



Oracle Cloud Infrastructure



Migrating Oracle Identity and Access Management to Oracle Cloud Infrastructure (OCI)

May, 2021 | Version 1.2
Copyright © 2021, Oracle and/or its affiliates
Public

PURPOSE STATEMENT

This document provides a description, a summary of requirements, and the setup procedure for moving Oracle Identity and Access Management (IDM) from an existing deployment into Oracle Cloud Infrastructure (OCI). This paper is oriented to a technical audience having knowledge of Oracle Identity and Access Management, Oracle WebLogic, Oracle Database administration, and basic operating system knowledge.

DISCLAIMER

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates. This document is for informational purposes only and is intended solely to assist you in planning for the implementation and product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

REVISION HISTORY

The following revisions have been made to this technical brief:

Date	Revision	Comments
February 2021	1.0	Initial Release
March 2021	1.1	Feedback Incorporated
May 2021	1.2	Feedback Incorporated

TABLE OF CONTENTS

Purpose Statement	1
Disclaimer	1
Revision History	1
Introduction	4
Assumptions	5
Oracle Internet Directory	5
Oracle Unified Directory	5
Oracle Access Manager	5
Oracle Identity Governance (Formerly Oracle Identity Manager)	5
Oracle Database	5
Oracle Cloud Infrastructure	5
Environment Variables	7
Cloning Strategy	8
Reference Architectures	8
Oracle Internet Directory	8
Oracle Unified Directory	8
Oracle Access Manager	9
Oracle Identity Governance	10
Cloning Approach	10
Oracle Internet Directory	10
Oracle Unified Directory	11
Oracle Access Manager	11
Oracle Identity Governance	12
Source Environment Validation	12
Check for The Use of Host Names	12
Preparing OCI Objects	15
Creating Compute and Database Instances	15
Operating System Configurations	16
Creating the Load Balancer	17
Creating a Secondary IP Address to Support Service Migration	17
OCI Hosts Files	18
Cloning the Source Environment	19
Cloning the Database to OCI	19
Cloning the database using Export/Import	20
Cloning the Source Binaries	29
Cloning the WebLogic Domain	29
Confirm host file overrides on OCI for source hostnames and FQDN	30
Shutdown the Domain Completely	30
Restart the Domain	31
Replicate the backup files to the Target Environment	31
Restore the backups on OCI instances	31
Clean Up Any Lock and Log Files Copied From The Source Environment	32
Start the OCI Cloned Domain	33
Cloning the Oracle Internet Directory Instance	33
Take a backup of the Source Instance Configuration	33
Replicate the backup files to the Target Environment	33
Restore the backups on OCI instances	34
Start the OID instances	34
Cloning Oracle Unified Directory	34
Create an OUD Replica in OCI	34
Grant OUD Changelog Access	35
Create OUD Indexes	35

Validating Access to the Clone Environment	36
Post Clone Tasks	37
Execute the OIM LDAP Consolidated Full Reconciliation Job	37
Migrate OIM Object Cache to Unicast	39
Cutover to OCI	40
Cutover Load Balancers	40
OCI Load Balancer	40
On-Premise Load Balancer	40
References	41

INTRODUCTION

Many customers are looking to move their existing Oracle Fusion Middleware deployments to Oracle Cloud Infrastructure (OCI). There are many approaches to accomplishing this, and customers often take the opportunity to upgrade the components as part of the exercise. This technical brief is concerned only with copying your existing deployment to OCI. The purpose of this paper is to show an approach which involves the minimum amount of reconfiguration necessary to clone your existing environment to OCI. The source environment can reside on-premise hardware or other cloud platforms.

This paper describes a solution for the preparation, installation, and configuration procedures, as well as operational best practices for moving Oracle Identity and Access Management into Oracle Cloud Infrastructure (OCI). The originating configuration will have the same version in both the source system and OCI.

The solution involves cloning both the database and Identity and Access Management installation. Should you wish to perform an upgrade to a later version at reduced risk, then the procedures in this paper can be used to take a clone of your environment. Afterwards you can use the documented in place upgrade guides to upgrade the environment to your targeted release.

This approach should be practiced prior to performing for real. The approach has minimal impact on your running system so can be repeated as many times as necessary to gain confidence in the process.

Whilst the process identified in this document is targeted at Oracle Identity and Access Management the concepts and procedures can be applied to any type of Oracle Fusion Middleware deployment.

This document covers several different topics, including OCI object creation and administration, Oracle Fusion Middleware (FMW) installation, configuration, and administration, and Oracle Database administration. The solution involves cloning your system to OCI.

During the cloning process a short outage may be required to take a consistent backup of the of the environment, this may depend on the type of backup performed. Oracle recommends a full shut down of the WebLogic Server domain when taking the backup of a WebLogic domain. The duration of the outage will depend on multiple factors including the size of your deployment, domain restart times to name a few. Maintenance outage duration may be reduced if the source database and WebLogic Server domain can be cloned in parallel.

The approach in this document relies on host name equivalence, and as such the approach can be followed for both stand alone and integrated environments and could be used to provide an incremental approach. The approach identified in this document can be followed for both single instance/single host deployments as well as highly available multi-host deployments.

Please note, the solution identified in this paper is a point in time clone. Once the clone has been deployed changes made to the existing system will not be replicated to the cloned system. Certain procedures could be adapted to meet this requirement, but this is outside of the scope of this paper.

Assumptions

This document covers the following environment configurations and assumes that the majority of administrators planning to move Oracle Identity and Access Management into OCI are using similar configurations.

It is important to note that to simplify this migration, host names will remain the same in OCI as they are in the source system. Any configurations using hard-coded IP addresses should be reviewed and updated in the source environment to use host names or FQDN prior to performing the cloning operations provided in this document. If you have followed the recommendations in the Enterprise Deployment guide then you will be using virtual host names, if however, you have not followed this approach then the process detailed in this paper can still be followed.

The cloned environment will be an exact copy of the source environment. If you have 10 hosts/VMs in your source environment, you will have 10 hosts/VMs in your OCI environment.

Oracle Internet Directory

Oracle Internet Directory is configured as part of an enterprise or highly available (HA) deployment. An enterprise deployment would have several instances configured over several nodes, mainly for the purpose of scaling or high availability. However, users may have all applications deployed on single server configurations.

Oracle Unified Directory

Oracle Unified Directory is configured as part of an enterprise or highly available (HA) deployment. An enterprise deployment would have several instances configured over several nodes, mainly for the purpose of scaling or high availability. However, users may have all applications deployed on single server configurations.

Oracle Access Manager

Oracle Access Manager is configured as part of an enterprise or highly available (HA) deployment. An enterprise deployment would have several instances configured over several nodes, mainly for the purpose of scaling or high availability. However, users may have all applications deployed on single server configurations.

Oracle Identity Governance (Formerly Oracle Identity Manager)

Oracle Identity Governance is configured as part of an enterprise or highly-available (HA) deployment. An enterprise deployment would have several instances configured over several nodes, mainly for the purpose of scaling or high availability. However, customers may have all applications deployed on single server configurations. Whilst customizations are not covered explicitly in this document, because the procedure uses a cloned approach customizations should still work in the cloned environment.

Oracle Database

As with Oracle Internet Directory and Oracle Access Manager, Oracle Database may be set up as part of an HA deployment. In the case of Oracle Database, HA is accomplished with Oracle Grid Infrastructure and an Oracle Real Application Cluster (RAC). However, customers may also have their databases deployed in a single node configuration.

Oracle Cloud Infrastructure

Users should have a certified license agreement for Oracle Cloud Infrastructure and a basic knowledge of OCI administration. See [Oracle Cloud Infrastructure Documentation](#) for more information.

This document is concerned with the processes of copying an existing Oracle Identity and Access Management deployment from one set of hardware to another. In this document we are demonstrating the move to Oracle Cloud Infrastructure (OCI). Where appropriate, OCI information has been included. This document does not include all of the best practices associated with deploying applications to OCI. For example, there is no reference to topics such as security rules determining how you block/allow access to the internet and how you lock down access to the compute instances/services. You should refer to

the [Oracle Cloud Infrastructure Documentation](#) and Oracle Technical briefs on the best practices associated with deploying applications in OCI.

Environment Variables

Administrators of Oracle Identity and Access Management should be familiar with various environment variables that need to be configured on each host or OCI Compute Instance hosting FMW products. These variables are required when referencing the Oracle documentation and make executing tasks much simpler. The following is a listing of the environment variables required for the lift and shift configuration.

ORACLE_HOME: The location of the base of the 11g Oracle Identity installation.

For example:

```
/u01/oracle/products/identity
```

JAVA_HOME: The location of the base Java installation.

For example:

```
/u01/oracle/products/jdk
```

ASERVER_HOME: The base location of the WebLogic domain configuration.

For example:

```
/u01/oracle/config/domains/IAMGovernanceDomain
```

MSERVER_HOME: The location of the WebLogic domain configuration where managed servers are started from

For example:

```
/u02/private/oracle/config/domains/IAMGovernanceDomain
```

NOTE: Having 2 domain directories is the recommendation in the Oracle Enterprise Deployment Guide, if you have a single instance deployment or a deployment that has not followed the practices outlined in the Enterprise Deployment Guide then you may only have one DOMAIN_HOME directory.

APPLICATION_HOME: The location of the domain's application files

For example:

```
/u01/oracle/config/applications/IAMGovernanceDomain
```


CLONING STRATEGY

The following is an overview of the tasks required to clone Oracle Identity and Access Management into OCI from an on-premises implementation. The procedure is version agnostic.

Reference Architectures

The source domain and database topology and scaling may differ from the reference Oracle Enterprise Reference Architecture for Oracle Identity & Access Management.

Oracle Internet Directory

Figure 1: The High-Level Oracle Internet Directory Migration Topology below is an example architecture. Scaling may differ from a user's implementation.

Note: Export and import only need to be configured from one Oracle Internet Directory instance in the on-premises environment to one instance in the OCI environment. All other instances in the OCI environment will synchronize the data from the database, which serves the cluster.

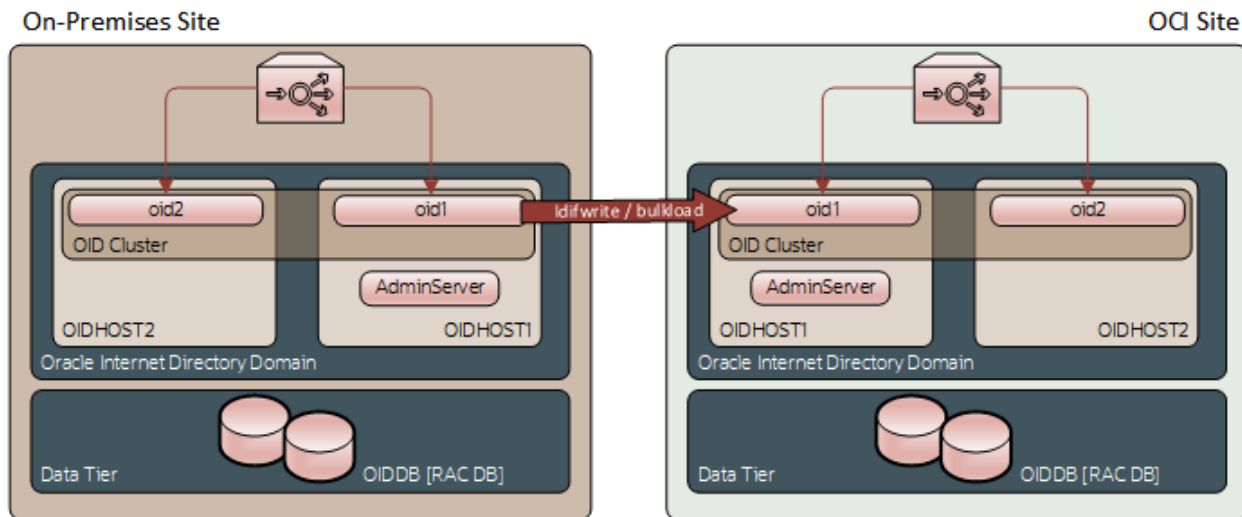


Figure 1: High-Level Oracle Internet Directory Topology

Oracle Unified Directory

Figure 2: The High-Level Oracle Unified Directory Migration Topology below is an example architecture. Scaling may differ from a user's implementation.

