ORACLE

Clone and Upgrade Case Study

Oracle Access Manager

March, 2021 | Version 1.0

PURPOSE STATEMENT

This document provides a description, a summary of requirements, and the setup procedure for upgrading Oracle Access Manager (OAM) from 11.2.1.3 to 12.2.1.4, migrating an on-premises deployment into Oracle Cloud Infrastructure (OCI). This paper is oriented to a technical audience having knowledge of Oracle Identity Management, Oracle WebLogic, Oracle Database administration, and basic operating system knowledge.

This paper discusses a mechanism for moving Oracle Access Manager from Oracle 11g to 12.2.1.4 in with minimum impact to the existing deployment. This document uses an example using Oracle Cloud Infrastructure, but the procedure is applicable to any target system.

DISCLAIMER

REVISION HISTORY

The following revisions have been made to this white paper:

Date	Revision	Comments
March, 2021	1.0	Initial Release

TABLE OF CONTENTS

INTRODUCTION

Many customers are looking at alternative ways of upgrading their Identity systems from one release to another. The traditional method of upgrading an existing system in-place is not suitable for all. The purpose of this paper is to show an alternative approach whereby an existing system is migrated to a higher release on duplicate hardware, by first cloning the original deployment. The advantage of the approach is that the upgrade procedure can be practiced, new hardware can be utilized and the existing system is still available should a fallback be required.

This paper describes a solution for the preparation, installation, and configuration procedures, as well as operational best practices for moving Oracle Access Manager from an on-premises location into Oracle Cloud Infrastructure (OCI). The originating on-premises configuration will have an 11g version and its data copied to an 11g version in OCI prior to being upgraded to 12c. The solution involves Cloning the database and Cloning the installation to 11g prior to performing an in place upgrade.

This approach should be practiced prior to performing for real. It is required that prior to performing this transition that the LDAP directory has already been migrated.

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 provided combines lift and shift to OCI, while performing a software upgrade in a single set of procedures.

This document does not cover Oracle Access Manager Multidata center deployments.

During the cloning process a small outage will be required to take a consistent backup of the domain. The length of the outage will depend on the size of your deployment.

Once the final cloning operation is underway (after you have tested the procedure a number of times), then data will not be kept in sync between the source and target systems. As such a “freeze” should be imposed for the duration of the final migration.

Assumptions

This document covers the following environment configurations and assumes that the majority of administrators planning to move Oracle Access Manager from an on-premises configuration into OCI are using similar configurations.
It is important to note that to simplify this migration host names will be the same in OCI as they are in the source On-Prem location.

Oracle Internet Directory

Oracle Internet Directory must be cloned to OCI via the Migration whitepaper prior to Oracle Access Manager. If you are using Oracle Unified directory instead then this must also be migrated before Oracle Access Manager.

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.
The assumed on-premises version should be 11gR2 Patch Set 3 with the latest Bundled Patch applied.

Oracle Database

As with Oracle Internet Directory, Oracle Database are 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, users may also have their databases deployed on 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 moving an existing Oracle Access Manager Deployment from One set of hardware to another, in this example we are demonstrating the move to Oracle Cloud Infrastructure (OCI). Where appropriate OCI information has been included but this document does not include all of the best practices associated with deploying your application to OCI. For example, it makes no reference to such things 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 Whitepapers on the best practice associated with deploying applications in OCI.

Environment Variables

Administrators of Oracle Access Manager should be familiar with various environment variables that need to be configured on each host (for on-premises) or instance (for OCI). 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. Note these examples are based on the Enterprise Deployment Guide (EDG)

ORACLE_HOME: The location of the base of the 11g Oracle Access Manager installation.
For example:
/u01/oracle/products/access

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/IAMAccessDomain

MSERVER_HOME: The location of the Weblogic domain configuration where managed servers are started from
For example:
/u02/private/oracle/config/domains/IAMAccessDomain

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/IAMAccessDomain

CLONING STRATEGY

The following is an overview of the tasks required to Clone Oracle Access Manager into OCI from an on-premises implementation, and then perform a subsequent upgrade.

Reference Architecture

Figure 1: High-Level Oracle Access Manger example architecture. Scaling may differ from a user's implementation.

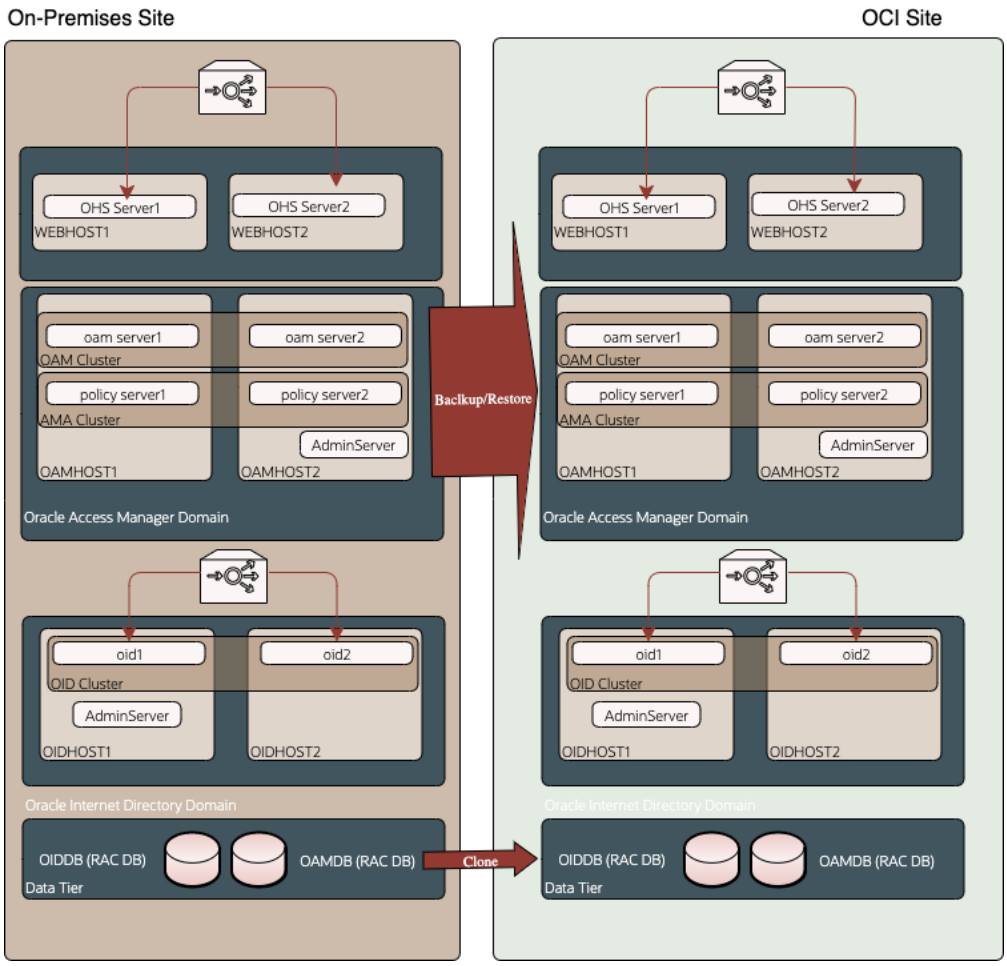


Figure 1: High-Level Oracle Access Manager migration Topology

Solution Process

The following are the detailed steps required to configure the lift and shift of Oracle Access Manager in OCI.

