nested exception: org.quartz.JobPersistenceException: Failed
to obtain DB connection from data source 'SeedOracleDS': java.lang.NoClassDefFoundError:
org/apache/commons/collections/CursorableLinkedList [See nested exception:
java.lang.NoClassDefFoundError: org/apache/commons/collections/CursorableLinkedList]]
```

```
Caused by: org.quartz.JobPersistenceException: Failed to obtain DB connection from data source
'SeedOracleDS': java.lang.NoClassDefFoundError:
org/apache/commons/collections/CursorableLinkedList [See nested exception:
java.lang.NoClassDefFoundError: org/apache/commons/collections/CursorableLinkedList]
```

```
[2018-11-14T11:48:56.041-08:00] [as] [ERROR] [] [oracle.as.provisioning] [tid: 42] [ecid:
0000MSJkhym8XrS_QDs1yd1Rv7iO000005,0] Failure occured during job
recovery.[[org.quartz.SchedulerConfigException: Failure occured during job recovery. [See
nested exception: org.quartz.JobPersistenceException: Failed to obtain DB connection from data
source 'SeedOracleDS': java.lang.NoClassDefFoundError:
org/apache/commons/collections/CursorableLinkedList [See nested exception:
java.lang.NoClassDefFoundError: org/apache/commons/collections/CursorableLinkedList]]
```

```
Caused by: org.quartz.JobPersistenceException: Failed to obtain DB connection from data source
'SeedOracleDS': java.lang.NoClassDefFoundError:
org/apache/commons/collections/CursorableLinkedList [See nested exception:
java.lang.NoClassDefFoundError: org/apache/commons/collections/CursorableLinkedList]
```

Step	Reference	URL	Solution
T2P pasteConfig	N/A	N/A	cp IGD_MW_HOME/iam/server/ext/jakarta-commons/commons-collections-3.2.2.jar to IGD_MW_HOME/iam/inventory/Scripts/ext/jlib

Troubleshooting Item #11: xelsysadm user sees error when accessing the OIM System Admin application:

```
You do not have access to Sysadmin application...
```

```
and cannot see the Admin Roles in the Self Service application
```

Step	Reference	URL	Solution
Application Validation	IAM Enterprise Deployment Guide Chapter 19.14	https://docs.oracle.com/cd/E52734_01/core/IMEDG/config_oim.htm#A1016628927	Follow the referenced IAM Enterprise Deployment Guide chapter

Troubleshooting Item #12: Cannot retrieve reports in OIM Self Service app. Error in OIM log:

```
<Warning><oracle.iam.selfservice.uself.uselfmgmt.impl><BEA-000000><URL is not
proper:http://OIMHOST2:9704,OIMHOST1:9704>
```

Step	Reference	URL	Solution
Application Validation	MOS Article 2164640.1	https://support.oracle.com/epmos/faces/DocumentDisplay?id=2164640.1&displayIndex=1#SYMPTOM	Only a single host can be configured as the BI publisher URL.

Troubleshooting Item #13: In BI Logs:

```
<Warning> <oracle.bi.nanserver.fwk.servlet> <BEA-000000> <Failed to load
EndpointManagerConfigLoader [will default back to

using properties files]; java.lang.NoClassDefFoundError:
oracle/bi/endpointmanager/pub/EndpointContext>

WLJMSServiceSecure.getInitialContext is secure: BISystemUser

javax.naming.AuthenticationException [Root exception is
javax.security.auth.login.FailedLoginException: [Security:090304]Authentication Failed: User
BISystemUser javax.security.auth.login.FailedLoginException: [Security:090302]Authentication
Failed: User BISystemUser denied]
```

Step	Reference	URL	Solution
Application Validation	MOS Article 1572993.1 OIM Docs	https://support.oracle.com/epmos/faces/DocumentDisplay?id=1572993.1 https://docs.oracle.com/cd/E21764_01/bi.1111/e10543/privileges.htm#CHDFHDBE	Create an alternative BI System User and configure the new user to execute BI functions via the OIG Admin Console

Appendix B: Referenced Documentation

- *Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*
- *Fusion Middleware Administrator's Guide*
- *Fusion Middleware Administrator's Guide - Moving from a Test to a Production Environment*
- *Fusion Middleware Administrator's Guide - Moving from a Test to a New Production Environment Using Movement Scripts*
- *Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*
- *Creating and Configuring an Oracle Database*
- *Oracle Maximum Availability Architecture (MAA)*
- *MAA Best Practices - Oracle Fusion Middleware*
- My Oracle Support Articles
  - How to Enable Debug Log Level in T2P/CLONING Scripts (Doc ID 1662633.1)
  - Error "oracle.as.t2p.exceptions.FMWT2PCopyConfigException: Error in examining OWSM policies" During 'copyConfig' Phase of Cloning Oracle Fusion Middleware Domain (Doc ID 1456515.1)
  - T2P Pasteconfig for 11.1.1.7 OBIEE environment fails (Doc ID 1609041.1)
  - Pasteconfig.sh Encounters Exception at AMSuiteT2PPasteConfigException (Doc ID 2193594.1)
  - "URL is not proper" Error For BI Publisher on OIM R2PS3 (Doc ID 2164640.1)
  - OBIEE 11g: Error: "[Security:090302]Authentication Failed: User BISystemUser denied" Unable to Log in after LDAP Corruption (Doc ID 1572993.1)

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

- blogs.oracle.com/oracle
- facebook.com/oracle
- twitter.com/oracle
- oracle.com

Hardware and Software, Engineered to Work Together

Oracle Fusion Middleware MAA: Separating Oracle Identity Management Applications Into Multiple Domains
Author: Chuck Boucher

Oracle is committed to developing practices and products that help protect the environment