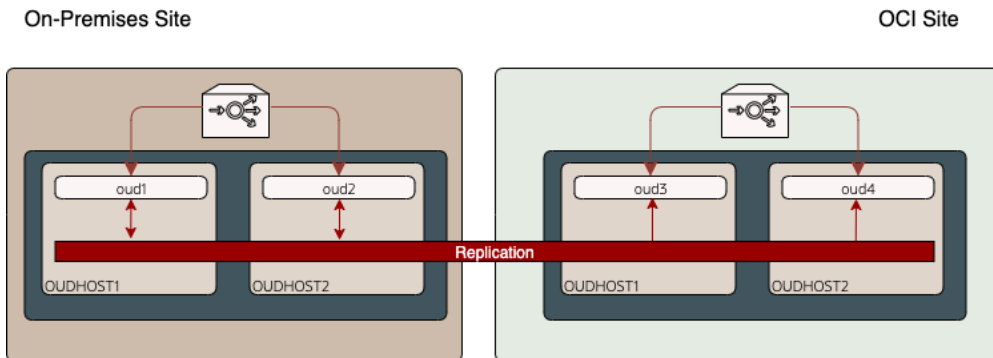


Figure 2: High-Level Oracle Unified Directory Topology

Oracle Access Manager

Figure 3: High-Level Oracle Access Manger example architecture. Scaling may differ from a user's implementation.

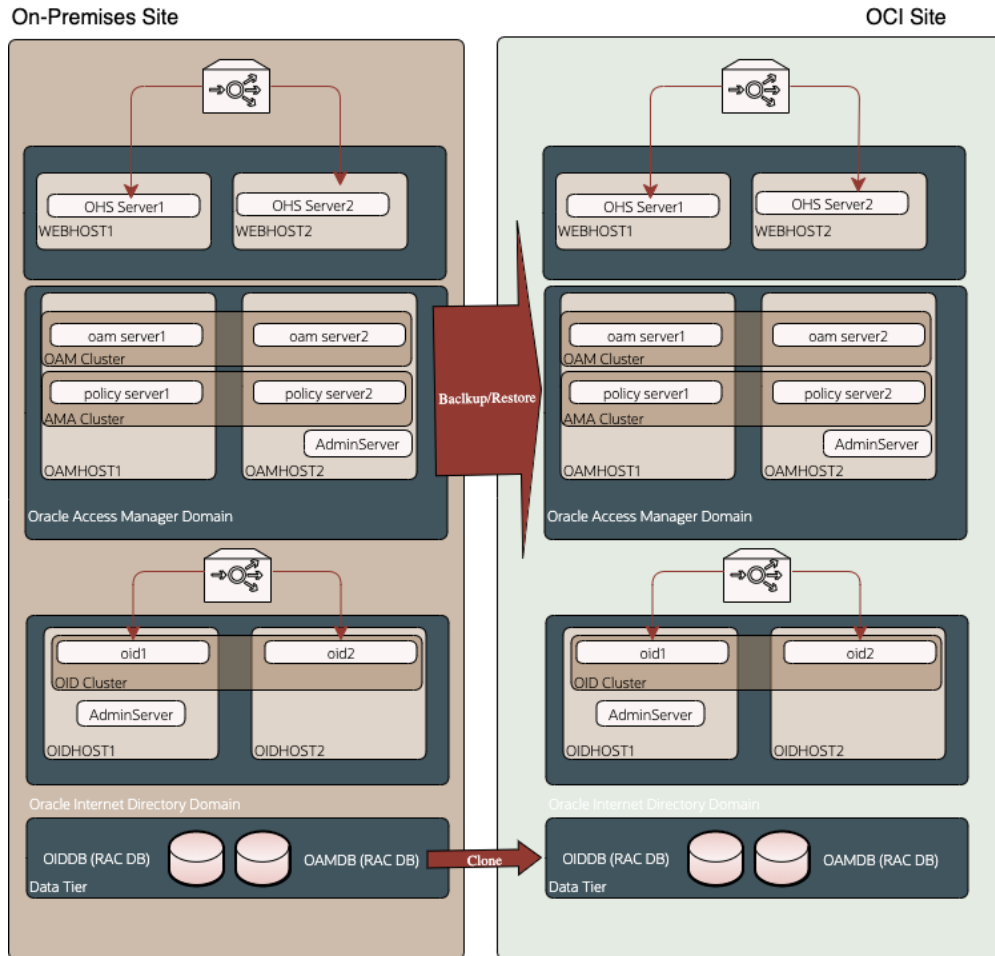


Figure 3: High-Level Oracle Access Manager Topology

Oracle Identity Governance

Figure 4: High-Level Oracle Identity Governance example architecture. Scaling may differ from a user's implementation.

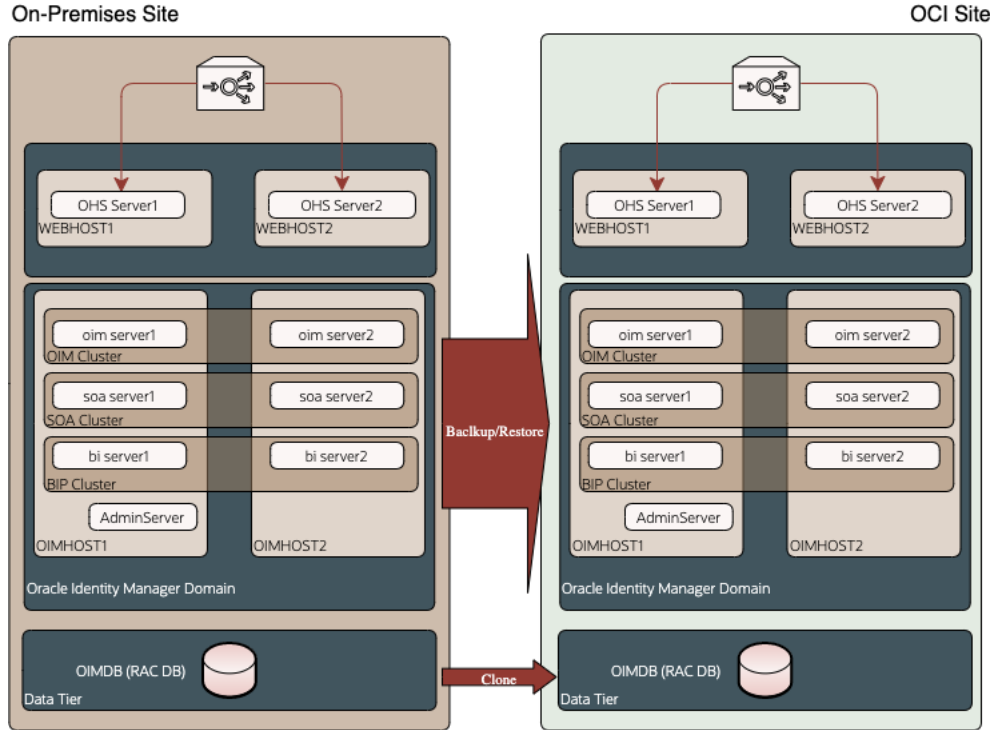


Figure 4: High-Level Oracle Identity Governance Topology

Cloning Approach

Oracle Internet Directory

There are several approaches which could be considered for Oracle Internet directory.

Approach 1 – Backup and Restore

- Backup the existing Oracle Database Objects and Restore to OCI.
- Backup and restore the Oracle Internet Binaries to the OCI instance.
- Backup and restore the Oracle Internet Directory instance/Domain to the OCI instance.
- Start up the Database and the instances on OCI

Approach 2 – Dataguard

- Create a Dataguard copy of the source database and restore to OCI
- Enable Database replication from the source system to OCI
- Backup and restore the Oracle Internet Binaries to the OCI instance.
- Backup and restore the Oracle Internet Directory instance/Domain to the OCI instance.
- Switchover to the Database on OCI
- Start Oracle Internet Directory instances in OCI.

Approach 3 – OID Replication

- Install Oracle Internet Directory on the target system.
- Set up Oracle Internet Directory replication between the source and target systems.

The advantage of Approach 1 is that the OCI system is an exact copy of the target system, therefore all interactions with that system will remain the same, the downside is that any changes to the primary system are not replicated to the OCI system. So, the version on OCI is a point in time replica.

Approaches 2 and 3 allow changes applied on the source system to be continually applied to the target system. In approach 2 this will be via the database and in approach 3 this will be via OID's replication mechanism.

Approach 2 results in an exact copy of the source system so all interactions with that system will remain the same. The downside is that because the entire database must be part of the Dataguard configuration then all data in that database will be replicated.

Approach 3 allows just the OID data to be replicated, the replication should be one way to avoid conflict resolution. The downside to approach 3 is that both OID installations will generate different changelogs. Oracle Identity Governance relies on these change logs for reconciliation. If this approach were to be adopted, then if you are also using Oracle Identity Governance then you would need to perform a full reconciliation against the new directory upon cutover.

Oracle Unified Directory

Oracle Unified directory maintains a loosely coupled replication mechanism along with a cookie-based change log. This is ideal for migration to other systems. The approach for Oracle Unified Directory cloning is:

- Install the Oracle Unified Directory binaries on your target OCI system.
- Create new OUD instance(s) on your target OCI system.
- Enable replication between your source system and OCI.
- Create any additional indexes or access permissions on your target OCI instances.

Data created on your source system will automatically be replicated to your target OCI system. Cutover just involves using the OCI OUD instances rather than the source ones and removing the source systems from the replication configuration.

Oracle Access Manager

There are two approaches that can be followed for Oracle Access Manager.

Approach 1 – Backup and Restore

- Backup the existing Oracle Database Objects and Restore to OCI.
- Backup and restore the Oracle Identity and Access Management binaries to the OCI instance.
- Backup and restore the Oracle Access Management Domain to the OCI container.
- Start up the Database and the domain on OCI.

Approach 2 – Multi Datacenter

- Backup and restore the Oracle Identity and Access Management binaries to the OCI instance.
- Create Access Management Schemas in a database in OCI
- Create an Access Manager domain in OCI
- Set up Multi-datacenter between the source site and OCI.

Approach 1 ensures an identical copy of Oracle Access Manager at a point in time. On-going changes will not be propagated to the OCI system.

Approach 2 creates two identical systems both running active-active. Changes made on the primary system will be replicated to the target system until cutover. Cutover will involve making the OCI OAM deployment the OAM Source system and directing requests to it.

This paper will not address Approach 2, should you wish to use Approach 2 then refer to the Oracle documentation on setting up Oracle Access Manager multi-datacenter.