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 Access Manger 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 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 on-premises 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 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 be similar to that of the hosts in the on-premises environment.

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 Allow GUI-Based Installers and Configuration Tools

By default, OCI compute instances do not have X11 forwarding configured. X11 forwarding is required for users to use GUI-based installation and configuration tools. To enable X11, perform the following steps. Refer to the Running Graphical Applications Securely on Oracle Cloud Infrastructure white paper for more information.:

1. Log in to the instance
2. Configure SSHD to not use localhost for X11:
3. Open `/etc/ssh/sshd_config` in your favorite editor
4. Search for the line that has `X11UseLocalhost yes` (it's commented out)
5. Remove the comment from the beginning of the line
6. Change the yes to no
7. Save the file
8. Restart SSHD: `sudo systemctl restart sshd`
9. Install libXrender: `sudo yum install libXrender`
10. Install libXtst: `sudo yum install libXtst`
11. Install xauth: `sudo yum -y install xauth`
12. Install xterm (used to verify X configuration): `sudo yum -y install xterm`
13. Add the following host environment variable:
    `export _JAVA_OPTIONS="-Dsun.java2d.xrender=FALSE"`
14. Log out of the instance

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

```
* soft  nofile  4096
* hard  nofile  65536
* 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. 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
```

Default ports for Oracle Internet Access Manager are: 5556, 7001, 14100 and 14150

2. Restart the firewall service after all ports are configured by executing:
   ```
   sudo systemctl restart firewalld
   ```
3. Validate the firewall configuration by executing the following:
   ```
   sudo firewall-cmd --list-ports
   ```

Users 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. To this end it is recommended that the same Account Owners and groups are created in your OCI instance. To create a user called Oracle and a group called oinstall then following procedure can be used:

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

Creating the Load Balancer

In a high availability configuration Oracle Access Manager will reside behind an Oracle HTTP server which will be used to route requests to the Oracle Access Manager 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 Access Manager at cut-over.

For details of using a load balancer with Oracle Access Manager refer to the Oracle Enterprise Deployment Guide.

Creating a Virtual IP Address

If your on-premise installation uses a virtual IP addresses for your weblogic administration server as described in the Oracle Enterprise Deployment Guide then you will need to create a similar virtual IP address in OCI.

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 for example OAMHOST1.
2. Click Assign Private IP address
   Set the host name to IADADMINVHN or whatever name you are using everything else can be left as the default. Click assign,
   you will now see you new IP address assigned.
3. Inside the compute instance assign the IP address to your active VNIC (check using ipaddr) for example if your main VNIC is ens3 then you can use the following command to assign it to the network

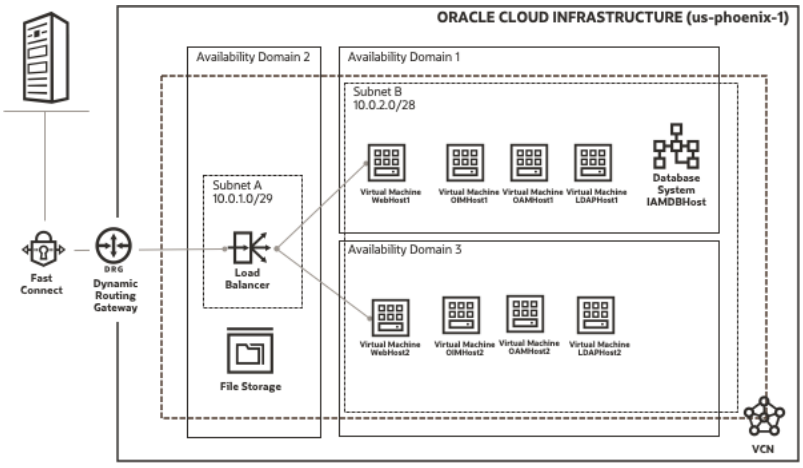
   ```
   sudo ip addr add 100.105.19.213 dev ens3 label ens3:0
   ```

   check using the command ip addr
4. You then need to create an entry in the /etc/hosts file for each of your compute instances.

Note: If you wish to directly access the Weblogic Administration server outside of OCI, that is to say that you are not accessing your WebLogic Administration Server via an OHS then the virtual IP address must be a public facing IP Address.

Summary of OCI Objects

Below is a summary of the OCI objects which were used in the validation of this paper



OCI Hosts Files

It is imperative that in a clone situation that the host names in OCI are the same as the host names in your on-premise system. If you have followed the recommendations in the Enterprise Deployment Guide and used virtual host names then this is simply a matter of aliasing these entries to the real OCI host names for example:

100.x.19.x oamhost1.iamu.tenancey.oraclevcn.com oamhost1

If you are using physical host names in your on-premise WebLogic configuration then you you must alias these names to the real OCI host names, for example

100.x.19.x oamhost1.iamu.tenancey.oraclevcn.com oamhost1 host02vm0024.example.com host02vm0024

In addition if you are using a virtual IP address then this should also be aliased to your virtual hostname for example

100.x.19.x IADADMINVHN

Ensure that entries for each of the OCI instances is present in all the host files in the topology, this includes any database host names/scan addresses.

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 Database to OCI

The strategy is based on cloning the database objects from the source on-premise system to the destination OCI system. 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
- Is a complete copy redoing the exercise requires data to be deleted from the target each time.
- No on-going synchronization
- During Cut-over the source system will need to be frozen for updates

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 synchronisation. 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 whitepaper we will describe using export/import.

Cloning the database using Export/Import

On your on-premise system export the data from your database to an export file. To do this:

1. 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 OAM in a separate pluggable databse (PDB).
2. Make a Directory on the Source and the Destination OCI Hosts

```
mkdir -p /u01/installers/database
```

3. Create a Database Directory Object pointing to this location on the source and destination databases.

```
SQL> CREATE DIRECTORY orcl_full AS '/u01/installers/database';
```

4. Export Source Database

```
export ORACLE_BASE=/u01/app/oracle
export ORACLE_HOME=${ORACLE_BASE}/product/12.2.0.1/dbhome_1
export GRID_HOME=/u01/app/12.2.0.1/grid
export PATH=$PATH:$ORACLE_HOME/bin
export DB_NAME=iadupgdb
export ORACLE_SID=iadupgdb1
```

Export the system.schema_version_registry table and view

```
$ expdp \"sys/<password>@<sourcedb> as sysdba \" \
     DIRECTORY=orcl_full \
     DUMPFILE=oam_system.dmp \
     LOGFILE=oam_system_exp.log \
     SCHEMAS=SYSTEM \
     INCLUDE= VIEW:"IN('SCHEMA_VERSION_REGISTRY')"
TABLE:"IN('SCHEMA_VERSION_REGISTRY$')" \
     JOB_NAME=MigrationExportSys

expdp \"sys/password@IADUPGDB1 as sysdba \" \
     DIRECTORY=orcl_full \
     DUMPFILE=full_oam.dmp \
     LOGFILE=full_oam_exp.log \
     SCHEMAS=iadupg_oam,IADUPG_MDS,IADUPG_OPSS,IADUPG_OMSM,IADUPG_IAU_VIEWER,\
     IADUPG_IAU_APPEND,IADUPG_IAU\
EXCLUDE=STATISTICS
```

NOTE: If you are using a RAC database make sure you have a tns connection which is forced to a specific instance/PDB unless you want to create the directories on each node.

IADUPG is an example RCU Prefix

5. Copy the generated file to the destination database host
6. Extract DDL from the source database. The import will only import the data you have extracted from the source database it will not create any tablespaces or users, not having those present will cause the import to fail. This can be resolved by extracting the DDL for these objects from the database to do this:

a. Create a file called extract_ddl.sql using your favourite editor with the following content:

```
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

Notes:
Lines in red above 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).
```

b. In SQLPLUS execute the file:

```
SQL> @extract_ddl
```

This will generate a file called ddl.sql

7. Copy the generated file to the destination database host
8. Create TNS entry for the Pluggable Database in OCI if necessary, for example

```
IADPDB =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)
                 (HOST = iamdbhost.iamu.susengdev2phx.oraclevcn.com)
                 (PORT = 1521)
      )
      (CONNECT_DATA =
          (SERVER = DEDICATED)
          (SERVICE_NAME = iadpdb.iamu.susengdev2phx.oraclevcn.com)
      )
     )
```

9. Validate that the target database meets all of the criteria of Oracle Access Manager as defined in the Oracle Identity Management Installation Guide.
10. Create a database restore point in case of having to roll back the transaction.
11. Create the Tablespaces/Users etc for Oracle Access Manager. To do this execute the script you generated above ddl.sql. In SQLPLUS execute the file:

```
SQL> @ddl
```

Carefully review the output and correct any errors that may be encountered.

12. Import the data into the destination database, this database need not be at the same database version as the source.

```
export ORACLE_BASE=/u01/app/oracle
export ORACLE_HOME=${ORACLE_BASE}/product/12.2.0.1/dbhome_1
export GRID_HOME=/u01/app/12.2.0.1/grid
export PATH=$PATH:$ORACLE_HOME/bin:$ORACLE_HOME/OPatch
export DB_NAME=iamcdb_phx1g8
export ORACLE_SID=iamcdb

impdp \"SYS/Password@IADPDB AS SYSDBA\" DIRECTORY=orcl_full DUMPFILE=oam_system.dmp
LOGFILE=oam_system_imp.log FULL=YES;
impdp \"SYS/Password@IADPDB AS SYSDBA\" DIRECTORY=orcl_full DUMPFILE=full_oam.dmp
LOGFILE=full_oam_imp.log FULL=YES;
```

13. Create a database service in OCI with the same name as the primary.

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

After you have imported the schemas 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.

```
set linesize 100
col comp_id for a10
col comp_name for a50
col version for a10
```

```
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                                      11.1.1.9.0 VALID           N
MDS        Metadata Services                                  11.1.1.9.0 VALID           N
OAM        Oracle Access Manager                              11.1.2.3.0 VALID           N
OID        Oracle Internet Directory                          11.1.1.9.0 VALID           N
OMSM       Oracle Mobile Security Manager                     11.1.2.3.0 VALID           N
OPSS       Oracle Platform Security Services                  11.1.1.9.0 VALID           N
```

Cloning the Source Binaries/Configuration

Take a backup of the On-Premise installation

1. Using your preferred backup tool take a backup the following locations on the source site:

   - oraInventory
   - MW_HOME
   - 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.

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

   ```
   tar cfvzP oamhost1.tar.gz /u01/oracle/oraInventory /u01/oracle/products/access
   /u01/oracle/config/domains/IAMAccessDomain /u01/oracle/config/nodemanager/OAMHOST1
   /u01/oracle/config/nodemanager/OAMHOST2 /u01/oracle/config/nodemanager/IADADMINVHN
   /u01/oracle/config/keystores /u02/private/oracle/config/domains/IAMAccessDomain
   ```

   You may encounter issues with lock files if you do not shut the domain down before taking a backup.

2. Repeat on any supplementary nodes, for example a command on OAMHOST2 may look something like

   ```
   tar cfvzP oamhost2.tar.gz /u02/private/oracle/config/domains/IAMAccessDomain
   ```

3. Copy the resulting backup files to their appropriate OCI hosts

Restore the backup on OCI instances

Using your preferred extraction tool extract the backups to your OCI nodes for example:

On OAMHOST1

```
tar xvfzP oamhost1.tar.gz
```

On OAMHOST2

```
tar xvfzP oamhost12tar.gz
```

Start the OAM Domain

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

- Start the Node Manager for the ASERVER_HOME
- Start the Node Manager for the MSERVER_HOME
- Start the Administration Server
- Start the OAM Managed Servers
- Start the Policy Manager Managed Servers

Note if you do not have separate domain directories for the administration server/managed servers as recommended by the Enterprise Deployment Guide then you will only have a single node manager to start per host.

Validating the Clone

If you front your Oracle Access Manager installation via Oracle HTTP servers then you must have migrated them to OCI first. If you have moved your Oracle HTTP Server to 12c then you will not be able to validate the clone until you have upgraded it to 12c.

Your system 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 application names in your local hosts file.

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

http://iadadmin.example.com/console
https://login.example.com

iadadmin.example.com and login.example.com will be resolved in your corporate DNS to 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 address of the on-premise hosts to that of the OCI hosts as-needed prior to go-live for the environment.

Change the IP addresses in your local hosts file.

1. Update and validate /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 server (if accessible), optionally the database address (or SCAN). Verify responses are from OCI IP addresses.
    a. iadadmin.example.com
    b. login.example.com
    c. oamhost1.example.com
    d. oamhost2.example.com
    e. ldaphost2.example.com
    f. ldaphost2.example.com
    g. src-DB-SCAN.example.com

5. Validate that you can access the OAM Administration Server by accessing

http://iadadmin.example.com/console

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, then you have successfully logged in to your cloneVerify client traffic is logged in the OCI WEBHOST1/2 OHS access logs.