Oracle Identity Governance

There is only one approach considered for Oracle Identity Governance and that is:

Approach 1 – Backup and Restore

- Backup the existing Oracle Database Objects and Restore to OCI.
- Backup and restore the Oracle Identity and Access Management binaries to the OCI instance.
- Backup and restore the Oracle Identity Governance Domain to the OCI instance.
- Start up the Database and the domain on OCI.

SOURCE ENVIRONMENT VALIDATION

Check for The Use of Host Names

The cloning solution in this paper relies on the use of host names and not IP addresses in all configuration properties. Validate the various domain and application configuration parameters in the source environment to assure there are no IP addresses directly configured. If IP addresses are found to be in-use, then the source environment must be updated the prior to beginning the cloning process.

Audit the WebLogic Server Domain Configuration

Verify the domain is not configured with IP addresses for the various listener, nodemanager, data source host/SCAN/ONS parameters, etc...As customer configurations vary in scope and the number of parameters to review are too enumerate specifically, only a basic audit process can be provided here. A simple search of the domain configuration files for each known hostname, or by domain name, IP address list, or network range can provide a quick report.

From the example host file below, the source environment might have host records such as:

```
# On-Prem Host Entries
10.99.5.42  srchost27.example.com srcHost27  webhost1
10.99.5.43  srchost28.example.com srcHost28  webhost2
10.99.5.44  srchost20.example.com srcHost20  ldaphost1
10.99.5.45  srchost21.example.com srcHost21  ldaphost2
10.99.5.46  srchost23.example.com srcHost23  oamhost1
10.99.5.47  srchost24.example.com srcHost24  oamhost2
10.99.5.48  srchost25.example.com srcHost25  oimhost1
10.99.5.49  srchost26.example.com srcHost26  oimhost2

# Compute VNIC Secondary IP for AdminServer floating VIPs
10.99.5.61 srcVIPIad.example.com srcVIPIad
10.99.5.62 srcVIPigd.example.com srcVIPigd

# Database Systems with on-prem override aliases
10.99.5.20 src-DB-SCAN.example.com src-DB-SCAN
# Load Balancer IP
```

```
10.99.5.6 prov.example.com login.example.com idstore.example.com iadadmin.example.com
igdadmin.example.com iadinternal.example.com igdinternal.example.com
```

Values to check for can be written to a file for easy command-line use. Include the corporate network range, partial domain names, and partial strings from any corporate host naming convention that might be relevant; then execute a search of all XML configuration files from the DOMAIN_HOME/config folder.

```
cat << EOF > /tmp/domainHostNameSearchList.txt
10.99.
.example.com
srcHost
webhohst
ldaphost
oamhost
oimhost
EOF

cd /u01/oracle/config/domains/domain_name/config
find .-name "*.xml" -exec grep -H -f /tmp/domainHostNameSearchList.txt {} \;
```

This will result in a list of configuration file paths/names, and the line the text is found on. The resulting list should include machine and listen-address entries, JDBC URLs, ONS Node List entries (if using Gridlink JDBC Drivers), and likely others.

```
./config.xml: <machine>OIMHOST1</machine>
./config.xml: <listen-address>OIMHOST1</listen-address>
./config.xml: <arguments>-Dtangosol.coherence.wka1=OIMHOST1 -
Dtangosol.coherence.wka2=OIMHOST2 -Dtangosol.coherence.localhost=OIMHOST1 -
Dtangosol.coherence.wka1.port=8089 -Dtangosol.coherence.wka2.port=8089 -
Dtangosol.coherence.localport=8089</arguments>
./config.xml: <machine>OIMHOST1</machine>
./config.xml: <listen-address>10.99.5.48</listen-address>
./config.xml: <machine>OIMHOST1</machine>
./config.xml: <listen-address>OIMHOST1</listen-address>
./config.xml: <name>OIMHOST2</name>
./config.xml: <name>OIMHOST2</name>
./config.xml: <listen-address>srcHost26</listen-address>
./jdbc/mds-soa-jdbc.xml:
<url>jdbc:oracle:thin:@(DESCRIPTION=(ENABLE=BROKEN)(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=
src-DB-SCAN.example.com)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=igdupgdb.example)))</url>
./jdbc/mds-soa-jdbc.xml: <ons-node-list>src-DB-SCAN.example.com:6200</ons-node-list>
```

Verify all entries are using hostnames, either short or fully-qualified are fine. These are the values that must be confirmed in the OCI host files.

Note: Any configurations specifying IP Addresses should be corrected in the source system prior to cloning.

Audit the Application Configuration Data Stored in Metadata Service (MDS)

Oracle Identity and Access Management stores configuration details in a Fusion Middleware Metadata Store (MDS) database schema. These configuration details include endpoint URI and JDBC connection strings that include should be reviewed and validated prior to cloning the environment. The hosts referenced in these URI and connection strings must be configured as hostnames or fully-qualified domain names (FQDN) rather than IP addresses. If IP addresses are used, they cannot be overridden in the target OCI environment and would have to be changed during the cloning process.

These parameters can be reviewed one-by-one in the Enterprise Manager System MBean Browser, or exported en-masse and quickly searched via WLST from the command line.

It is recommended to correct the source environment to replace any hard-coded IP addresses with appropriate host names prior to the cloning maintenance. The example given below is for Oracle Identity Governance.

To audit the stored metadata configuration for OIG via WLST:

1. Log into an OIM host in the source environment as the OS user with privileges to the ORACLE_HOME directory
2. Create a temporary working directory

```
mkdir -p /tmp/mds/oig/
```
3. Connect to the AdminServer via WLST

```
$ ORACLE_HOME/common/bin/wlst.sh  
wls:/offline> connect()  
Please enter your username :weblogic_idm  
Please enter your password :  
Please enter your server URL [t3://localhost:7001] :t3://igdadminvhn:7001  
Connecting to t3://igdadminvhn:7001 with userid weblogic_idm ...  
Successfully connected to Admin Server 'AdminServer' that belongs to domain  
'IAMGovernanceDomain'.  
wls:/IAMGovernanceDomain/serverConfig>
```
4. Export the OIM configuration XML data from the FMW Metadata Store and exit from WLST.
 - Application='OIMMetadata'
 - server='WLS_OIM1' (your server name may vary)
 - toLocation='/tmp/mds/oim'
 - docs= '/db/oim-config.xml'

For example:

```
wls:/IAMGovernanceDomain/serverConfig> exportMetadata(application='OIMMetadata',  
server='WLS_OIM1', toLocation='/tmp/mds/oim', docs='/db/oim-config.xml')
```

Executing operation: exportMetadata.

Operation "exportMetadata" completed. Summary of "exportMetadata" operation is:
1 documents successfully transferred.

List of documents successfully transferred:

```
/db/oim-config.xml
```

```
wls:/IAMGovernanceDomain/serverConfig> exit()
```

5. Create a file of search terms to be used to filter for the relevant data from the OIM configuration
There are a lot of configuration elements in the exported XML file. Create a short list to use for filtering.
Note: the "<" character in the example is not a typo.

For example:

```
$ cat << EOF > /tmp/mds/oig/grepHostValidationTerms.txt  
<directDBConfigParams  
bIPublisherURL  
oimFrontEndURL  
oimExternalFrontEndURL  
oimJNDIURL  
backOfficeURL  
accessServerHost  
tapEndpointUrl  
soapurl
```

```
rmiurl
host
serviceURL
EOF
```

6. Search the OIM configuration data using the search terms

For example:

```
$ grep -f /tmp/mds/oig/grepHostValidationTerms.txt /tmp/mds/oig/db/oim-config.xml
```

```
<directDBConfigParams checkoutTimeout="1200"
connectionFactoryClassName="oracle.jdbc.pool.OracleDataSource"
connectionPoolName="OIM_JDBC_UCP" driver="oracle.jdbc.OracleDriver" idleTimeout="360"
maxCheckout="1000" maxConnections="5" minConnections="2" passwordKey="OIMSchemaPassword"
sslEnabled="false" url="jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=src-DB-
SCAN.example.com))(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=igdupgdb.example)))"
username="IGDUPG_OIM" validateConnectionOnBorrow="true">
<bIPublisherURL>http://OIMHOST2:9704,OIMHOST1:9704</bIPublisherURL>
<oimFrontEndURL>http://igdinternal.example.com</oimFrontEndURL>
<oimExternalFrontEndURL>https://prov.example.com:443</oimExternalFrontEndURL>
<oimJNDIURL>@oimJNDIURL</oimJNDIURL>
<backOfficeURL/>
<accessServerHost>srcHost23</accessServerHost>
<tapEndpointUrl>https://login.example.com:443/oam/server/dap/cred_submit</tapEndpointUrl>
<soapurl>http://OIMHOST2:8001</soapurl>
<rmiurl>cluster:t3://cluster_soa</rmiurl>
<host>@oaacghost</host>
<serviceURL>@oaacgserviceurl</serviceURL>
```

7. Review the search results, verify all configuration properties use appropriate hostnames or fully-qualified domain names.
Note: some properties may have placeholder values (e.g. @oaacghost or @oaacgserviceurl). These are okay as-is.
Note: the <rmiurl> URI specified is typically a WLS t3 protocol URI addressed to a WLS server name or cluster name and does not use a hostname. This is also okay as-is.

PREPARING OCI OBJECTS

Before any installation and configuration of software can begin, objects need to be created in your OCI tenancy. Obtaining a tenancy, creating users, and configuring the virtual networking and are not in scope for this document. Refer to the [Oracle Cloud Infrastructure Documentation](#) for more information.

Creating Compute and Database Instances

In OCI, a server host is referred to as a compute instance. For each compute instance creation, there are several options for instance images and shapes. An image is the operating system that is installed on the compute instance and a shape is the compute instance type; virtual machine or bare metal, and the resources, CPU and memory, configured on the compute instance. For each Oracle Identity Governance host that is configured in the user's on-premises environment, a matching number of compute instances should be created in the OCI site. The choice of operating system should be maintained. However, the version of the operating system can be upgraded according to the [Oracle Fusion Middleware Supported System Configurations](#) matrices. Instance selection and creation is not in scope for this document, as the needs of each customer differ.

Likewise, each database node configured in the source environment should have a matching number of database instances created in OCI. Like compute instances, you have a choice of instance types. These are virtual machines, bare metal machines, and Exadata machines. Instance selection and creation is not in scope for this document, as the needs of each customer differ.

Each compute instance that is created needs equivalent storage created for it. The choice of storage type used, and the sizing of the storage is up to the user and is not in scope for this document. Refer to [Cloud Storage](#) for more information. Mount points for the storage should match that of the hosts in the on-premise environment as to allow for the direct copy of the WebLogic Server domain as-is.

Operating System Configurations

There are several operating system requirements that need to be configured in order to perform certain aspects of the installation and configuration in the OCI compute and database instances. The following are detailed descriptions of each.

Configuration to enable Pluggable Authentication Modules (PAM)

Assure that PAM is enabled for the SSH daemon on all hosts.

1. Log in to the instance
2. Open `/etc/ssh/sshd_config` in your favorite editor
3. Search for the line that has the `UsePAM` parameter
4. If commented, remove the comment from the beginning of the line
5. Verify the `UsePAM` parameter value to `Yes`. Change the value if set to `No`.
6. Save the file

Note: restart of SSHD will occur in the next section.

OS Packages consistency between Source and Target Hosts

Compare the deployed OS packages, identify any gaps or differences, and correct as necessary.

Required Linux Operating System Settings for Fusion Middleware Operation

The following configurations are requirements for Fusion Middleware 12c.