Conduct other tests as you feel appropriate.

UPGRADE ORACLE ACCESS MANAGER TO 12C

Upgrade Oracle Access Manager 11g to 12.2.1.3

The Oracle Fusion Middleware Infrastructure and Oracle Identity Management for 12c binaries are required to be installed in the OCI compute nodes. The following are the steps to perform the installations. All software should be acquired from Oracle's eDelivery web site and the user must have acquired the proper licensing for its use. The required software packages are:

- Oracle JDK 1.8.0_211 or higher
- Oracle Fusion Middleware 12c (12.2.1.3.0) Infrastructure
- Oracle Fusion Middleware 12c (12.2.1.3.0) Identity Access Manager

Install Oracle 12.2.1.3 Binaries

The Oracle 12.2.1.3 binaries will be installed alongside the existing binaries in a different directory structure. If you are using redundant binaries as described in the Enterprise Deployment Guide then install the binaries into each redundant location

Installing the JDK

Perform the following steps on all Oracle Access Manager compute instances.

1. Unzip the contents of contents of the acquired package into a temporary location.
2. Create the base location where the JDK will be installed:
   For example:
   ```
   mkdir -p /u01/oracle/products/12c
   ```
3. Copy the `*.tar.gz` file from the temporary location into the base location:
   For example:
   ```
   cp jdk-8u261-linux-x64.tar.gz /u01/oracle/products/12c
   ```
4. Decompress the archive:
   For example:
   ```
   tar zxvf jdk-8u261-linux-x64.tar.gz
   ```
5. Remove the archive file and rename the decompressed directory
   For example:
   ```
   rm jdk-8u261-linux-x64.tar.gz
   mv jdk1.8.0_261 jdk
   ```
6. Set the `JAVA_HOME` and `PATH` variables:
   For example:
   ```
   export JAVA_HOME=/u01/oracle/products/12c/jdk
   export PATH=$JAVA_HOME/bin:$JAVA_HOME/jre/bin:$PATH
   ```

Installing Fusion Middleware Infrastructure

Perform the following steps on all Oracle Access Manager compute instances. To start the installation program, perform the following steps:

1. Go to the directory where you downloaded the installation program.
2. Launch the installation program by invoking the java executable from the JDK directory on your system, as shown in the example below:

```
JAVA_HOME/bin/java -d64 -jar distribution_file_name.jar
```

4. In this example:
    - Replace `JAVA_HOME` with the environment variable or actual JDK location on your system
    - Replace `distribution_file_name` with the actual name of the distribution JAR file
5. If you download the distribution from the Oracle Technology Network (OTN), then the JAR file is typically packaged inside a downloadable ZIP file.
6. To install the software required for the initial Infrastructure domain, the distribution you want to install is:

    ```
    fmw_12.2.1.3.0_infrastructure.jar
    ```

7. When the installation program appears, you are ready to begin the installation. Follow the onscreen prompts to install the Oracle Infrastructure into the Oracle Home:

    /u01/oracle/products/12c/access

For further information refer to : Installing and Configuring the Oracle Fusion Middleware Infrastructure 12.2.1.3

Installing Oracle Identity and Access Management

Perform the following steps on all Oracle Access Manager compute instances. To start the installation program, perform the following steps:

1. Go to the directory where you downloaded the installation program.
2. Launch the installation program by invoking the java executable from the JDK directory on your system, as shown in the example below:

    ```
    JAVA_HOME/bin/java -d64 -jar distribution_file_name.jar
    ```

3. In this example:
    - Replace `JAVA_HOME` with the environment variable or actual JDK location on your system
    - Replace `distribution_file_name` with the actual name of the distribution JAR file
4. If you download the distribution from the Oracle Technology Network (OTN), then the JAR file is typically packaged inside a downloadable ZIP file.
5. To install the software required for the initial Infrastructure domain, the distribution you want to install is:

    ```
    fmw_12.2.1.3.0_idm.jar
    ```

6. When the installation program appears, you are ready to begin the installation. Follow the onscreen prompts to install the Oracle Infrastructure into the Oracle Home:

    /u01/oracle/products/12c/access

7. When prompted choose: Collocated Oracle Identity and Access Manager (Managed through WebLogic Server)

For further information refer to : Installing and Configuring Oracle Identity and Access Management 12.2.1.3

Upgrade Oracle Access Manager Schemas

The first step in the upgrade process is to upgrade the Oracle Access Manager schemas. To do this perform the following steps:

Pre Upgrade Steps

Before performing the upgrade you need to create a backup of the existing system in case you need to rollback the change. The Environment needs to be shutdown prior to upgrading the schemas.

- Shutdown the entire Access Domain including the Administration Server, All WebLogic Managed Servers and node managers.
- Create a database restore point. The fastest way to rollback database changes is to create a restore point, then you can flash the database back to this point if you need to rollback. If you wish to use this method you must have flashback database enabled. If you do not use this method it is recommended taking a backup of the database using your preferred method.

```
SQL> create restore point pre_upgrade;
```

Create a user in the database to perform the upgrade.

```
create user FMW identified by <password>;
grant dba to FMW;
grant execute on DBMS_LOB to FMW with grant option;
grant execute on DBMS_OUTPUT to FMW with grant option;
grant execute on DBMS_STATS to FMW with grant option;
grant execute on sys.dbms_aqadm to FMW with grant option;
grant execute on sys.dbms_aqin to FMW with grant option;
grant execute on sys.dbms_aqjms to FMW with grant option;
grant execute on sys.dbms_aq to FMW with grant option;
grant execute on utl_file to FMW with grant option;
grant execute on dbms_lock to FMW with grant option;
grant select on sys.V_$INSTANCE to FMW with grant option;
grant select on sys.GV_$INSTANCE to FMW with grant option;
grant select on sys.V_$SESSION to FMW with grant option;
grant select on sys.GV_$SESSION to FMW with grant option;
grant select on dba_scheduler_jobs to FMW with grant option;
grant select on dba_scheduler_job_run_details to FMW with grant option;
grant select on dba_scheduler_running_jobs to FMW with grant option;
grant select on dba_aq_agents to FMW with grant option;
grant execute on sys.DBMS_SHARED_POOL to FMW with grant option;
grant select on dba_2pc_pending to FMW with grant option;
grant select on dba_pending_transactions to FMW with grant option;
grant execute on DBMS_FLASHBACK to FMW with grant option;
grant execute on dbms_crypto to FMW with grant option;
grant execute on DBMS_REPUTIL to FMW with grant option;
grant execute on dbms_job to FMW with grant option;
grant select on pending_trans$ to FMW with grant option;
grant select on dba_scheduler_job_classes to fmw with grant option;
grant select on SYS.DBA_DATA_FILES to FMW with grant option;
grant select on SYS.V_$ASM_DISKGROUP to FMW with grant option;
grant select on v$xatrans$ to FMW with grant option;
grant execute on sys.dbms_system to FMW with grant option;
grant execute on DBMS_SCHEDULER to FMW with grant option;
grant select on dba_data_files to FMW with grant option;
grant execute on UTL_RAW to FMW with grant option;
grant execute on DBMS_XMLDOM to FMW with grant option;
grant execute on DBMS_APPLICATION_INFO to FMW with grant option;
grant execute on DBMS_UTILITY to FMW with grant option;
grant execute on DBMS_SESSION to FMW with grant option;
grant execute on DBMS_METADATA to FMW with grant option;
grant execute on DBMS_XMLGEN to FMW with grant option;
```

```
grant execute on DBMS_DATAPUMP to FMW with grant option;
grant execute on DBMS_MVIEW to FMW with grant option;
grant select on ALL_ENCRYPTED_COLUMNS to FMW with grant option;
grant select on dba_queue_subscribers to FMW with grant option;
grant execute on SYS.DBMS_ASSERT to FMW with grant option;
grant select on dba_subscr_registrations to FMW with grant option;
grant manage scheduler to FMW;
```

Start the Upgrade Assistant on OAMHOST1

```
cd /u01/oracle/products/12c/access/oracle_common/upgrade/bin
./ua
```

Upgrade IAU Schema.

1. Click Next on the Welcome Screen
2. Select Individually Selected Schemas on the Upgrade Type screen – Click Next
3. Select Oracle Audit Services and click Next
4. When Prompted enter the directory where your Admin Server is running for example : /u01/oracle/config/domains/IAMAccessDomain Click Next
5. Acknowledge the Pre-requisite checks and Click Next
6. On the IAU Schema Page enter the database connection details.
7. Connect as your upgrade user.
8. Select the IAU user for the access Schema from the drop-down list.
9. Click Next

   If you see the error UPGAST-00224. The specified database does not contain any schemas for Oracle Audit Services or the database user lacks the privilege to view the schemas. Check that the database schema system.schema_version_registry if not then export/import the data for the table once again from the source system.

10. On the Examine Page Click Next
11. On the Upgrade Summary Page Click Upgrade
12. Click Next to finish.

Upgrade Remaining Access Schemas

1. Restart the Upgrade Assistant
2. Click Next on the Welcome Screen
3. Select All Schemas used by a domain on the Upgrade Type screen – Click Next

   If your 11g domain contains Oracle Identity Navigator, choose Individually Selected Schemas and select only the Oracle Access Manager(OAM) and the OAM-related schemas.

4. When Prompted enter the directory where your Admin Server is running for example : /u01/oracle/config/domains/IAMAccessDomain Click Next
5. Verify that Oracle Access Manager schemas are selected on the Component List page
6. Acknowledge the Pre-requisite checks and Click Next
7. On the OPSS Schema Page enter the database connection details.
8. Connect as your upgrade user.
9. Select the IAU user for the access Schema from the drop-down list.
10. Click Next

    If you see the error UPGAST-00224. The specified database does not contain any schemas for Oracle Audit Services or the database user lacks the privilege to view the schemas. Check that the database schema system.schema_version_registry if not then export/import the data for the table once again from the source system.

11. Verify the database connection on the OAM Schema Page and Click Next
12. Verify the database connection on the MDS Schema Page and Click Next
13. On the create schemas page, either enter individual passwords for each of the schemas to be created or select User the same password for all schemas.
14. On the Examine Page Ensure that all checks show Ready for Upgrade - Click Next
15. On the Create Schemas Progress page click Next
16. On the Upgrade Summary Page Click Upgrade
17. Click Next to finish

Reconfigure the WebLogic Access Domain

Take a backup

Take a backup of the domain using your favourite backup tool. In case you need to restore it:

```
tar cvfz access_backup.tar /u01/oracle/config/domains/IAMAccessDomain
```

Running the Reconfiguration Wizard

Start the reconfiguration wizard

1. Navigate to the 12c oracle_common directory for example:
   ```
   cd /u01/oracle/products/12c/access/oracle_common/common/bin
   ```
2. Start the reconfiguration utility using the command:
   ```
   ./reconfig.sh -log=log_file -log_priority=ALL
   ```
3. Navigate through the screens:
4. On the Select Domain Screen enter the location of the domain for example:
   ```
   /u01/oracle/config/domains/IAMAccessDomain
   ```
5. Click Next
6. On the Setup Progress screen click Next
7. On the Reconfig summary screen click Next
8. On the Domain Node and jdk screen select the location of your JDK, click Next
9. On the Grid Link Data source screen if shown Click Next
10. On the JDBC DS Test Screen Click next
11. On the database configuration Type screen enter the connection details for your database.
    - For the schema owner user the user you created above it will have the same prefix as your other users for example IAD_STB
    - Click Get RCU Connection when complete Click Next
    - On the Components Data Source Screen
    - If you are not using a RAC database, then complete the host/port/service details for those accounts missing them
    - If you are using a RAC database select the users with host/port details missing and Select Convert to Grid Link and Click Next
12. On the Grid Link screen supply the Service Name, Schema Password, ONS Host and Port, SCAN and SCAN Hostname and port. Also change the prefix for each Schema Owner to reflect your environment. Click Next
13. On the JDBC Test Screen ensure all tests pass then Click Next, if any fail go back and correct the values on the previous screen until all tests succeed.
14. *If a test fails because you see the error table or view does not exist for the table system.schema_version_registry then issue the following statement in the database*
    ```
    SQL> grant all on system.schema_version_registry to USER;
    ```
15. Where the user is the name of the failing user.
16. On the Node Manager screen select:
    - Type: Per Domain Default Location
    - Choose create a new Node Manager Configuration if this is an EDG deployment. Otherwise choose whatever is appropriate to you.

- Specify the Node manager credentials you wish to use.

17. On the Advanced Configuration screen select: Administration Server, Topology, Domain Front End Capture. Click Next
18. On the Administration Server Page, ensure the details are correct and click Next.
19. On the Managed Servers Page
    - Assign OAM-MGD-SVRS to each of the OAM Managed servers for example WLS_OAM1 and WLS_OAM2
    - Assign OAM-POLICY-MANAGED-SERVER to each of the Policy Managed Servers for example WLS_AMA1 and WLS_AMA2.
    - Remove any MSM Servers.
    - Click Next when finished.
20. On the clusters Page remove the MSM cluster if you have one and verify the information is correct and click Next. *Do NOT assign anything to Dynamic Server Groups, this is not supported here.*
21. On the Server Templates Page click Next.
22. On the Dynamic Servers Page click Next.
23. On the Assign Servers to Clusters Page click Next.
24. On the Coherence Clusters Page click Next,
25. On the machines page click Next.
26. On the assign Servers to Machines Page click Next.
27. On the Virtual Targets Page Click Next.
28. On the Partitions Page Click Next.
29. On the Domain Front End Page, validate that the details are correct and click Next.
30. On the Configuration Summary Page verify the details and click Reconfig.