1. Edit the `/etc/sysctl.conf` file, adding the following:
`kernel.sem 256 32000 100 142`
`kernel.shmmax = 4294967295` (minimum requirement)
2. Activate the changes by executing: `/sbin/sysctl -p`
3. Edit the `/etc/security/limits.conf` or `/etc/security/limits.d/20-nproc.conf` file, depending on the OS version. Verify and set these parameters to these values or higher as required.
`* soft nofile 32767`
`* hard nofile 327679`
`* soft nproc 2047`
`* hard nproc 16384`

Instance Firewall Rules for Linux Compute Instances

As SELINUX is enabled by default in all Linux compute instances, for each port that needs to be accessed from outside of the instance, a firewall rule needs to be created on the compute instance. The steps to configure the rules are:

1. Verify the full set of service listener ports on every host in your source OIG Domain as root with the command:
`netstat -tulpn | grep LISTEN | grep java | sort -n`

Default ports for WebLogic Server, Oracle Identity Governance, SOA, and BIP include: 5556, 7001, 7010, 8001, 8089, 8090, 9704, 14000, 46067

2. For every port that needs to be accessed, execute:
`sudo firewall-cmd --permanent --add-port=YOUR PORT/tcp`
For example
`sudo firewall-cmd --permanent --add-port=7001/tcp`
3. Restart the firewall service after all ports are configured by executing:

```
sudo systemctl restart firewalld
```

4. Validate the firewall configuration by executing the following:

```
sudo firewall-cmd --list-ports
```

Users and Groups for Linux Compute Instances

It is not mandatory to have the same users and groups configured in your OCI instances as in your on-premise installation however it can simplify things as we clone the 11g installation. To this end it is recommended that the same Account Owners and groups are created in your OCI instance. To create the oinstall group and oracle user with matching UID/GID for your source environment, the following procedure can be used:

```
sudo groupadd -g 1002 oinstall
sudo adduser -u 1001 -g oinstall -G oinstall oracle
```

Creating the Load Balancer

In a high availability configuration Oracle Identity and Access Management will reside behind an Oracle HTTP server which will be used to route requests to the Oracle Identity and Access Management WebLogic components. Access to the Oracle HTTP servers will be via a load balancer. This can either be inside OCI or you can use your existing on-premise load balancer to direct requests to your new OCI deployment at cut-over.

For details of using a load balancer with Oracle Identity and Access Management refer to the [Oracle Enterprise Deployment Guide](#).

Creating a Secondary IP Address to Support Service Migration

If your source installation uses a virtual IP addresses for your WebLogic administration server, or other services as described in the [Oracle Enterprise Deployment Guide](#) then you will need to create a similar Secondary IP address in OCI on the primary VNIC for the appropriate compute instance.

To do this:

1. From the OCI console navigate to: **Compute - Instances - Instance Details - Attached VNICs - VNIC Details - IP Addresses** for one of your compute instances that will run the AdminServer for the domain (e.g. OIMHOST1).
2. Click Assign Private IP address
3. Set the host name to IGDADMINVHN or whatever name you are using. Everything else can be left as the default.
4. Click assign and verify you see the new IP address assigned.
5. Log-in to the compute instance.
6. Assign the IP address to your active VNIC (check using ip addr).

For example, if your main VNIC is **ens3** then you can use the following command to assign the new secondary IP address to that interface.

```
sudo ip addr add 10.0.2.21 dev ens3 label ens3:0
```

7. Verify the assignment with the command:

```
ip addr
```

8. Create an entry in the /etc/hosts file consistently on all hosts for the new IP address, OCI hostname, and source environment fully-qualified hostname used in the domain configuration. See the section on OCI Hosts Files below for more information.

```
10.0.2.21 igdadminvhn.idm.tenant.oraclevcn.com igdadminvhn srcVIPigd.example.com srcVIPigd
```

Summary of OCI Objects

The topology and placement of OCI objects in your deployment may vary depending on the current number of Availability Domains available in your choice of regional Oracle Cloud Infrastructure data center. Examples shown here include

topologies when multiple Availability Domains are provided, and the use of Fault Domains when only a single Availability Domain is provided. Please note that cross-region High Availability is out-of-scope for this paper.

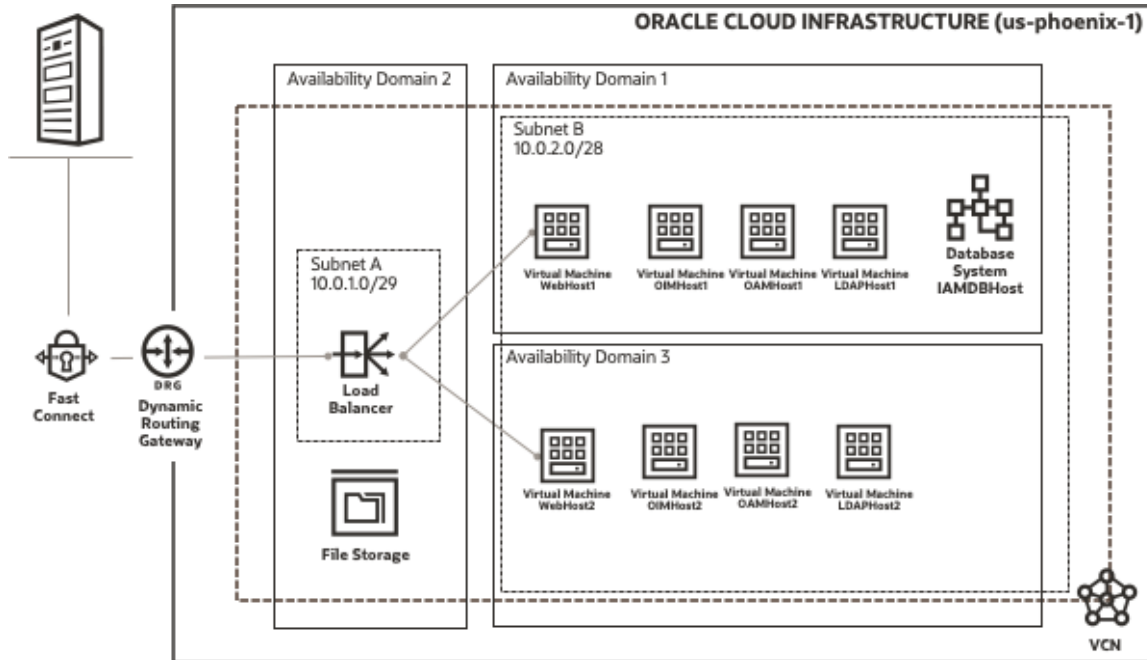


Figure 1 - OCI Topology with multiple Availability Domains

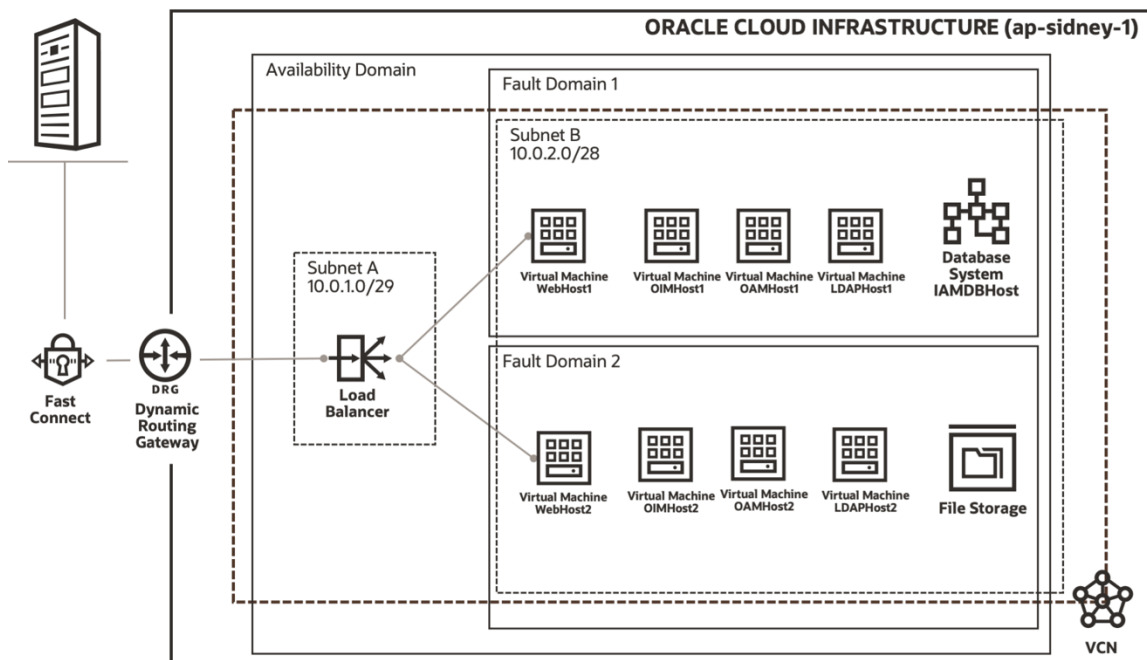


Figure 2 - OCI Topology with a single Availability Domain

OCI Hosts Files

It is imperative in a cloned environment situation that the referenced host names in OCI are the same as the host names in your source system. This is the key to the cloning strategy. If you have followed the recommendations in the Enterprise

Deployment Guide and used virtual host names for all configurations, then this is simply a matter of aliasing these entries to the real OCI host names. For example:

```
10.0.2.17 oimhost1.idm.tenant.oraclevcn.com oimhost1
```

If you are using physical host names in your source WebLogic configuration then you must alias these names to the real OCI host names. For example:

```
10.0.2.17 oimhost1.idm.tenant.oraclevcn.com oimhost1 srchost25.example.com srcHost25
```

In addition, if you source environment has additional floating VIPs and FQDN for the AdminServer's Machine listen address and Node Manager host declaration, then OCI Secondary IP addresses should be configured on the VNICs for the appropriate OCI compute instances and added to the hosts file. These secondary IP address entries should also include the source environment FQDNs and hostnames to override DNS when connecting to your AdminServer.

```
10.0.2.21 igdadminvhn.idm.tenant.oraclevcn.com igdadminvhn srcVIPigd.example.com srcVIPigd
```

An example `/etc/hosts` file:

```
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

# Compute with on-prem override aliases
10.0.2.11 webhost1.idm.tenant.oraclevcn.com webhost1 srchost27.example.com srcHost27
10.0.2.12 webhost2.idm.tenant.oraclevcn.com webhost2 srchost28.example.com srcHost28
10.0.2.13 ldaphost1.idm.tenant.oraclevcn.com ldaphost1 srchost20.example.com srcHost20
10.0.2.14 ldaphost2.idm.tenant.oraclevcn.com ldaphost2 srchost21.example.com srcHost21
10.0.2.15 oamhost1.idm.tenant.oraclevcn.com oamhost1 srchost23.example.com srcHost23
10.0.2.16 oamhost2.idm.tenant.oraclevcn.com oamhost2 srchost24.example.com srcHost24
10.0.2.17 oimhost1.idm.tenant.oraclevcn.com oimhost1 srchost25.example.com srcHost25
10.0.2.18 oimhost2.idm.tenant.oraclevcn.com oimhost2 srchost26.example.com srcHost26

# Compute VNIC Secondary IP for AdminServer floating VIPs
10.0.2.20 iadadminvhn.idm.tenant.oraclevcn.com iadadminvhn srcVIPIad.example.com srcVIPIad
10.0.2.21 igdadminvhn.idm.tenant.oraclevcn.com igdadminvhn srcVIPigd.example.com srcVIPigd

# Database Systems with on-prem override aliases
10.0.2.19 iamdbhost.idm.tenancy.oraclevcn.com iamdbhost src-DB-SCAN.example.com src-DB-SCAN

# Load Balancer IP
10.0.1.10 prov.example.com login.example.com idstore.example.com iadadmin.example.com
igdadmin.example.com iadinternal.example.com igdinternal.example.com
```

Note: Ensure that entries for each of the OCI compute instances and DB Host/SCAN addresses are present in the host file for all hosts in the topology.