Upgrade Domain Component Configurations

Now that the domain is reconfigured the Upgrade Assistant must be run once again to update the component versions in the domain.

Start the Upgrade Assistant on OAMHOST1

```
cd /u01/oracle/products/12c/access/oracle_common/upgrade/bin
./ua
```

1. On the Welcome Screen Click Next
2. On the Upgrade Type Page Select All Configurations Used by a Domain
   Enter the Domain Directory, for example:

   /u01/oracle/config/domains/IAMAccessDomain

   Click Next

3. On the Component List screen, verify that the list includes all the components for which you want to upgrade configurations and click Next.
4. On the Prerequisites screen, verify each of the prerequisites and click Next
5. On the Examine screen ensure no errors are reported. Some components may show an upgraded is not needed. Click Next when satisfied.
6. On the Upgrade Summary Screen click Upgrade.
7. After the upgrade completes verify the upgrade has been successful and Click Next

Creating a Separate Domain Directory for Managed Servers

If you deployment is based on the Oracle Enterprise Deployment Guide (EDG) then you will have a separate directory for the WebLogic managed servers on OAMHOST1. After you have performed the upgrade you will need to recreate this directory. To do this perform the following steps:

1. Pack up the domain on OAMHOST1 using the commands:

```
cd /u01/oracle/products/12c/access/oracle_common/common/bin
mkdir -p /u01/oracle/config/backup

./pack.sh -managed=true \
          -domain=/u01/oracle/config/domains/IAMAccessDomain \
          -template=/u01/oracle/config/backup/IAMAccessDomain.jar \
          -template_name=IAMAccessDomain \
          -log_priority=DEBUG \
          -log=/u01/oracle/config/backup/pack_iad.log
Change the Paths/Filenames to reflect your environment
```

2. Unpack the domain on OAMHOST1 using the commands:

```
cd /u01/oracle/products/12c/access/oracle_common/common/bin

./unpack.sh -domain=/u02/private/oracle/config/domains/IAMAccessDomain \
            -overwrite_domain=true \
            -template=/u01/oracle/config/backup/IAMAccessDomain.jar \
           -log_priority=DEBUG \
            -log=/u01/oracle/config/backup/unpack_iad.log \
            -app_dir=/u02/private/oracle/config/domains/IAMAccessDomain/applications

Change the Paths/Filenames to reflect your environment
```

Propogating the Domain to Secondary Hosts

If you have a highly available deployment where Oracle Access Manager runs on multiple hosts then you need to copy the domain to the remaining hosts in the topology for example OAMHOST2. To do this perform the following steps:

1. Pack up the domain on OAMHOST1 using the commands:
   Note: If you have already done this in the previous section then this step can be omitted.

```
cd /u01/oracle/products/12c/access/oracle_common/common/bin
mkdir -p /u01/oracle/config/backup

./pack.sh -managed=true \
          -domain=/u01/oracle/config/domains/IAMAccessDomain \
          -template=/u01/oracle/config/backup/IAMAccessDomain.jar \
          -template_name=IAMAccessDomain \
          -log_priority=DEBUG \
          -log=/u01/oracle/config/backup/pack_iad.log
Change the Paths/Filenames to reflect your environment
```

2. Copy the generated archive (=/u01/oracle/config/backup/IAMAccessDomain.jar) to OAMHOST2.
3. Unpack the domain on OAMHOST2 using the commands:

```
cd /u01/oracle/products/12c/access/oracle_common/common/bin

./unpack.sh -domain=/u02/private/oracle/config/domains/IAMAccessDomain \
            -overwrite_domain=true \
            -template=/u01/oracle/config/backup/IAMAccessDomain.jar \
           -log_priority=DEBUG \
            -log=/u01/oracle/config/backup/unpack_iad.log \
            -app_dir=/u02/private/oracle/config/domains/IAMAccessDomain/applications

Change the Paths/Filenames to reflect your environment
```

Delete MSM Directories

You may find after reconfiguring the domain that you see directories for the obsolete Mobile Security Managed Servers in the domain, whilst you have removed the servers from the configuration it is good practice to remove any remnants of these from the file system as well. This needs to be performed manually for example:

rm -rf /u01/oracle/config/domains/IAMAccessDomain/servers/WLS_MSM*
rm -rf /u02/private/oracle/config/domains/IAMAccessDomain/servers/WLS_MSM* - *If you are using and EDG topology*

Starting Up the Domain

Start Node Manager

In EDG Environments, after you create the Managed Server domain directory, there are two domain home directories and two corresponding Node Manager instances on OAMHOST1. You use one Node Manager to control the Administration Server, running from Administration Server domain home, and you use the other Node Manager to control the Managed Servers, running from the Managed Server domain home.

You must start the two Node Managers independently.

If you have not separated out the Administration Server from the Managed Servers then just start the Node Manager in the Admin Server Domain Directory.

Starting the Node Manager in the Admin Server Domain Directory on OAMHOST1

1. Change to the following directory:

```
cd /u01/ oracle/config/domains/IAMAccessDomain/bin
```

2. Use the following command to start the Node Manager:

```
nohup ./startNodeManager.sh > /u01/oracle/config/domains/IAMAccessDomain
/nodemanager/nodemanager.out 2>&1 &
```

Starting the Node Manager in the Managed Server Domain Directory on OAMHOST1

Note: The Node Manager for the Managed Server's IAD_MSERVER_HOME will be reset every time the domain configuration is unpacked.

The ListenAddress will be changed to the *ADMINVHN* instead of the correct hostname. This needs to be changed to the correct value before starting the Node Manager service after an unpack is performed.

Follow these steps to update and start the Node Manager from the Managed Server home:

1. Verify that the listen address in the nodemanager.properties file is set correctly, by completing the following steps:
2. Change to the following directory:

```
cd /u02/private/oracle/config/domains/IAMAccessDomain/nodemanager/
```

3. Open the nodemanager.properties file for editing.
4. Update the ListenAddress property to the correct hostname as follows:

```
ListenAddress=OAMHOST1
```

5. Update the ListenPort property with the correct Listen Port details.
6. Make sure that QuitEnabled is set to 'true'. If this line is not present in the nodemanager.properties file, add the following line:

```
QuitEnabled=true
```

7. Change to the following directory:

```
cd /u02/private/oracle/config/domains/IAMAccessDomain/bin
```

8. Use the following command to start the Node Manager:

```
nohup ./startNodeManager.sh > /u02/private/oracle/config/domains/IAMAccessDomain
/nodemanager/nodemanager.out 2>&1 &
```

Starting the Node Manager in the Managed Server Domain Directory on OAMHOST2

Start Node Manager on subsequent OAMHOSTs.