CLONING THE SOURCE ENVIRONMENT

Cloning the Database to OCI

Cloning Oracle Internet Directory, Oracle Access Manager and Oracle Identity Governance involve cloning your source database to OCI.

There are multiple ways of doing this and each has their different merits. Below is a list of the options which can be used:

Option 1 – Database Export Import

- Suitable for smaller sized databases
- Allows movement between versions for example 12.1.0.3 to 19c
- Allows movement into Container Databases / Private Databases on a per-application / per-PDB basis
- Is a complete copy. Re-doing the exercise requires data to be deleted from the target each time
- No on-going synchronization
- During Cut-over the source system will need to be frozen for updates
- Shutdown of the WLS domain is recommended during database export

Option 2 – Duplicate Database using RMAN

- Suitable for any size of database
- Takes a backup of an entire database
- Database upgrades will need to be performed as a separate task
- CDB/PDB migration will have to be done after restoring.
- No On-going synchronization
- During Cut-over the source system will need to be frozen for updates

Option 3 – Dataguard Database

- Suitable for any size of database
- Takes a backup of an entire database
- Database upgrades will need to be performed as a separate task
- CDP/PDB migration will have to be done as a separate exercise.
- On-going synchronization. Database can be opened to test the upgrade and closed again to keep data synchronized with the on-premise source

For the purposes of this technical brief we will describe using export/import. For information on the other solutions refer to:

[Database Backup and Recovery Users Guide](#)
[Dataguard Concepts and Administration](#)

Cloning the database using Export/Import

On the source environment:

1. Create and set directory details for the export process on the source DB hosts
 - a. Make a Directory on the Source DB Hosts in a location with sufficient space.
`mkdir -p /u01/installers/database`
 - b. Create a Database Directory Object pointing to this location on the source and destination databases.
`SQL> CREATE DIRECTORY orcl_full AS '/u01/installers/database';`
2. Shutdown WebLogic Server Managed Servers or Clusters.
Note: if executing in parallel with the domain backup, coordinate the shutdown of the entire domain including AdminServer and NodeManagers.
3. Stop the SOA DBMS Queues in the source database if your are using Oracle Identity Governance.
 - a. Connect as the SOAINFRA schema user and query for the user queues

```

$ sqlplus <PREFIX>_SOAINFRA@<sourceDB>
SQL> COLUMN name FORMAT A32
SQL> SELECT name,enqueue_enabled,dequeue_enabled
FROM USER_QUEUES where queue_type = 'NORMAL_QUEUE' order by name;

```

NAME	ENQUEUE	DEQUEUE
B2B_BAM_QUEUE	YES	YES
EDN_EVENT_QUEUE	YES	YES
EDN_OA00_QUEUE	YES	YES
IP_IN_QUEUE	YES	YES
IP_OUT_QUEUE	YES	YES
TASK_NOTIFICATION_Q	YES	YES

6 rows selected.

- b. Stop each queue.

```

SQL> BEGIN

DBMS_AQADM.STOP_QUEUE ('B2B_BAM_QUEUE');

DBMS_AQADM.STOP_QUEUE ('EDN_OA00_QUEUE');

DBMS_AQADM.STOP_QUEUE ('EDN_EVENT_QUEUE');

DBMS_AQADM.STOP_QUEUE ('IP_IN_QUEUE');

DBMS_AQADM.STOP_QUEUE ('IP_OUT_QUEUE');

DBMS_AQADM.STOP_QUEUE ('TASK_NOTIFICATION_Q');

END;

/
exit

```

4. Query for and stop any running OIG DBMS_SCHEDULER jobs in the source database as the OIM schema user


```

$ sqlplus <PREFIX>_OIM@<sourceDB>

```

```

SQL> SELECT job_name,session_id,running_instance,elapsed_time
FROM user_scheduler_running_jobs ORDER BY job_name;

```

no rows selected

NOTE: In case of any running jobs, either wait till its completion or stop the job 'gracefully' using:

```

SQL> BEGIN

DBMS_SCHEDULER.stop_job('REBUILD_OPTIMIZE_CAT_TAGS');

END;

/

```

```
SQL> exit
```

- Grant system policies to avoid errors during export datapump jobs

```
$ sqlplus SYS as SYSDBA
```

```
SQL> GRANT EXEMPT ACCESS POLICY TO SYSTEM;
```

```
SQL> exit
```

- Export system and schema dumps from the source database, setting the directory property appropriately.

- Export the system.schema_version_registry table and view

```
$ expdp \"sys/<password>@<sourcedb> as sysdba \" \
```

```
  DIRECTORY=orc1_full \
```

```
  DUMPFILE=idm_system.dmp \
```

```
  LOGFILE=idm_system_exp.log \
```

```
  SCHEMAS=SYSTEM \
```

```
  INCLUDE= VIEW:"IN('SCHEMA_VERSION_REGISTRY')" TABLE:"IN('SCHEMA_VERSION_REGISTRY$')\"
```

```
  JOB_NAME=MigrationExportSys
```

- Export **all** of the schemas used by the datasources in the source WebLogicServer domain

OIG example

```
$ expdp \"sys/<password>@<sourcedb> as sysdba \" \
```

```
  DIRECTORY=orc1_full \
```

```
  DUMPFILE=idm.dmp \
```

```
  LOGFILE=idm_exp.log \
```

```
  SCHEMAS=IGD_OIM,IGD_SOAINFRA,IGD_BIPLATFORM, \
```

```
  IGD_MDS,IGD_ORASDPM,IGD_OPSS,IGDJMS,IGDTLOGS \
```

```
  JOB_NAME=MigrationExport \
```

```
  EXCLUDE=STATISTICS
```

OAM example

```
expdp \"sys/password@IADUPGDB1 as sysdba \" \
```

```
  DIRECTORY=orc1_full \
```

```
  DUMPFILE=idm.dmp \
```

```
  LOGFILE=idm_exp.log \
```

```
  SCHEMAS=IAD_OAM,IAD_MDS,IAD_OPSS,IAD_OMSM,IAD_IAU_VIEWER, \
```

```
  IAD_IAU_APPEND,IAD_IAU \
```

```
  EXCLUDE=STATISTICS
```

To obtain the full list of schemas for your installation execute the following sql script:

```
Select username
```

```
From all_users
```

```
Where username like 'RCU_PREFIX%';
```

- Extract the source database DDL for the tablespaces, schema users, and grants

This step allows the efficient creation of the correct tablespaces on the target database and retains the schema user passwords so no domain reconfiguration is necessary in this regard. System and Object grants for objects outside the exported schemas are also accounted for to reduce the risk of invalid objects and recompilation difficulties.

An example script is provided to create the complete SQL DDL output all at once. The example will need to be modified if not using a CDB/PDB.

- a. In SQLPLUS, execute the example SQL script to extract the DDL to a ddl.sql file in the same directory as the datapump exported dumps. Enter the source environment RCU prefix and the target PDB. output will be copied to both screen and a file named ddl.sql.

```
$ cd /u01/installers/database
$ sqlplus SYS as SYSDBA
SQL> @extract_ddl.sql
Enter RCU Prefix: RCUPREFIX
Enter PDB: targetPDB
```

- b. Delete any object grants for system QT*_BUFFER views in the output ddl.sql. The buffer views will not exist in the target database and cause errors to be thrown.

```
$ sed -i.bak -e '/QT.*_BUFFER/d' /u01/installers/database/ddl.sql
```

Example Script:

Note: Lines in red are only applicable if your target database is a pdb.

This SQL assumes that all of your objects are created using the RCU prefix. If you have created objects without the prefix (for example tablespaces/users for JMS or TLogs then you will need to add these in manually).

```
$ cat << EOF > extract_ddl.sql
set pages 0
set feedback off
set heading off
set long 5000
set longchunksize 5000
set lines 200
set verify off
exec dbms_metadata.set_transform_param (dbms_metadata.session_transform, 'SQLTERMINATOR',
true);
exec dbms_metadata.set_transform_param (dbms_metadata.session_transform, 'PRETTY', true);
accept PREFIX char prompt 'Enter RCU Prefix:'
accept PDBNAME char prompt 'Enter PDB:'

spool ddl.sql

select 'alter session set container=;&&PDBNAME;'
from dual
/
SELECT DBMS_METADATA.GET_DDL('TABLESPACE',Tablespace_name)
from dba_tablespaces
where tablespace_name like '&&PREFIX%'
/
set lines 600
SELECT DBMS_METADATA.GET_DDL('USER',USERNAME)
from DBA_USERS
where USERNAME like '&&PREFIX%'
/
set lines 200
SELECT DBMS_METADATA.GET_GRANTED_DDL ('SYSTEM_GRANT',USERNAME)
from DBA_USERS
```



```

where USERNAME like '&&PREFIX%'
and USERNAME NOT LIKE '%_IAU_APPEND'
and USERNAME NOT LIKE '%_IAU_VIEWER'
/

SELECT DBMS_METADATA.GET_GRANTED_DDL ('OBJECT_GRANT',USERNAME)
from DBA_USERS
where USERNAME like '&&PREFIX%'
and USERNAME NOT LIKE '%TLOGS'
and USERNAME NOT LIKE '%JMS'
/

spool off
EOF

```

8. Re-start the SOA DBMS Queues if you are cloning Oracle Identity Governance. Connect as the SOAINFRA schema user and restart each queue stopped earlier.

```

$ sqlplus PREFIX_SOAINFRA@sourceDB
SQL> BEGIN

        DBMS_AQADM.START_QUEUE ('B2B_BAM_QUEUE');

        DBMS_AQADM.START_QUEUE ('EDN_OA00_QUEUE');

        DBMS_AQADM.START_QUEUE ('EDN_EVENT_QUEUE');

        DBMS_AQADM.START_QUEUE ('IP_IN_QUEUE');

        DBMS_AQADM.START_QUEUE ('IP_OUT_QUEUE');

        DBMS_AQADM.START_QUEUE ('TASK_NOTIFICATION_Q');

END;

/
SQL> COLUMN name FORMAT A32
SQL> SELECT name,enqueue_enabled,dequeue_enabled
FROM USER_QUEUES where queue_type = 'NORMAL_QUEUE' order by name;

NAME                                ENQUEUE DEQUEUE
-----
B2B_BAM_QUEUE                        YES      YES
EDN_EVENT_QUEUE                      YES      YES
EDN_OA00_QUEUE                       YES      YES
IP_IN_QUEUE                          YES      YES
IP_OUT_QUEUE                         YES      YES
TASK_NOTIFICATION_Q                  YES      YES

6 rows selected.
SQL> exit

```

9. Re-start the WebLogic Server Managed Servers or Clusters for OIM, SOA, and BIP

10. Replicate DDL SQL and datapump dump files to the target database host
 - oim.dmp
 - oim_system.dmp
 - ddl.sql

On the target OCI environment:

1. Install/Configure the target database sufficiently in accordance with FMW requirements
Install an Oracle Database on OCI of the version you wish to use, this database can be a Single Instance Database, a real applications cluster (RAC) database. It can be a standard database or a Container Database with OIG in a separate pluggable database (PDB).
2. Validate that the target database is configured to meet all of the criteria of Oracle Access Manager as defined in the Oracle Identity and Access Management Installation Guide.

3. Create TNS entry for the Pluggable Database in OCI if necessary; For example:

```
IGDPDB =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)
      (HOST = iamdbhost.idm.tenancy.oraclevcn.com)
      (PORT = 1521)
    )
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = igdpdb.idm.tenancy.oraclevcn.com)
    )
  )
```

4. Create and set directory details for the export process on the source DB hosts
 - a. Make a Directory on the OCI DB Hosts in a location with sufficient space.
\$ mkdir -p /u01/installers/database
 - b. Create a Database Directory Object pointing to this location on the source and destination databases.
SQL> CREATE DIRECTORY orcl_full AS '/u01/installers/database';
5. Create a database restore point in case of having to roll back the transaction.
6. Create and start a database service for the new database with the same service name as the source environment

For example:

```
$ srvctl add service -db iamcdb_phx1g8 -pdb igdpdb -service onpremservice -rlbgoal
SERVICE_TIME -clbgoal SHORT
$ srvctl start service -db iamcdb_phx1g8 -service onpremservice
$ srvctl status service -db iamcdb_phx1g8 -service onpremservice
```

7. Confirm exported datapump dump files and SQL files are available on the target database host in the correct directory and the dba directory name and path in the database match

```
$ ls -al /u01/installers/database
$ sqlplus / as sysdba
SQL> ALTER SESSION SET CONTAINER = igdpdb;
SQL> CREATE DIRECTORY orcl_full AS '/u01/installers/database';
```

To verify:

```
$ sqlplus / as sysdba
```

```
SQL> ALTER SESSION SET CONTAINER = igdpdb;
```

```
SQL> COLUMN directory_name FORMAT A32
```

```
SQL> COLUMN directory_path FORMAT A64
```

```
SQL> set linesize 128
```

```
SQL> SELECT directory_name,directory_path FROM dba_directories ORDER BY directory_name;
```

8. Confirm the required DBMS_SHARED_POOL and XATRANS database objects exist and create them if they do not. Check for a count of 2 for each of the following SQLs on the target database where the Schema export dump is to be restored.

```
SQL> SELECT COUNT(*) FROM dba_objects  
WHERE owner = 'SYS' AND object_name = 'DBMS_SHARED_POOL'  
AND object_type IN ('PACKAGE','PACKAGE BODY');
```

```
      COUNT(*)  
-----  
           2
```

```
SQL> SELECT COUNT(*) FROM dba_objects  
WHERE owner = 'SYS' AND object_name like '%XATRANS%';
```

```
      COUNT(*)  
-----  
           0
```

- c. If DBMS_SHARED_POOL count is < 2, run the appropriate SQL to re-configure

```
SQL> @/u01/app/oracle/product/19.0.0.0/dbhome_1/rdbms/admin/dbmspool.sql
```

```
SQL> @/u01/app/oracle/product/19.0.0.0/dbhome_1/rdbms/admin/prvtpool.plb
```

- d. If XATRANS count is < 2, run the appropriate SQL to reconfigure

```
SQL> @/u01/app/oracle/product/19.0.0.0/dbhome_1/rdbms/admin/xaview.sql
```

9. Import the source database system dump from the correct folder to create the schema_version_registry table and view, then create the required public synonym manually via SQL.

```
$ cd /u01/installers/database
```

```
$ impdp \"/SYS/<password>@<targetdb> AS SYSDBA\" \  
  PARALLEL=4  
  DIRECTORY=orcl_full \  
  DUMPFILE=idm_system.dmp \  
  LOGFILE=idm_system_imp.log \  
  FULL=YES;
```

```
$ sqlplus / as sysdba
```

```
SQL> alter session set container=igdpdb;
```

```
SQL> CREATE PUBLIC SYNONYM schema_version_registry FOR system.schema_version_registry;
SQL> exit
```

10. Verify the schema_version_registry table data matches your source environment.

It is important to check that the following query returns rows that are consistent with your deployment, this table should have been imported as part of the steps above. If it fails to do so you must populate the table with values from your source system.

```
$ sqlplus / as sysdba
SQL> alter session set container=igdpdb;
SQL> set linesize 100
SQL> col comp_id for a10
SQL> col comp_name for a50
SQL> col version for a10
SQL> select comp_id, comp_name, version, status, upgraded
from system.schema_version_registry;
```

Output will look something like:

COMP_ID	COMP_NAME	VERSION	STATUS	U
IAU	Audit Service	12.2.1.2.0	VALID	N
IAU_APPEND	Audit Service Append	12.2.1.2.0	VALID	N
IAU_VIEWER	Audit Service Viewer	12.2.1.2.0	VALID	N
MDS	Metadata Services	12.2.1.3.0	VALID	N
OAM	Oracle Access Manager	12.2.1.3.0	VALID	N
OPSS	Oracle Platform Security Services	12.2.1.0.0	VALID	N
STB	Service Table	12.2.1.3.0	VALID	N
WLS	WebLogic Services	12.2.1.0.0	VALID	N

11. Execute the DDL SQL from the source database to create the required tablespaces, schema users with the same passwords, system grants, and object grants. If using a PDB, be sure to set your container correctly.

```
$ sqlplus / as sysdba
SQL> alter session set container=igdpdb;
SQL> @'/u01/installers/database/ddl.sql'
SQL> exit
```

12. Import the FMW application schemas dump.

Note: There will be ORA-31684 errors because we pre-created the users. Ignore the following types of errors:

- o Procedure/Package/Function/Trigger compilation warnings
- o DBMS_AQ errors
- o ORA-31684: Object type USER:"" already exists

For example:

```
$ cd /u01/installers/database
$ impdp \"/SYS/<password>@<targetdb> AS SYSDBA\" \
PARALLEL=4 \
DIRECTORY=orcl_full \
DUMPFILE=idm.dmp \
LOGFILE=oim_imp.log
FULL=YES;
```

13. Query for any invalid objects for the imported schemas and execute a recompile for each schema with invalid objects.

For example:

```
$ sqlplus / as sysdba
SQL> alter session set container=igdpdb;
SQL> COLUMN owner          FORMAT A24
SQL> COLUMN object_type    FORMAT A12
SQL> COLUMN object_name    FORMAT A32
SQL> SET LINESIZE 128
SQL> SET PAGESIZE 50
```

```
SQL> SELECT owner,object_type,object_name, status
FROM   dba_objects
WHERE  status = 'INVALID'
AND    owner like '<RCUPREFIX>%
ORDER BY owner, object_type, object_name;
```

OWNER	OBJECT_TYPE	OBJECT_NAME	STATUS
IGDUPG_OIM	SYNONYM	ALTERNATE_ADF_LOOKUPS	INVALID
IGDUPG_OIM	SYNONYM	ALTERNATE_ADF_LOOKUP_TYPES	INVALID
IGDUPG_OIM	SYNONYM	FND_LOOKUPS	INVALID
IGDUPG_OIM	SYNONYM	FND_STANDARD_LOOKUP_TYPES	INVALID

```
SQL> EXECUTE UTL_RECOMP.RECOMP_SERIAL('IGDUPG_OIM');
```

```
SQL> SELECT owner,object_type,object_name, status
FROM   dba_objects
WHERE  status = 'INVALID'
AND    owner like '<RCUPREFIX>%
ORDER BY owner, object_type, object_name;
```

no rows selected

14. Start the SOA DBMS Queues if cloning Oracle Identity Governance.

- e. Connect as the SOAINFRA schema user and query for the user queues

```
$ sqlplus <PREFIX>_SOAINFRA@<sourceDB>
```

```
SQL> COLUMN name FORMAT A32
```

```
SQL> SELECT name,enqueue_enabled,dequeue_enabled FROM USER_QUEUES where queue_type =
'NORMAL_QUEUE' order by name;
```

NAME	ENQUEUE	DEQUEUE
B2B_BAM_QUEUE	YES	YES
EDN_EVENT_QUEUE	YES	YES
EDN_OA00_QUEUE	YES	YES
IP_IN_QUEUE	YES	YES
IP_OUT_QUEUE	YES	YES
TASK_NOTIFICATION_Q	YES	YES

6 rows selected.

- f. Start each queue.

```
SQL> BEGIN

DBMS_AQADM.START_QUEUE ('B2B_BAM_QUEUE');

DBMS_AQADM.START_QUEUE ('EDN_OA00_QUEUE');

DBMS_AQADM.START_QUEUE ('EDN_EVENT_QUEUE');

DBMS_AQADM.START_QUEUE ('IP_IN_QUEUE');

DBMS_AQADM.START_QUEUE ('IP_OUT_QUEUE');

DBMS_AQADM.START_QUEUE ('TASK_NOTIFICATION_Q');

END;

/

exit
```

Cloning the Source Binaries

The Oracle binaries that the source and target systems use must be identical. The easiest way to achieve this is to perform a backup and restore operation using your preferred backup tool. The example below uses tar.

Using your preferred backup tool take a backup of the following locations from OIMHOST1 on the source site:

- oraInventory
- MW_HOME

For Example:

```
tar cvzPpsf oim_binaries.tar.gz \  
  /u01/oracle/oraInventory \  
  /u01/oracle/products/identity

tar cvzPpsf oam_binaries.tar.gz \  
  /u01/oracle/oraInventory \  
  /u01/oracle/products/access

tar cvzPpsf ldap_binaries.tar.gz \  
  /u01/oracle/oraInventory \  
  /u01/oracle/products/dir
```

Cloning the WebLogic Domain

When cloning the source WebLogic Server domain it is recommended to shut down the domain completely for the duration of the backup portion of the process. WebLogic Server and NodeManager processes create numerous lock files at runtime that can interfere with start-up of the cloned environment, and in-flight runtime transactions may be inconsistent if not completely quiesced.

Confirm host file overrides on OCI for source hostnames and FQDN

Validate that the hostnames and SCAN addresses in the cloned domain configuration resolve properly to OCI IP addresses.

1. Verify source host/FQDN enumerated earlier are listed on the OCI IP addresses in the `/etc/hosts` files. See the OCI Hosts Files section above for an example.
2. Ping the source FQDN from an OCI host, verify ping replies with the correct IP address.

Shutdown the Domain Completely

Stop all Managed Servers, AdminServer, and NodeManager processes until the backup process is complete on all hosts.

Take a backup of the Source Domain Configuration

1. Using your preferred backup tool take a backup of the following locations from OIMHOST1 on the source site:
 - ASERVER_HOME
 - MSERVER_HOME
 - Keystores
 - Nodemanager configuration files

Note: If you have a combined DOMAIN_HOME rather than a segregated one as described in the Enterprise Deployment Guide then include DOMAIN_HOME rather than ASERVER_HOME and MSERVER_HOME.

Note: If using tar, be sure to preserve permissions and root paths.