1. Change to the following directory:

```
cd /u02/private/oracle/config/domains/IAMAccessDomain/bin
```

2. Use the following command to start the Node Manager:

```
nohup ./startNodeManager.sh > /u02/private/oracle/config/domains/IAMAccessDomain
/nodemanager/nodemanager.out 2>&1 &
```

Start the Administration Server

Start the Administration Server using the standard method you use. Because this is an Enterprise Deployment it is started using nodemanager.

After you have configured the domain and configured the Node Manager, you can start the Administration Server by using the Node Manager. In an enterprise deployment, the Node Manager is used to start and stop the Administration Server and all the Managed Servers in the domain.

To start the Administration Server by using the Node Manager:

1. Start the WebLogic Scripting Tool (WLST):

```
cd /u01/oracle/products/12c/access/ORACLE_COMMON_HOME/common/bin
./wlst.sh
```

2. Connect to Node Manager by using the Node Manager credentials:

```
wls:/offline>nmConnect('nodemanager_username','nodemanager_password',
            'IADADMINVHN','5556','IAMAccessDomain',
            '/u01/oracle/config/domains/IAMAccessDomain')
```

   Note:
   This user name and password are used only to authenticate connections between Node Manager and clients. They are independent of the server administrator ID and password and are stored in the nm_password.properties file located in the following directory:

```
IAD_ASERVER_HOME/config/nodemanager
```

3. Start the Administration Server:

```
nmStart('AdminServer')
```

Start the Managed Servers

Using the weblogic console or node manager start the Managed Servers for OAM and OAM Policy Manager.

Backup the Environment

Having validated the environment, it is advisable to take a complete backup of your environment at this time.

Upgrade Oracle Access Manager to 12.2.1.4

Having upgraded the environment to 12.2.1.3 you are now ready to upgrade to 12.2.1.4. The steps below describe how to do this.

Backup the Environment

Before starting the Upgrade, it is good practice to create a backup of the existing environment if you haven't already done so. This should include creating a database restore point (If you have flashback database enabled).

Shutdown the Domain

To perform the database the entire domain needs to be shut down this includes:

- All WebLogic Manged Servers.
- WebLogic Administration Server.
- Node Manager(s)

Deinstall Oracle Fusion Middleware 12.2.1.3

Start the deinstall wizard using the following command:

```
cd /u01/oracle/products/12c/oui/bin
./deinstall.sh
```

When the deinstall wizard loads select Oracle Identity Management 12.2.1.3 from the drop down list, then click Uninstall. The screen will close and another will open on this new screen select the following options:

1. On the Welcome Screen click Next
2. Verify that the feature sets to install do not include Oracle WebLogic server and click De-install
3. Once the Deinstallation is complete click Next and Finish.

Repeat the steps to Uninstall Oracle WebLogic server from the same location.

Manually removing the Oracle Home (/u01/oracle/products/12c/access) and any remaining.

Install Oracle Fusion Middleware 12.2.1.4 Binaries

Installing Fusion Middleware Infrastructure

Perform the following steps on all Oracle Access Manager compute instances. To start the installation program, perform the following steps:

1. Go to the directory where you downloaded the installation program.
2. Launch the installation program by invoking the java executable from the JDK directory on your system, as shown in the example below:

   ```
   set JAVA_HOME to /u01/oracle/products/12c/jdk

   JAVA_HOME/bin/java -d64 -jar distribution_file_name.jar
   ```

4. In this example:
   - Replace `JAVA_HOME` with the environment variable or actual JDK location on your system
   - Replace `distribution_file_name` with the actual name of the distribution JAR file

5. If you download the distribution from the Oracle Technology Network (OTN), then the JAR file is typically packaged inside a downloadable ZIP file.
6. To install the software required for the initial Infrastructure domain, the distribution you want to install is:

   ```
   fmw_12.2.1.4.0_infrastructure.jar
   ```

7. When the installation program appears, you are ready to begin the installation. Follow the onscreen prompts to install the Oracle Infrastructure into the Oracle Home:

   /u01/oracle/products/12c/access

For further information refer to : Installing and Configuring the Oracle Fusion Middleware Infrastructure 12.2.1.4

Installing Oracle Identity and Access Management

Perform the following steps on all Oracle Access Manager compute instances. To start the installation program, perform the following steps:

1. Go to the directory where you downloaded the installation program.
2. Launch the installation program by invoking the java executable from the JDK directory on your system, as shown in the example below:

   ```
   JAVA_HOME/bin/java -d64 -jar distribution_file_name.jar
   ```

3. In this example:
   - Replace `JAVA_HOME` with the environment variable or actual JDK location on your system
   - Replace `distribution_file_name` with the actual name of the distribution JAR file
4. If you download the distribution from the Oracle Technology Network (OTN), then the JAR file is typically packaged inside a downloadable ZIP file.
5. To install the software required for the initial Infrastructure domain, the distribution you want to install is:

   ```
   fmw_12.2.1.4.0_idm.jar
   ```

6. When the installation program appears, you are ready to begin the installation. Follow the onscreen prompts to install the Oracle Infrastructure into the Oracle Home:

   /u01/oracle/products/12c/access

7. When prompted choose: Collocated Oracle Identity and Access Manager (Managed through WebLogic Server)

For further information refer to : Installing and Configuring Oracle Identity and Access Management 12.2.1.4

The domain and database schemas do not change from release 12.2.1.3 to 12.2.1.4 so no further configuration/upgrade is required.

Starting Up the Domain

Start Node Manager

In EDG Environments, after you create the Managed Server domain directory, there are two domain home directories and two corresponding Node Manager instances on OAMHOST1. You use one Node Manager to control the Administration Server, running from Administration Server domain home, and you use the other Node Manager to control the Managed Servers, running from the Managed Server domain home.

You must start the two Node Managers independently.

If you have not separated out the Administration Server from the Managed Servers then just start the Node Manager in the Admin Server Domain Directory.

Starting the Node Manager in the Admin Server Domain Directory on OAMHOST1

8. Change to the following directory:

```
cd /u01/ oracle/config/domains/IAMAccessDomain/bin
```

9. Use the following command to start the Node Manager:

```
nohup ./startNodeManager.sh > /u01/oracle/config/domains/IAMAccessDomain
/nodemanager/nodemanager.out 2>&1 &
```

Starting the Node Manager in the Managed Server Domain Directory on OAMHOST1

Note: The Node Manager for the Managed Server's IAD_MSERVER_HOME will be reset every time the domain configuration is unpacked.

The ListenAddress will be changed to the *ADMINVHN* instead of the correct hostname. This needs to be changed to the correct value before starting the Node Manager service after an unpack is performed.

Follow these steps to update and start the Node Manager from the Managed Server home:

10. Verify that the listen address in the nodemanager.properties file is set correctly, by completing the following steps:
11. Change to the following directory:

```
cd /u02/private/oracle/config/domains/IAMAccessDomain/nodemanager/
```

12. Open the nodemanager.properties file for editing.
13. Update the ListenAddress property to the correct hostname as follows:

```
ListenAddress=OAMHOST1
```

14. Update the ListenPort property with the correct Listen Port details.
15. Make sure that QuitEnabled is set to 'true'. If this line is not present in the nodemanager.properties file, add the following line:

```
QuitEnabled=true
```

16. Change to the following directory:

```
cd /u02/private/oracle/config/domains/IAMAccessDomain/bin
```

17. Use the following command to start the Node Manager:

```
nohup ./startNodeManager.sh > /u02/private/oracle/config/domains/IAMAccessDomain
/nodemanager/nodemanager.out 2>&1 &
```

Starting the Node Manager in the Managed Server Domain Directory on OAMHOST2

Start Node Manager on subsequent OAMHOSTs.

18. Change to the following directory:

```
cd /u02/private/oracle/config/domains/IAMAccessDomain/bin
```

19. Use the following command to start the Node Manager:

```
nohup ./startNodeManager.sh > /u02/private/oracle/config/domains/IAMAccessDomain
/nodemanager/nodemanager.out 2>&1 &
```

Start the Administration Server

Start the Administration Server using the standard method you use. Because this is an Enterprise Deployment it is started using nodemanager.

After you have configured the domain and configured the Node Manager, you can start the Administration Server by using the Node Manager. In an enterprise deployment, the Node Manager is used to start and stop the Administration Server and all the Managed Servers in the domain.

To start the Administration Server by using the Node Manager:

20. Start the WebLogic Scripting Tool (WLST):

```
cd /u01/oracle/products/12c/access/ORACLE_COMMON_HOME/common/bin
./wlst.sh
```

21. Connect to Node Manager by using the Node Manager credentials:

```
wls:/offline>nmConnect('nodemanager_username','nodemanager_password',
            'IADADMINVHN','5556','IAMAccessDomain',
            '/u01/oracle/config/domains/IAMAccessDomain')
```

Note:
This user name and password are used only to authenticate connections between Node Manager and clients. They are independent of the server administrator ID and password and are stored in the nm_password.properties file located in the following directory:

```
IAD_ASERVER_HOME/config/nodemanager
```

22. Start the Administration Server:

```
nmStart('AdminServer')
```

Start the Managed Servers

Using the weblogic console or node manager start the Managed Servers for OAM and OAM Policy Manager.

Upgrade Webgates

Now that you have upgraded your environment to Oracle Access Manager 12.2.1.4 you should start to upgrade your Webgates, whilst this is not a mandatory step as existing 11g Webgates will continue to work against Oracle Access Manager 12c it is best practice to ensure that you are using the latest security fixes.

Create an OHS 12.2.1.4 Installation

The procedure below can be used as an example:

- Install or Upgrade Oracle HTTP Server 12.2.1.4, this process is described elsewhere.
- If you have created a new Oracle HTTP server 12.2.1.4 installation you will need to move your existing configuration to the new Oracle HTTP 12.2.1.4 installation, this process is described elsewhere.

Configuring Oracle HTTP Server 12c WebGate

This section describes how to configure an already deployed Oracle HTTP instance.

1. Change directory to the following location in the Oracle HTTP Server Oracle home:

```
cd WEB_ORACLE_HOME/webgate/ohs/tools/deployWebGate/
```

2. Run the following command to create the WebGate Instance directory and enable WebGate logging on OHS Instance:

```
./deployWebGateInstance.sh -w WEB_CONFIG_DIR -oh WEB_ORACLE_HOME
```

For example:

```
./deployWebGateInstance.sh -w
/u02/private/oracle/config/domains/ohsDomain/config/fmwconfig/components/OHS/ohs1 -oh
/u02/private/oracle/products/web
```

3. Run the following command to ensure that the LD_LIBRARY_PATH environment variable contains WEB_ORACLE_HOME/lib directory path:

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:WEB_ORACLE_HOME/lib
```

4. Change directory to the following directory

```
WEB_ORACLE_HOME/webgate/ohs/tools/setup/InstallTools
```

5. Run the following command from the InstallTools directory.

```
./EditHttpConf -w WEB_CONFIG_DIR -oh WEB_ORACLE_HOME -o output_file_name
```

Note:
The -oh WEB_ORACLE_HOME and -o output_file_name parameters are optional.

Regenerate Webgate Artifacts

The simplest way to regenerate the WebGate Artifacts is to make a benign change to the WebGate you wish regenerate. For example:

1. Login to the OAM console.
2. Click on Agents
3. Search for the Agent you are interested in and click on it to bring up the configuration page, for example Webgate_IDM_11g
4. Change one of the existing values and click Apply (you can always change it back and apply again) this will force the agent to be regenerated
5. Click Download and the Agent Config will be downloaded you your machine.

Copy Artifacts to WEBHOSTs

Copy the file that was downloaded you your host to each of the webgate machines

Configure WebGate

Login to each of your WEBHOSTs and use the uploaded file to configure the webgates.

1. Change Directory to the WebGate configuration directory
   For example:

```
cd
/u02/private/oracle/config/domains/ohsDomain/config/fmwconfig/components/OHS/ohs1/webga
te
```

2. Unzip the file you uploaded it should place the files in the correct locations inside the config.

Note:
If you need to redeploy the ObAccessClient.xml to WEBHOST1 and WEBHOST2, delete the cached copy of ObAccessClient.xml and its lock file, ObAccessClient.xml.lck from the servers. The cache location on WEBHOST1 is: WEB_DOMAIN_HOME/servers/ohs1/cache/

3. Restart the Oracle HTTP Server

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 Access Manager deployment via Load Balancer then you have two options available to you, you can either switch to using the load balancer inside OCI which you will have configured to access your new application, or you can point your existing On Premise Load Balancer to point to your new OCI OAM Deployment

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.

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 host names (iadadmin/login) point to the virtual hosts inside the OCI load balancer.

Cutover Applications

If you have applications with webgates or other identity agents then you need to update your DNS so that the entries for OAMHOST1 and OAMHOSTn point to the OAM servers in OCI.

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 Access Manager 12.2.1.3

  Upgrading Oracle Access Manager 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

Clone and Upgrade Case Study – Oracle Access Manager
March, 2021
Author: Michael Rhys