For example, if you have a typical Enterprise Deployment then your backup command may look something like:

For Oracle Identity Governance

```
tar cvzPpsf oimhost1_config.tar.gz \  
  
  /u01/oracle/config/nodemanager/OIMHOST1 \  
  /u01/oracle/config/nodemanager/OIMHOST2 \  
  /u01/oracle/config/nodemanager/IGDADMINVHN \  
  /u01/oracle/config/keystores \  
  /u01/oracle/runtime/domains/IAMGovernanceDomain \  
  /u01/oracle/config/domains/IAMGovernanceDomain \  
  /u02/private/oracle/config/domains/IAMGovernanceDomain
```

For Oracle Access Manager

```
tar cvzPpsf oamhost1_config.tar.gz \  
  
  /u01/oracle/config/nodemanager/OAMHOST1 \  
  /u01/oracle/config/nodemanager/OAMHOST2 \  
  /u01/oracle/config/nodemanager/IADADMINVHN \  
  /u01/oracle/config/keystores \  
  /u01/oracle/config/domains/IAMAccessDomain \  
  /u02/private/oracle/config/domains/IAMAccessDomain
```

For Oracle Internet Directory 12c

```
tar cvzPpsf oamhost1_config.tar.gz \  
  
  /u01/oracle/config/nodemanager/LDAPHOST1 \  
  /u01/oracle/config/nodemanager/LDAPHOST2
```

```
/u01/oracle/config/domains/OIDDomain \  
/u02/private/oracle/config/domains/OIDDomain
```

2. Repeat on any supplementary nodes, for example a command on OIMHOST2 may look something like
`tar cvzPpsf OIMHOST2.tar.gz /u02/private/oracle/config/domains/IAMGovernanceDomain`

Restart the Domain

Start all NodeManager processes, AdminServer, and all managed servers

Replicate the backup files to the Target Environment

Copy the resulting backup files to their appropriate OCI hosts

Restore the backups on OCI instances

Restore the Configuration backup

Extract the binary backups to your OCI nodes using your preferred extraction tool. If you are using shared storage you only need to perform this once per share.

Note: If using tar, be sure to preserve permissions and root paths.

On OIMHOST1

```
tar xvzPpsf oig_binaries.tar.gz
```

On OAMHOST1

```
tar xvzPpsf oam_binaries.tar.gz
```

On LDAPHOST1

```
tar xvzPpsf ldap_binaries.tar.gz
```

Restore the Configuration backup

Extract the backups to your OCI nodes using your preferred extraction tool.

Note: If using tar, be sure to preserve permissions and root paths.

For example:

On OIMHOST1

```
tar xvzPpsf oimhost1_config.tar.gz
```

On OIMHOST2

```
tar xvzPpsf oimhost2_config.tar.gz
```


On OAMHOST1

```
tar xvzPpsf oamhost1_config.tar.gz
```

On OAMHOST2

```
tar xvzPpsf oamhost2_config.tar.gz
```

On LDAPHOST1

```
tar xvzPpsf ldaphost1_config.tar.gz
```

On LDAPHOST2

```
tar xvzPpsf ldaphost2_config.tar.gz
```

Clean Up Any Lock and Log Files Copied From The Source Environment

If you have attempted an online-backup of the domain, then remove any lock files copied from the running domain. Also optionally clean up the old log files from the source environment.

For example:

On OIMHOST1

```
# Lock Files Cleanup:

find /u01/oracle/config/nodemanager -type f -name "*.lck" -exec rm -f {} \;

find /u01/oracle/config/domains/IAMGovernanceDomain \
  -type f \( -name "*.lck" -or -name "*.lok" \) -print -exec rm -f {} \;

find /u02/private/oracle/config/domains/IAMGovernanceDomain \
  -type f \( -name "*.lck" -or -name "*.lok" \) -print -exec rm -f {} \;

# Log File Cleanup:

find /u01/oracle/config/nodemanager/OIMHOST1 \
  -type f \( -name '*.log' -or -name '*.out' \) -print -exec rm -f {} \;

find /u01/oracle/config/nodemanager/OIMHOST2 \
  -type f \( -name '*.log' -or -name '*.out' \) -print -exec rm -f {} \;

find /u01/oracle/config/nodemanager/IGDADMINVHN \
  -type f \( -name '*.log' -or -name '*.out' \) -print -exec rm -f {} \;

find ${ASERVER_HOME}/servers/AdminServer/logs \
  -type f ! -size 0c -print -exec rm -f {} \+

find ${MSERVER_HOME}/servers/*/logs \
  -type f ! -size 0c -print -exec rm -f {} \+
```

On OIMHOST2

```
# Lock Files Cleanup:

find /u02/private/oracle/config/domains/IAMGovernanceDomain \
  -type f \( -name "*.lck" -or -name "*.lok" \) -print -exec rm -f {} \;

# Log File Cleanup:

find ${MSERVER_HOME}/servers/*/logs \
  -type f ! -size 0c -print -exec rm -f {} \+
```

Start the OCI Cloned Domain

Having successfully restored the backup to the OCI instances start the domain on OCI

- Start the Node Manager for the ASERVER_HOME
- Start the Node Manager for the MSERVER_HOME on all nodes
- Start the Administration Server and check logs
- Start the OAM Managed Server/Cluster (OAM)
- Start the Policy Managed Server/Cluster (OAM)
- Start the SOA Managed Server/Cluster and check logs (OIG)
- Start Business Intelligence Platform Managed Server/Cluster and check logs (OIG)
- Start the OIM Managed Server/Cluster and check logs (OIG)

Cloning the Oracle Internet Directory Instance

If you are cloning Oracle Internet Directory 12c then you will have deployed it in a weblogic domain and should follow the instructions above for Cloning a Weblogic Domain.

If you are cloning from Oracle Internet Directory 11g then you will need to clone the instance directories to OCI. For example:

Take a backup of the Source Instance Configuration

Using your preferred backup tool take a backup of the following locations from OIMHOST1 on the source site:

- INSTANCE_HOME

Note: If using tar, be sure to preserve permissions and root paths.

For example, your backup command may look something like:

```
tar cvzPpsf ldaphost1_config.tar.gz \
  /u02/private/oracle/config/instances/oid1
```

Repeat for each LDAPHOST

Replicate the backup files to the Target Environment

Copy the resulting backup files to their appropriate OCI hosts

Restore the backups on OCI instances

Extract the backups to your OCI nodes using your preferred extraction tool.

Note: If using tar, be sure to preserve permissions and root paths.

For example:

On LDAPHOST1

```
tar xvzPpsf ldaphost1_config.tar.gz
```

Start the OID instances

The OID instances can now be started using the command

```
INSTANCE_HOME/bin/opmnctl startall
```

Cloning Oracle Unified Directory

Cloning Oracle Unified directory is the process of adding an extra Oracle Unified directory replica into your existing deployment, however the new replica will reside inside OCI.

For full information refer to the [Oracle Unified Directory Installation Guide](#)

Create an OUD Replica in OCI

The following are the steps required:

1. Set the environment variable JAVA_HOME to JAVA_HOME.
2. Change Directory to DIR_ORACLE_HOME/oud
3. Set the environment variable INSTANCE_NAME to ../../admin/oud2.

For example:

```
export INSTANCE_NAME=../../../../../u02/private/oracle/config/instances/oud2
```

4. Start the Oracle Unified Directory configuration assistant by executing the command:

```
./oud-setup
```

5. Complete the setup screens as described in the [Enterprise Deployment guide](#) with the following exceptions
 - a. On the topology options screen make sure you select This server will be part of a replication topology select this option even if you source environment is not setup for replication.
 - b. On the Topology Options screen select There is already a server in the topology, and enter one of the source hosts and its credentials.
 - c. If this is your first time setting up replication you will be asked to create a Global Administrator ID.
6. When you have created the instance all of your data in the source system will be replicated to your OCI instance.

Grant OUD Changelog Access

Now that the instance is create you need to grant access to the changelog. This is achieved using the following commands these commands are to be executed against the new instance only:

1. Create a password file with your OUD administration password in this example will use the name passwordfile.
2. Remove the existing change log permissions by executing the command:

```
OID_ORACLE_INSTANCE/OU/bin/dsconfig set-access-control-handler-prop \
--remove \
global-aci:"(target=\"ldap:///cn=changelog\")(targetattr=\"*\")(version 3.0; aci \"External changelog access\"; deny (all) userdn=\"ldap:///anyone\");" \
--hostname OUD Host \
--port OUD Admin Port \
--trustAll \
--bindDN cn=oudadmin \
--bindPasswordFile passwordfile \
--no-prompt
```

3. Add a new OCI using the command:

```
OID_ORACLE_INSTANCE/OU/bin/dsconfig set-access-control-handler-prop \
--add \
global-aci:"(target=\"ldap:///cn=changelog\")(targetattr=\"*\")(version 3.0; aci \"External changelog access\"; allow (read,search,compare,add,write,delete,export) groupdn=\"ldap:///cn=OIMAdministrators,cn=groups,dc=example,dc=com\");" \
--hostname OUD Host \
--port OUD Admin Port \
--trustAll \
--bindDN cn=oudadmin \
--bindPasswordFile passwordfile \
--no-prompt
```

Where OimAdministrators is the group you have in LDAP for managing OIM. See the Enterprise Deployment guide for more information.

Create OUD Indexes

Create local OUD indexes on the newly created instance. To do this perform the following commands:

```
OID_ORACLE_INSTANCE/OU/bin/ldapmodify -h LDAPHOST2.example.com -Z -X -p 4444 -a -D "cn=oudadmin" -j passwordfile -c \-f IAD_ORACLE_HOME/idm/oam/server/oim-intg/ldif/ojd/schema/ojd_user_index_generic.ldif
```

```
OID_ORACLE_INSTANCE/OU/bin/ldapmodify -h LDAPHOST2.example.com -Z -X -p 4444 -a -D "cn=oudadmin" -j passwordfile -c \-f IAD_ORACLE_HOME/idm/idmtools/templates/oud/oud_indexes_extn.ldif
```

Once the indexes have been created you need to force and index rebuild using the commands:

1. Shutdown the OUD instance using the command:

```
OID_ORACLE_INSTANCE/OU/bin/stop-ds
```

2. Execute the command:

```
OID_ORACLE_INSTANCE/OID/bin/rebuild-index --rebuildAll -b "dc=example,dc=com"
```

3. Restart the OUD instance using the command:

```
OID_ORACLE_INSTANCE/OID/bin/start-ds
```

Validating Access to the Clone Environment

If you front your Oracle Identity and Access Management installation via Oracle HTTP servers then you must have migrated them to OCI first prior to attempting to validate the clone of this domain.

Your environment will be accessed either directly or via a load balancer, this configuration should not be changed until cutover time. However, you can still validate your configuration by overriding your environment's host names in your local hosts file.

For example in an Oracle Identity Manager installation you will access your application using entry points such as:

- <http://igdadmin.example.com/console>
- <http://igdadmin.example.com/identity>
- <https://login.example.com>

The hostnames in these URLs will be resolved by your corporate DNS to the IP address of the load balancer which routes your requests. To override the default name resolution to the source environment IP addresses, point these host names to either a separate load balancer which is sending traffic to your OCI hosts or the internal OCI Load balancer if you have configured it.

For validation purposes before clone environment launch, use the local hosts file on client systems to override the IP addresses of the on-premise hosts to that of the OCI compute instances as-needed prior to go-live for the environment. This is the same configuration used on the OCI compute instances, just on client workstations for browser use.

1. Update and validate your workstation's /etc/hosts file entries
2. Clear client OS DNS caches
3. Clear browser cache
4. Ping the source environment FQDN for the load-balancer and managed servers (if accessible), and optionally the database address (or SCAN) if needed. Verify the responses are from OCI IP addresses.
 - igdadmin.example.com
 - login.example.com
 - oimhost1.example.com
 - oimhost2.example.com
 - ldaphost1.example.com
 - ldaphost2.example.com
 - src-DB-SCAN.example.com
5. Browse to your OIM URL endpoints using the source-environment's FQDNs.
Note: If webgates and OAM not fully deployed or functional yet, disable the webgates in httpd.conf for duration of this validation.
 - <https://igdadmin.example.com/console>
 - <https://igdadmin.example.com/identity>
6. Verify client traffic is logged in the OCI WEBHOST1/2 OHS access logs.
7. Verify request are logged in the WebLogic Server logs.

As you browse, you should be redirected to your login page and then when you enter your login credentials you should be presented with the Oracle WebLogic Console . If you have gone through this interaction, and see request in the access logs, then you have successfully logged in to your clone.

Conduct other tests as you feel appropriate.

POST CLONE TASKS

Execute the OIM LDAP Consolidated Full Reconciliation Job

If you have used Oracle Internet Directory Replication to clone your Oracle Internet Directory then the Change numbers will be out of sync. To bring the domain back into sync you must rerun your Oracle Identity Governance Full Reconciliation Jobs.

After cloning the domain, a full reconciliation job needs to be executed. See the [Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager](#) for detailed information.

1. Browse to <https://igdadmin.example.com/sysadmin> and authenticate as xelsysadm
2. In the left-pane, under System Configuration, click Scheduler. A popup window will appear
3. In the Identity System Administration popup window, search for the scheduled job: LDAP Consolidated Full Reconciliation

If you are cloning Oracle Identity Governance 12c and have migrated to connector based synchronization then you must run the jobs:

- SSO Connector Integration Group Full Reconciliation
 - SSO Connector Integration User Reconciliation
 - SSO Connector Integration Group Membership Full Reconciliation
 - SSO Connector Integration Group Hierarchy Sync Full Reconciliation
4. Click on the "LDAP Consolidated Full Reconciliation" entry in the search results to view the job details.
 5. Click the "Run Now" button to execute the job and verify the confirmation message: "Job is running"
 6. Periodically click the "Refresh" button and verify job status
 7. When the Job status shows "Stopped", validate the Execution Status for "Success". Check logs and troubleshoot as needed.

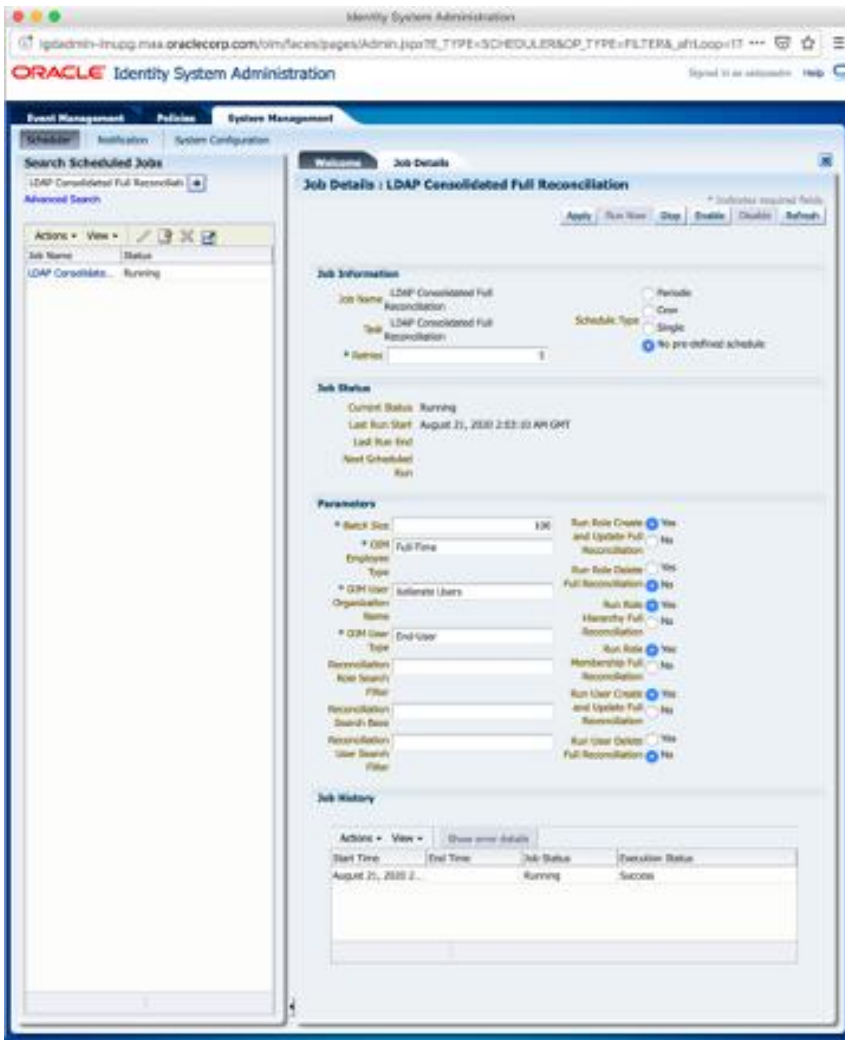


Figure 3 - Identity System Administration - Scheduled Job Details - LDAP Consolidated Full Reconciliation

8. Switch tabs to "Event Management" and execute an empty search for all recent reconciliation events.
9. Spot-check events to assure the current status is either "Creation Succeeded" or "Update Succeeded"

The screenshot displays the Oracle Identity System Administration interface. The main window is titled 'Event Management' and is divided into several sections:

- Reconciliation:** A search bar and a table of reconciliation events. The table has columns for Event ID, Profile Name, and Key Fields. Event ID 30184 is highlighted.
- Event Details: ID 30184:** A detailed view of the selected event, showing its status as 'Creation Succeeded' and other metadata like 'Date and Time' (August 28, 2020, 1:45:43 AM GMT).
- Linked To:** Information about the linked user, 'XLTESTUSER100003 - Test User100003', and the linking rule, 'Rule Based Linking'.
- Notes:** A section for adding or viewing notes related to the event.
- Reconciliation Data:** A sub-section with tabs for 'Matched Users' and 'History'. It contains a table with columns for Attribute Name, Attribute Value, and OIM Mapped Field.

Event ID	Profile Name	Key Fields
30196	LDAPRole	AAA788BF6A5969B7E050D60...
30195	LDAPRole	AAA788BF6A5869B7E050D60...
30194	LDAPRole	AAA788BF6A5769B7E050D60...
30193	LDAPRole	AAA788BF6A5669B7E050D60...
30192	LDAPRole	AAA788BF6A5069B7E050D60...
30191	LDAPRole	AAA788BF6A4E69B7E050D60...
30190	LDAPRole	AAA788BF6A4D69B7E050D60...
30189	LDAPRole	AAA788BF6A4C69B7E050D60...
30188	LDAPUser	ACD82B561B8C5B44E053D31...
30187	LDAPUser	AAA7CDC0255DB411E050D60...
30186	LDAPUser	AAA7CDC0255CB411E050D60...
30185	LDAPUser	AAA7CDC0255BB411E050D60...
30184	LDAPUser	AAA7CDC0255AB411E050D60...
30183	LDAPUser	AAA7CDC02559B411E050D60...
30182	LDAPUser	AAA7CDC02558B411E050D60...
30181	LDAPUser	AAA7CDC02557B411E050D60...
30180	LDAPUser	AAA7CDC02556B411E050D60...
30179	LDAPUser	AAA7CDC02555B411E050D60...
30178	LDAPUser	AAA7CDC02554B411E050D60...
30177	LDAPUser	AAA7CDC02553B411E050D60...
30176	LDAPUser	AAA7CDC02552B411E050D60...
30175	LDAPUser	AAA7CDC02551B411E050D60...
30174	LDAPUser	AAA7CDC02550B411E050D60...
30173	LDAPUser	AAA7CDC0254FB411E050D60...
30172	LDAPUser	AAA7CDC0254EB411E050D60...
30171	LDAPUser	AAA7CDC0254DB411E050D60...
30170	LDAPUser	AAA7CDC0254CB411E050D60...
30169	LDAPUser	AAA7CDC0254BB411E050D60...
30168	LDAPUser	AAA7CDC0254AB411E050D60...
30167	LDAPUser	AAA7CDC02440B411E050D60...
30166	LDAPUser	AAA7CDC0243FB411E050D60...
30165	LDAPUser	AAA7CDC0243EB411E050D60...
30164	LDAPUser	AAA7CDC0243DB411E050D60...
30163	LDAPUser	AAA7CDC0243CB411E050D60...
30162	LDAPUser	AAA7CDC0243BB411E050D60...
30161	LDAPUser	AAA7CDC0243AB411E050D60...
30160	LDAPUser	AAA7CDC02439B411E050D60...
30159	LDAPUser	AAA7CDC02438B411E050D60...
30158	LDAPUser	AAA7CDC02437B411E050D60...
30157	LDAPUser	AAA7CDC02436B411E050D60...
30156	LDAPUser	AAA7CDC02435B411E050D60...
30155	LDAPUser	AAA7CDC02434B411E050D60...

Attribute Name	Attribute Value	OIM Mapped Field
orcidguid	AAA7CDC0255AB4...	LDAP GUID
givenname	Test	First Name
sn	User100003	Last Name
employeetype	EMP	Role
uid	XLTESTUSER100003	User Login
cn	Test User100003	Common Name
dn	cn=Test User1000...	LDAP DN

Migrate OIM Object Cache to Unicast

If are migrating Oracle Identity Manager from an on-premise deployment you may have been using Multicast communications for the OIM Cache. Multicast is is not available in many cloud deployments including OCI. If you are using multicast then you will need to convert to Unicast following the instructions in:

[How To Deploy OIM Cluster With Unicast Configuration For Cachine](#) (Doc ID 2387392.1)

CUTOVER TO OCI

When you are ready to switch-over to your OCI deployment you have to point your existing resources to the new OCI deployment.

Cutover Load Balancers

If you access your Oracle Identity and Access deployment via a Load Balancer then you have two options available. You can either switch to using the load balancer inside OCI which you will have configured to access your new application, or you can reconfigure your existing On-Premise Load Balancer to point to your new OCI OIM Deployment

OCI Load Balancer

If you have configured a new OCI load balancer be sure to load any SSL certificates from your existing On-Premise load balancer to the new OCI load balancer.

Update DNS so that your application fully-qualified host names (igdadmin.example.com, etc...) point to the virtual hosts inside the OCI load balancer.

On-Premise Load Balancer

If you have an On-Premise Load balancer that you wish to continue using for your deployment. Then you need to add the new OAM OCI Hosts to your existing load balancer pool removing the existing entries.

REFERENCES

- [Oracle Cloud Infrastructure Documentation](#)
- [Running Graphical Applications Securely on Oracle Cloud Infrastructure](#)
- [Oracle Fusion Middleware Supported System Configurations](#)
- [Oracle Identity and Access Management Enterprise Deployment Guide \(11.1.2.3.0\)](#)
- [Oracle Identity and Access Management Enterprise Deployment Guide \(12.2.1.4.0\)](#)
- [Upgrading Oracle Identity Governance 12.2.1.3](#)
- [Upgrading Oracle Identity Governance 12.2.1.4](#)

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.

Outside North America, find your local office at oracle.com/contact.

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2021, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0120

Moving Oracle Internet Directory from On-Premises to Oracle Cloud Infrastructure
May, 2021

Author: Michael Rhys, Contributors: Frank Rizzo

